RADWARE LTD
Form 20-F
March 28, 2018

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 20-F

REGISTRATION STATEMENT PURSUANT TO SECTION 12(b) OR 12(g) OF THE SECURITIES EXCHANGE ACT OF 1934

OR

ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the fiscal year ended
December 31, 2017

OR

TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the transition period from __________ to __________

OR

SHELL COMPANY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

Date of event requiring this shell company report _________

Commission file number: 000-30324

RADWARE LTD.
(Exact name of registrant as specified in its charter)

Israel
(Jurisdiction of incorporation or organization)

22 Raoul Wallenberg Street, Tel Aviv 6971917, Israel
(Address of principal executive offices)

Gadi Meroz, Adv.
General Counsel
Tel. +972-3-7668666, Fax: +972-3-7668982

22 Raoul Wallenberg Street, Tel Aviv 6971917, Israel
(Name, Telephone, E-mail and/or Facsimile number and Address of Company Contact Person)

Securities registered or to be registered pursuant to Section 12(b) of the Act:

Title of each class	Name of each exchange on which registered
Ordinary Shares, NIS 0.05 par value per share	The Nasdaq Stock Market LLC

Securities registered or to be registered pursuant to Section 12(g) of the Act:
None
(Title of Class)

Securities for which there is a reporting obligation pursuant to Section 15(d) of the Act:
None
(Title of Class)

Indicate the number of outstanding shares of each of the issuer's classes of capital or common stock as of the close of the period covered by the annual report (December 31, 2017):

44,133,954 Ordinary Shares, NIS 0.05 par value per share

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act.

Yes No

If this report is an annual or transition report, indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934.

Yes No

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days.

Yes No

Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files).

Yes No

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer," and "emerging growth company" in Rule 12b-2 of the Exchange Act. (Check one):

Large Accelerated Filer Accelerated Filer

Non-Accelerated Filer o Emerging growth company

If an emerging growth company that prepares its financial statements in accordance with U.S. GAAP, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards† provided pursuant to Section 13(a) of the Exchange Act.

† The term "new or revised financial accounting standard" refers to any update issued by the Financial Accounting Standards Board to its Accounting Standards Codification after April 5, 2012.

Indicate by check mark which basis of accounting the registrant has used to prepare the financial statements included in this filing:

U.S. GAAP

International Financial Reporting Standards as issued by the International Accounting Standards Board

Other

If "Other" has been checked in response to the previous question indicate by check mark which financial statement item the registrant has elected to follow:

Item 17 Item 18

If this is an annual report, indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act).

Yes No

INTRODUCTION

Unless the context otherwise requires, all references in this annual report to:

- "we," "us," "our," the "Company," and "Radware" are to Radware Ltd. and its subsidiaries;
- "ordinary shares" are to our Ordinary Shares, par value NIS 0.05 per share;
- "Companies Law" or the "Israeli Companies Law" are to the Israeli Companies Law, 5759-1999, as amended;
- the "SEC" are to the U.S. Securities and Exchange Commission;
- the "U.S." are to the United States;
- "U.S. GAAP" are to generally accepted accounting principles in the United States;
- "Nasdaq" are to the Nasdaq Global Market (formerly, the Nasdaq National Market);
- "dollars", "$" or "US$" are to U.S. dollars; and
- "NIS" or "shekels" are to New Israeli Shekels.

We have registered trademarks for, among others, Radware®; Radware Logo: ®; OnDemand Switch®; Alteon®; APSolute®; LinkProof®; DefensePro®; CID®; SIPDirector®; AppDirector®; AppXcel®; AppXML®; AppWall®; APSolute Insite®; Triangulation®; SmartNat®; StringMatch Engine®; Web Server Director®; Fireproof®; SecureFlow®; APSolute Vision®; VAdapter®; vDirect®; Alteon VA®; AppShape®; FastView®; DefenseFlow®; TeraVIP®; Virtual Director®; DefensePipe®;"ADC Fabric®"; CyberStack® and "Virtual DefensePro® and we have trademark applications pending for, among others, "ADC-VX"™; VADI™ (Virtual Application Delivery Infrastructure) and "Inflight"™. Unless the context otherwise indicates, all other trademarks and trade names appearing in this annual report are owned by their respective holders.

Our consolidated financial statements appearing in this annual report are prepared in dollars and in accordance with U.S. GAAP, and are audited in accordance with the standards of the Public Company Accounting Oversight Board in the United States.

On March 25, 2018, the exchange rate between the NIS and the dollar, as quoted by the Bank of Israel, was NIS 3.491 to $1.00. Unless the context otherwise indicates, statements in this annual report that provide the dollar equivalent of NIS amounts or provide the NIS equivalent of dollar amounts are based on such exchange rate.

On April 12, 2013, we effected a two-for-one forward split of our ordinary shares, and accordingly the par value of our ordinary shares has changed from NIS 0.1 to NIS 0.05 per share. Unless indicated otherwise by the context, all ordinary shares, options and per share amounts as well as stock prices in this annual report have been adjusted to give retroactive effect to the stock split for all periods presented.

Statements made in this annual report concerning the contents of any contract, agreement or other document are summaries of such contracts, agreements or documents and are not complete descriptions of all of their terms. If we filed any of these documents as an exhibit to this annual report or to any registration statement or annual report that we previously filed, you may read the document itself for a complete description of its terms, and the summary included herein is qualified by reference to the full text of the document which is incorporated by reference into this annual report.

Unless otherwise indicated, information contained in this annual report concerning our industry and the markets in which we operate, including our competitive position and market opportunity, is based on information from our own management estimates and research, as well as from industry and general publications and research, surveys and studies conducted by third parties. Management estimates are derived from publicly available information, our knowledge of our industry and assumptions based on such information and knowledge, which we believe to be reasonable. Our management estimates have not been verified by any independent source, and we have not independently verified any third-party information. In addition, assumptions and estimates of our and our industry's future performance are necessarily subject to a high degree of uncertainty and risk due to a variety of factors, including those described in Item 3.D "Risk Factors" below.

CAUTIONARY STATEMENT REGARDING
FORWARD-LOOKING STATEMENTS

Except for the historical information contained herein, the statements contained in this annual report are forward-looking statements, within the meaning of the Private Securities Litigation Reform Act of 1995 and other federal securities laws with respect to our business, financial condition and results of operations. Actual results could differ materially from those anticipated in these forward-looking statements as a result of various factors, including all the risks discussed in "Risk Factors" and elsewhere in this annual report.

We urge you to consider that statements which use the terms "believe," "do not believe," "expect," "plan," "intend," "estimate," "anticipate," and similar expressions are intended to identify forward-looking statements. Such forward-looking statements appear in Item 3.D "Risk Factors", Item 4 "Information on the Company", and Item 5 "Operating and Financial Review and Prospects" as well as elsewhere in this annual report. These statements reflect our current views with respect to future events and are based on assumptions and are subject to risks and uncertainties, including those discussed under Item 3.D "Risk Factors" and in our other filings with the SEC. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of the date hereof.

Except as required by applicable law, including the securities laws of the United States, we do not intend to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise.

Table of Contents

PART I

ITEM 1. IDENTITY OF DIRECTORS, SENIOR MANAGEMENT AND ADVISERS

Not applicable.

ITEM 2. OFFER STATISTICS AND EXPECTED TIMETABLE

Not applicable.

ITEM 3. KEY INFORMATION

A. Selected Financial Data

The following tables present selected information from our consolidated statements of income and balance sheet data for the periods and as of the dates indicated. We derived the selected consolidated statements of income for the years ended December 31, 2015, 2016 and 2017 and the selected balance sheet data as of December 31, 2016 and 2017 from our audited consolidated financial statements included elsewhere in this annual report on Form 20-F, which have been prepared in accordance with U.S. GAAP and audited by Kost, Forer, Gabbay & Kasierer, an independent registered public accounting firm and a member firm of Ernst & Young Global. The selected consolidated statements of income data for the years ended December 31, 2013 and 2014 and the selected balance sheet data as of December 31, 2013, 2014 and 2015 are derived from our audited consolidated financial statements not included in this annual report, which have been prepared in accordance with U.S. GAAP.

You should read the following selected financial data together with the section of this annual report entitled "Operating and Financial Review and Prospects" and our consolidated financial statements together with the notes thereto included elsewhere in this annual report

	Year ended December 31,				
	2017	2016	2015	2014	2013
	(U.S. dollars and share amounts in thousands, except per share data)				
Consolidated Statements of Income Data:					
Revenues:					
Products	$117,968	$110,186	$136,793**	$143,466**	$118,727
Services	93,401	86,399	79,773 **	78,426 **	74,270
	211,369	196,585	216,566	221,892	192,997
Cost of revenues:					
Products	30,862	27,320	29,159	29,448	27,066
Services	8,754	8,375	9,041	10,284	9,669
	39,616	35,695	38,200	39,732	36,735
Gross profit	171,753	160,890	178,366	182,160	156,262
Operating expenses, net:					
Research and development, net	59,003	51,732	49,987	44,081	40,983
Sales and marketing	108,744	103,774	93,347	93,203	82,815
General and administrative	17,577	18,133	17,033	19,797	14,895
Other income	(6,900)	-	-	-	-
Total operating expenses	178,424	173,639	160,367	157,081	138,693
Operating income (loss)	(6,671)	(12,749)	17,999	25,079	17,569
Financial income, net	4,830	5,741	5,867	5,802	4,494
Income (loss) before taxes on income	(1,841)	(7,008)	23,866	30,881	22,063
Taxes on income	(5,652)	(1,651)	(5,297)	(5,931)	(4,008)
Net income (loss)	$(7,493)	$(8,659)	$18,569	$24,950	$18,055
Basic net earnings (loss) per share*	$(0.17)	$(0.20)	$0.40	$0.55	$0.40
Diluted net earnings (loss) per share*	$(0.17)	$(0.20)	$0.40	$0.53	$0.39

* See notes 2(y) and 11 to our consolidated financial statements included elsewhere in this annual report for an explanation regarding the computation of basic and diluted net earnings (loss) per ordinary share.

** The breakdown between product and service revenues for 2015 and 2014 was reclassified to include most subscription revenues in product revenues rather than allocating some to product and some to service revenues, which has resulted in a change to previously published figures for the periods ended December 31, 2015 and December 31, 2014, respectively.

	Year ended December 31, 2017	2016	2015	2014	2013
	(in thousands)				
Weighted average number of ordinary shares used in computing basic net earnings (loss) per share	43,476	43,868	45,895	45,309	44,760
Weighted average number of ordinary shares used in computing diluted net earnings (loss) per share	43,476	43,868	46,739	46,895	46,717

	As of December 31, 2017	2016	2015	2014	2013
	(U.S. dollars in thousands)				
Consolidated Balance Sheet Data:					
Cash and cash equivalents, short-term bank deposits and marketable securities	$200,961	$226,086	$130,669	$104,416	$134,826
Long-term bank deposits and marketable securities	143,338	94,059	184,457	226,273	150,874
Working capital	140,765	181,502	101,029	76,010	113,546
Total assets	469,088	430,336	430,887	442,573	388,734
Shareholders’ equity	315,356	299,763	319,123	333,697	294,120
Capital Stock	349,923	326,001	313,445	294,738	263,420

B. Capitalization and Indebtedness

Not applicable.

C. Reasons for the Offer and Use of Proceeds

Not applicable.

D. Risk Factors

You should carefully consider the following risks before deciding to purchase, hold or sell our ordinary shares. Our business, operating results and financial condition could be seriously harmed due to any of the following risks. The following risks are not the only risk factors facing our Company. Additional risks and uncertainties not presently known to us or that we currently deem immaterial may also affect our business. The trading price of our ordinary shares could decline due to any of these risks. You should also refer to the other information contained or incorporated by reference in this annual report, before making any investment decision regarding our Company.

Risks Related to Our Business and Our Industry

We have incurred net losses in the past, and may incur losses in the future.

Although we were profitable in the past several years, including 2015, we incurred net losses during 2016 and 2017, mainly as a result of an increase in our operating expenses compared to a lower rate of increase in our revenues in 2017 and a decrease in revenues in 2016. Our ability to achieve or increase profitability in the future depends in part on the following factors: the economic health of the global economy; the rate of growth of, and changes in technology trends in our market and other industries in which we currently or may in the future operate; our ability to develop and manufacture new products and technologies in a timely manner; the competitive position of our products; the continued acceptance of our products and services by our customers and in the industries that we serve; and our ability to manage expenses. In the future, it may be necessary to undertake cost reduction initiatives to become profitable, which could lead to a deterioration of our competitive position. Any difficulties that we encounter as we reduce our costs could negatively impact our results of operations and cash flows. We cannot assure you that we will return to profitability. Our revenues also may not grow, may grow at a lower rate than experienced in 2017 or may decline as they did in 2016, which would negatively impact our results of operations and cash flows. Over the past few years, we changed our sales model to increased product subscription sales, leading to deferral of revenue recognition, while our operating expenses are based on current sales levels regardless of revenue recognition.

During 2017, our operating expenses grew mainly due to investments in sales, the Seculert acquisition, marketing initiatives and the appreciation of the NIS against the dollar, which raised the dollar cost of our Israeli operations. We may continue to increase our operating expenses in future periods. Our decision to increase operating expenses and the scope of such increases depends upon several factors, including the market situation and the effectiveness of our past expenditures. We may continue to make additional expenditures in anticipation of generating higher revenues, which we may not realize, if at all, until sometime in the future. This could cause reductions in our profitability or lead to losses, as it did in 2016 and 2017. Additionally, a failure of any acquisition or product development initiative to produce increased revenues could have a material adverse effect on our operations and profitability.

If our revenues do not increase as anticipated or decline, or if our expenses increase more than anticipated, we may incur losses.

We must manage our anticipated growth effectively in order to be profitable.

We have actively expanded our operations in the past and may continue to expand them in the future in order to gain market share in the evolving market for cyber security and application delivery solutions. This expansion has required, and may continue to require, managerial, operational and financial resources.

In some cases, we may choose to increase our cost of operations at the expense of our short term profitability in order to support future expansion and growth. We cannot assure you that we will continue to expand our operations successfully. If we are unable to manage our expanding operations effectively, our revenues may not increase or may decline, our cost of operations may rise and we may not be profitable.

Global rollout of new information systems could disrupt our operations and cause unanticipated increases in our costs.

In the past few years, we have invested significant capital and human resources in a project for a company-wide enterprise resource planning, or ERP, system, including modules such as a new customer relationship management, or CRM, system for our sales operations and new customer service system for our customer support. We intend to continue to invest significant capital and human resources to further improve and implement our ERP and other information systems. Any major disruptions or deficiencies in the design and implementation of the new information systems, particularly those that impact our operations, could adversely affect our ability to process customer orders, ship products, provide services and support to our customers, bill and track our customers, timely report our financial results and otherwise run our business.

Changing or severe global economic conditions and volatility of the market for our products, including slow-down in expenditures and other trends in our industry, could have a material adverse effect on our results of operations.

Our business is affected by global economic conditions and their impact on current and anticipated market demand for our products. While the global economy has improved in recent years, uncertainties surrounding the strength of the recovery in many regions remain. As our operations are on a global level, we may be affected by such events and other economic and political uncertainties. Uncertainty about current global economic conditions continues to pose a risk as customers may postpone or reduce spending in response to such uncertainties. For example, Brexit and the withdrawal of the United Kingdom from the European Union, as well as other member countries' public discussions about the possibility of withdrawing from the European Union, may also create global economic uncertainty, which may impact, among other things, the demand for our products and services. Furthermore, should companies in our target markets reduce capital or operational expenditures, we may experience a reduction in sales, longer sales cycles, and slower adoption of new technologies as well as downward pressure on the price of our products. In addition, if the market for our products and services is flat and our customers experience low visibility, we may not be able to increase our sales (whether direct sales or indirect sales through our distributors). Each of the above scenarios could have a material adverse effect on our business, operating results and financial condition.

Competition in the market for cyber security and application delivery solutions and our industry in general is intense. As a result, we may lose market share and we may be unable to maintain profitability.

The information technology, or IT, marketplace is competitive and has very few barriers to entry. In particular, the cyber security and application delivery market in which we focus is highly competitive. We expect competition to intensify in the future, and we may lose market share if we are unable to compete effectively.

Most of our competitors have greater financial, personnel and other resources than us, which may limit our ability to effectively compete with them. Our principal competitors in the cyber security and application delivery market include: F5 Networks, Inc., Arbor Networks, Inc., Akamai Technologies, Inc., or Akamai, Citrix Systems, Inc., A10 Networks, Inc., Imperva, Inc., or Imperva, Amazon.Com, Inc. (through Amazon Web Services' ELB service), Microsoft Corporation (through Microsoft Azure) and Brocade Communications Systems, Inc. (through Broadcom Limited), HP Inc. and Intel Corporation (through McAfee, Inc.). We expect to continue to face additional competition as new participants enter the market or extend their portfolios into related technologies. Larger companies with substantial resources, brand recognition and sales channels may form alliances with or acquire competing cyber security and application delivery solutions and emerge as significant competitors.

Competition may result in lower prices or reduced demand for our products and a corresponding reduction in our ability to recover our costs, which may impair our ability to achieve, maintain and increase profitability. Furthermore, the dynamic market environment poses a challenge in predicting market trends and expected growth. We cannot assure you that we will be able to implement our business strategy in a manner that will allow us to be competitive. If any of our competitors offer products or services that are more competitive than ours, we could lose market share and our business, financial condition and results of operations could be materially and adversely affected as a result.

Our international sales may expose us to additional risks

We currently offer our products in over 40 countries, including the U.S. For the years ended December 31, 2017 and 2016, our sales outside the Americas (which include the U.S., Canada as well as Central America and Latin America, or CALA) represented approximately 54% and 57%, respectively, of our total sales. Our international business activity involves varying degrees of risk and uncertainty inherent in doing business in so many different jurisdictions. Such risks include, among others, difficulties and costs of staffing and managing foreign operations; the possibility of unfavorable circumstances and additional compliance costs arising from host country laws or regulations, including unexpected changes of interpretations thereof and reduced protection for intellectual property rights in some countries; partial or total expropriation, export duties and quotas; local tax exposure; political instability, insurrection or war; differences in business practices; and recessionary environments in multiple foreign markets, such as those that occurred in some European countries in the past several years. We cannot be certain that the foregoing factors will not have a material adverse effect on our future revenues and, as a result, on our business, operating results and financial condition.

We may experience significant fluctuations in our quarterly financial performance.

Our quarterly operating results have varied significantly in the past and may vary significantly in the future as a result of various factors, many of which are outside of our control. A delay in our recognition of revenue may have a negative impact on our results of operations for a given quarter. In addition, over the past few years, we changed our sales model, to increased product subscription sales, leading to a deferral of revenue recognition. While hardware products are recognized almost immediately upon their shipment and invoicing, product services and support services are recognized throughout the term of their respective contract length. At the same time, we base our decisions regarding our operating expenses on anticipated sales trends and our expense levels are relatively fixed. In addition, due to the change in our sales model, leading to deferral of revenue recognition, while operating expenses are based on current sales levels, we witnessed an increase in our total current operating expenses, leading to the operating loss we incurred in 2017. As such, because only a small portion of our expenses are dependent on our revenues, if our revenues fall below our expectations, our earnings and profitability for that period will be materially and adversely affected. Our future operating results will depend on many additional factors, including, but not limited to, the following:

- demand for our products;
- sales cycles (see "Risk Factors— Our products generally have long sales cycles, which increase our costs in obtaining orders and reduce the predictability of our earnings");
- seasonal trends, as more fully described below;
- new product announcements by us and our competitors;
- budgeting cycles of our customers;
- changes in our strategy;
- currency exchange rate fluctuations and economic conditions in the geographic areas where we operate; and
- those other factors discussed in this annual report.

In addition, our quarterly operating results have been, and are likely to continue to be, influenced by seasonal fluctuations in the sales of our products and services. Because our sales have mostly grown year-over-year since our inception, these fluctuations may not be apparent from our historical financial statements. However, we believe that our sales and sales growth have been, and will continue to be, affected by the seasonal purchasing patterns of some of our customers, primarily in the first quarter ended March 31 when our sales may be reduced due to our customers' annual purchasing budget planning process and in the third quarter ended September 30 due to a slowdown in business activities during the summer months in Europe. Conversely, our sales during the fourth quarter ended December 31 have typically increased because some of our customers tend to make greater capital expenditures towards the end of their fiscal years.

Due to the foregoing factors, our sales and operating results in any quarter are difficult to forecast, and period-to-period comparisons of our operating results may not necessarily be meaningful. In addition, in some future quarter our operating results may be below the expectations of public market analysts and investors. In such event the price of our ordinary shares may be materially adversely affected.

If the market for cyber security and application delivery solutions does not continue to develop and grow, we will not be able to sell enough of our products to maintain profitability.

The cyber security and application delivery market in which we operate is rapidly evolving and we cannot assure you that it will continue to develop and grow. In addition, we cannot assure you that our products and technology will keep pace with the changes to this market. Market acceptance of cyber security and application delivery solutions may be inhibited by, among other factors, a lack of anticipated congestion and strain on existing network infrastructures and the availability of alternative solutions. If demand for cyber security and application delivery solutions does not continue to grow, or grows in a slower pace than expected, we may not be able to sell enough of our products to maintain and increase our profitability.

If the market for our cloud based solutions does not continue to develop and grow, we will sustain capital and operation loses.

As our business continues to shift to the cloud and we continue to offer more cloud based solutions, our investments, both capital and operational, in our cloud business increases. We cannot assure you that our cloud bases sales will continue to develop and grow. In addition, we cannot assure you that our services and technology will keep pace with the changes to this market. Specifically, the emergence of alternative solutions, such as Amazon AWS and Microsoft Azure public cloud may negatively affect sales of our products and services.

We must develop new products and services as well as enhancements and new features to existing products to remain competitive. If we fail to develop new products and services of fail to develop product enhancements on a timely basis, we may lose market share.

The market for cyber security and application delivery solutions is characterized by rapid technological changes, frequent new product introductions, changes in customer requirements and evolving industry standards. Our products typically constitute a critical portion of our customers' data centers. In recent years, the capacity of transactions in such data centers has been steadily increasing. Due to such increases in capacity and in order to remain competitive in our industry, we must address the increased needs of our customers by developing more powerful platforms for our products. Additionally, we must address increased demands by our customers for advancements in our applications in order to support our customers' growing needs and evolutions in their data centers. In order to meet this challenge and remain competitive in the market, we have introduced and must continue to introduce new enhancements to our existing product lines. Furthermore, the cyber-security market is characterized by rapid changing customer requirements driven by legal, regulatory and self-regulatory compliance mandates, frequent new product introductions and enhancements and evolving industry standards in computer hardware and software technology. Customers and industry analysts expect speedy introduction of software and new functionality to respond to new cyber threats, requirements and risks and we may be unable to meet these expectations.

Accordingly, our future success will depend to a substantial extent on our ability to: invest significantly in research and development; develop, introduce and support new products and services and enhancements on a timely basis; and gain market acceptance of our products.

We have developed and are currently developing new products and enhancements to our existing products and services offerings. Our development of new products and enhancement of our offerings is undertaken in an effort to remain competitive in our market, and our failure to do so could result in a decrease in our revenues. In addition, we have invested and must continue to invest in research and development in order to remain competitive in our industry. However, there can be no assurances that continued investment and higher costs of research and development, including associated capital expenditures, will ultimately result in us maintaining or increasing our market share, which would result in a decline to our operating results. If our research and development expenses increase without a corresponding increase in our revenues, it could have a material adverse effect on our operating results. Also, we may not be able to successfully complete the development and market introduction of new products or product enhancements in a timely manner. If we fail to develop and deploy new products and product enhancements on a timely basis, or if we fail to gain market acceptance of our new products, our revenues will decline and we may lose market share to our competitors.

During 2017, we invested in, and plan to continue to invest in 2018, in developing or when appropriate, acquiring, capabilities to advance our product offering and market vision. One of the primary trends in the past few years in our industry is the shift to providing services through the cloud. We have also invested and intend to continue to invest substantial resources in developing and enhancing our cloud offerings. There is no assurance that we will be successful in marketing and selling our next generation cyber security and application delivery solutions, or that we will be able to grow revenues to justify our investments.

Moreover, we identified an industry trend in the past few years that drives a shift from customers' maintaining on-premise physical appliances or having internal specialized knowledge to support and maintain complex IT infrastructure to relying on third party provided managed IT services. In response to such market trend, we have increased our support offerings to include, among others, such managed services.

Our failure to develop and market new products, product enhancements or services on a timely basis or our failure to gain market acceptance of our new products and services could result in our loss of market share and our business and could materially and adversely affect our financial condition and results of operations.

Even if we are able to anticipate, develop and commercially introduce enhancements and new products and services, there can be no assurance that we will be successful in developing sufficient market awareness of them or that such enhancements or new products and services will achieve widespread market acceptance. For example, while the majority of our current revenues are derived from the sales of our DefensePro and Alteon appliances, we also offer our security products as cloud-based services. The market for cloud-based security solutions is relatively new and it is uncertain whether our security cloud-based services will continue to gain rapid market acceptance. In addition, diversifying our product offerings will require significant investment and planning, will bring us more directly into competition with software and cloud-based providers that may be better established or have greater resources than we do, will require additional investments of time and resources in the development and training of our channel and strategic partners and will entail a significant risk of failure.

Government regulation affecting our business is evolving, and unfavorable changes could harm our business.

Laws and regulations that apply to cloud-based solutions are becoming more prevalent and constantly evolving, particularly in the area of privacy. We may be impacted by changes in privacy-related regulations governing the collection, use, retention, sharing and security of data that we receive from our customers and/or visitors to their websites and others. Complying with a diverse range of privacy requirements could cause us to incur substantial costs or require us to change our business practices in a manner adverse to our business. Any failure, or perceived failure, by us to comply with any privacy-related laws, government regulations or directives, or industry self-regulatory principles could result in damage to our reputation or proceedings or actions against us by governmental entities or others, which could potentially have an adverse effect on our business. For example, the European General Data Protection Regulation (Regulation (EU) 2016/679), or GDPR, that will come into effect on May 25, 2018, includes operational requirements for companies that receive or process personal data of residents of the European Union and non-compliance will result in significant penalties. Our compliance with GDPR carried and will continue to carry capital expenditure investments.

Furthermore, laws, regulations and industry standards are subject to drastic changes that, particularly in the case of industry standards, may arrive with little or no notice, and these could either help or hurt the demand for our products. If we are unable to adapt our products and services to changing regulatory standards in a timely manner, or if our products fail to assist our customers with their compliance initiatives, our customers may lose confidence in our products and could switch to competing solutions. In addition, if regulations and standards related to cyber-security are changed in a manner that makes them less onerous, our customers may view government and industry regulatory compliance as less critical to their businesses, and our customers may purchase fewer of our products and services, or none at all. In either case, our sales and financial results would suffer.

Outages, interruptions or delays in hosting services could impair the delivery of our cloud-based security services and harm our business.

We operate infrastructure that supports our distributed denial of service (DDoS) and web application firewall (WAF) Cloud-based services and scrubbing centers' services. Despite precautions taken within our own internal network and at these third party facilities, the occurrence of a natural disaster or an act of terrorism or other unanticipated problems could result in lengthy interruptions in our services.

The DDoS and WAF cloud-based security services that we provide are operated from a network of third party facilities that host the software and systems that operate these security services. Any damage to, or failure of, our internal systems or systems at third party hosting facilities could result in outages or interruptions in our DDoS and WAF cloud-based services. Outages or interruptions in our DDoS and WAF cloud-based security services may cause our customers and potential customers to believe our DDoS and WAF cloud-based security services are unreliable, cause us to issue credits or pay penalties, cause customers to terminate their subscriptions and adversely affect our reputation and renewal rates and our ability to attract new customers, ultimately harming our business and revenue.

Some of our products contain "open source" software, and any failure to comply with the terms of one or more of these open source licenses could negatively affect our business.

Some of our products utilize open source technologies. Some open source software licenses require users who distribute or make available as a service open source software as part of their own software product to publicly disclose all or part of the source code of the users' software product or to make available any derivative works of the open source code on unfavorable terms or at no cost. We have established processes to help alleviate these risks, including a review process for screening requests from our development organization for the use of open source software, but we cannot be sure that all open source software is submitted for approval prior to use in our products. In addition, open source license terms may be ambiguous and many of the risks associated with use of open source software cannot be eliminated, and could, if not properly addressed, negatively affect our business. We may face ownership claims of third parties over, or seeking to enforce the license terms applicable to, such open source software, including by demanding the release of the open source software, derivative works or our proprietary source code. Any such requirement to disclose our source code or other confidential information related to our products could materially and adversely affect our competitive position and may adversely impact our business, results of operations and financial condition. In addition, if the license terms for the open source code change, we may be forced to re-engineer our software or incur additional costs.

We may pursue mergers or make acquisitions or other investments that could disrupt our business and harm our financial condition.

As part of our business strategy, we may invest in or acquire complimentary businesses, technologies or assets or enter into joint ventures or other strategic relationships with third parties. For example, in January 2017, we acquired Seculert, a company engaged in cyber-attack detection and HTTP analytics solutions and developing user and entity behavioral analysis "UEBA" solutions. In connection with the acquisition of Seculert and with any future acquisitions, we have and may in the future assume liabilities, incur acquisition related costs, incur amortization expenses or realize write-offs on assets no longer being used or phased out. In addition, the future valuation of these acquisitions may decrease from the market price paid by us which could result in the impairment of our goodwill and other intangible assets associated with the relevant acquired assets. Moreover, our operation of any acquired or merged businesses, technologies or assets could involve numerous risks, including:

- post-merger integration problems resulting from the combination of any acquired operations with our own operations or from the combination of two or more operations into a new merged entity;

- diversion of management's attention from our core business;
- substantial expenditures, which could divert funds from other corporate uses;
- entering markets in which we have little or no experience;
- loss of key employees of the acquired operations; and
- known or unknown contingent liabilities, including, but not limited to, tax and litigation costs.

We cannot be certain that the Seculert acquisition or that any future acquisitions or mergers will be successful. If the operation of the business of any future acquisitions or mergers disrupts our operations, our results of operations may be adversely affected, and even if we successfully integrate the acquired business with our own, we may not receive the intended benefits of the acquisition. In addition, our pursuit of potential acquisitions may divert our management's attention from our core business and require considerable cash outlays at the expense of our existing operations, whether or not such transactions are consummated. For example, in January 2017, we acquired Seculert Ltd., or Seculert, a company engaged in cyber-attack detection and hypertext transfer protocol (HTTP) analytics solutions, including the development user and user entity behavioral analysis (UEBA) solutions. This acquisition resulted in additional operating costs. A failure of any acquisitions or product developments to produce increased revenues could have a material adverse effect on our operations and profitability.

An increasing amount of intangible assets and goodwill on our books may in the future lead to significant impairment charges.

The amount of goodwill and intangible assets on our consolidated balance sheet is significant. We regularly review our intangible and tangible assets, including goodwill, for impairment. Goodwill and acquired research and development not yet ready for use are subject to impairment review at least annually. Other intangible assets are reviewed for impairment when there is an indication that impairment may have occurred. Impairment testing has led to and may in the future lead to significant additional impairment charges.

We depend upon independent distributors to sell our products to customers. If our distributors do not succeed in selling our products, we may not be able to operate profitably.

We sell our products primarily to independent distributors, including value added resellers (VARs), original equipment manufacturers (OEMs) and system integrators, and are highly dependent upon these distributors' active marketing and sales efforts. We currently have active independent distributors and resellers that sell our products to the end-user customer. Our distribution agreements with our distributors generally are non-exclusive, ranging from one-year agreements to multiple-year duration with no obligation on the part of our distributors to renew the agreements. Our distribution agreements also typically do not prevent our distributors from selling products of our competitors and do not contain minimum sales or marketing performance requirements. As a result, our distributors may give higher priority to products of our competitors or their own products, thereby reducing their efforts to sell our products. In addition, we may not be able to maintain our existing distribution relationships, and we may not be successful in replacing them on a timely basis or at all. We may also need to develop new distribution channels for new products, and we may not succeed in doing so. Any changes in our distribution channels, including a termination or other disruption of our commercial relationship with our distributors, or our inability to establish distribution channels for new products could impair our ability to sell our products and result in a material adverse effect on our business, financial condition and results of operations.

Our products generally have long sales cycles, which increase our costs in obtaining orders and reduce the predictability of our earnings.

Our products are technologically complex and are typically intended for use in applications that may be critical to the business of our customers. As a result, our pre-sales process is often subject to delays associated with budgetary constraints, lengthy approval and procurement processes that typically accompany the design and testing of new equipment. The sales cycles of our products to new customers can last as long as twelve months (and in some cases, for example with carrier customers, even longer) from initial presentation to sale. This long sales cycle results in a delay to our recognition of revenue and results in our need to make significant investments in marketing and sales. Long sales cycles also subject us to risks not usually encountered in a short sales cycle, including our customers' budgetary constraints and internal acceptance reviews and processes prior to purchase. In addition, orders expected in one quarter could shift to another because of the timing of our customers' procurement decisions. Furthermore, customers may defer orders in anticipation of new products or product enhancements introduced by us or by our competitors. Such long sales cycles and order deferrals may cause us to keep levels of inventory that are higher than what we will be eventually able to use, which, over time, may lead to write-offs of such unused inventory. These factors complicate our planning processes and reduce the predictability of our earnings.

Currency exchange rates and fluctuations of exchange rates could have a material adverse effect on our results of operations.

We are impacted by exchange rates and fluctuations thereof in a number of ways, including:

- A large portion of our expenses in Israel, principally salaries and related personnel expenses, are paid in NIS, whereas most of our revenues are generated in U.S. dollars. When the dollar is weak, our foreign currency denominated expenses will be higher, whereas if the dollar is strong, our foreign currency denominated expenses will be lower. If the NIS strengthens against the U.S. dollar (as happened in 2017), the dollar value of our Israeli expenses will increase and may have a material adverse effect on our business, operating results and financial condition;

- A portion of our international sales are denominated in currencies other than U.S. dollars, such as Euro, Chinese Yuan and Australian Dollar, thereby exposing us to currency fluctuations in such international sales transactions;
- We incur expenses in several other currencies in connection with our operations in Europe and Asia. Devaluation of the U.S. dollar relative to such local currencies causes our operational expenses to increase; and
- The majority of our international sales are denominated in U.S. dollars. Accordingly, devaluation in the local currencies of our customers relative to the U.S. dollar could cause our customers to decrease orders or default on payment.

We generally do not engage in hedging or other transactions intended to manage risks relating to foreign currency exchange rate fluctuations. Consequently, we are exposed to risks related to changes in currency exchange rates and fluctuations of exchange rates, any of which could result in a material adverse effect on our business, financial condition and results of operations. Even if we enter into hedging transactions in the future, they may not effectively protect us from currency exchange rate risks. For a further discussion of the impact on currency exchange rates on our business, see “Item 11. Quantitative and Qualitative Disclosures About Market Risk.”

Undetected defects and errors may increase our costs and impair the market acceptance of our products.

Our products have occasionally contained, and may in the future contain, undetected defects or errors, especially when first introduced or when new versions are released, due to defects or errors that we fail to detect, including in components supplied to us by third parties. These defects or errors may be found after the commencement of commercial shipments. In addition, because our customers integrate our products into their networks with products from other vendors, it may be difficult to identify the product that has caused the problem in the network. Regardless of the source of these defects or errors, we will then need to divert the attention of our engineering personnel from our product development efforts to address the detection and correction of these errors and defects. In the past, we have not incurred significant warranty or repair costs, nor have we been subject to liability claims for material damages related to product errors or defects, nor have we experienced any material lags or delays as a result thereof. However, we cannot assure you that we will not incur these costs or liabilities or experience these lags or delays in the future. Any insurance coverage that we maintain may not provide sufficient protection should a claim be asserted. Moreover, the occurrence of errors and defects, whether caused by our products or the components supplied by another vendor, may result in significant customer relations problems and injure our reputation, thereby impairing the market acceptance of our products.

A shortage of components or manufacturing capacity could cause a delay in our ability to fulfill orders or increase our manufacturing costs.

Our ability to meet customer demands depends in part on our ability to obtain timely deliveries of parts from our suppliers and contract manufacturers. We cannot assure you that we will not encounter supply and fulfillment issues in the future. Although in many cases we use standard parts and components for our products, certain components are presently available to us only from limited sources (see the risk factor below and the discussion under "Business Overview - Manufacturing and Suppliers"). We may not be able to diversify sources in a timely manner, which could harm our ability to deliver products to customers and seriously impact present and future sales.

We may experience a shortage of certain component parts as a result of our own manufacturing issues, manufacturing issues at our suppliers or contract manufacturers, capacity problems experienced by our suppliers or contract manufacturers, or strong demand in the industry for those parts, especially if there is growth in the overall economy. If there is growth in the economy, such growth is likely to create greater pressures on us and our suppliers to accurately project overall component demand and component demands within specific product categories and to establish optimal component levels. If shortages or delays persist, the price of these components may increase, or the components may not be available at all.

We may also encounter shortages if we do not accurately anticipate our needs. We may not be able to secure enough components at reasonable prices or of acceptable quality to build new products in a timely manner in the quantities or configurations needed. Accordingly, our revenues and gross margins could be materially and adversely affected until other sources can be developed.

In addition, our operating results could be materially and adversely affected if we anticipate greater demand than actually develops and we commit to the purchase more components than we actually require. We see this specifically with respect to dated components, which we need to order in large quantities due to manufacturing stoppage. Due to technology advancement, we are required from time-to-time to make “last buy” type of stock purchase of such dated components for our legacy products.

Any disruption in our supply chain could result in a material adverse effect on our business, financial condition and results of operations.

We rely on few vendors to provide our hardware platforms and components for our main accessories. If such vendors are not able to provide us with adequate supplies of these components and platforms on a timely basis and on acceptable terms, our business, financial condition and results of operations could be harmed.

We primarily rely on a few original design manufacturers, or ODMs, for the manufacture and supply of our hardware platforms, with approximately 80% of our direct product costs are from these vendors. In addition, we purchase components for our main accessories from such vendors, whereby we purchase approximately 13% of such accessories from these vendors. If we are unable to continue to acquire from these ODMs and/or components vendors on acceptable terms, or should any of these ODMs and/or components vendors cease to supply us with such platforms or components for any reason, we may not be able to identify and integrate an alternative source of supply in a timely fashion or at the same costs. Any transition to one or more alternate manufacturers would likely result in delays, operational problems and increased costs, and may limit our ability to deliver our products to our customers on time for such transition period, any of which could result in a material adverse effect on our business, financial condition and results of operations.

Our business and operating results could suffer if third parties infringe upon our proprietary technology.

Our success depends, in part, upon the protection of our proprietary software installed in our products, our trade secrets and our trademarks. We seek to protect our intellectual property rights through a combination of trademark and patent law, trade secret protection, confidentiality agreements and other contractual arrangements with our employees, affiliates, distributors and others. In the United States and several other countries, we have registered or acquired trademarks. In addition, we have registered patents in the U.S. and have pending patent applications and provisional patents in connection with several of our products' features.

The protective steps we have taken may be inadequate to deter infringement upon our intellectual property rights or misappropriation of our proprietary information. We may be unable to detect the unauthorized use of our proprietary technology or take appropriate steps to enforce our intellectual property rights. Effective trademark, patent and trade secret protection may not be available in every country in which we offer, or intend to offer, our products. Failure to adequately protect our intellectual property rights could devalue our proprietary content, impair our ability to compete effectively and eventually harm our operating results. Furthermore, defending our intellectual property rights, either by way of initiating intellectual property litigation or defending such, could result in the expenditure of significant financial and managerial resources. For example, in 2015, 2016 and 2017, intellectual property litigation costs amounted to \$3.4 million, \$4.3 million and \$2.1 million, respectively, and continues in 2018 (see "Item 8. Financial Information – Legal Proceedings"). Moreover, the outcome of such proceedings, if such outcome is negative, could result in devaluation of our proprietary technology and cause an additional significant financial impact which may harm our operating results.

Our products may infringe on the intellectual property rights of others.

Third parties may assert claims that we have violated a patent, trademark, copyright or other proprietary intellectual property right belonging to them. As is characteristic of our industry, there can be no assurance that our products do not or will not infringe the proprietary rights of third parties, that third parties will not claim infringement by us with respect to patents or other proprietary rights or that we would prevail in any such proceedings. We have received in the past, and may receive in the future, communications asserting that the technology used in some of our products requires third-party licenses. Any infringement claims, whether or not meritorious, could result in significant costly litigation or arbitration and divert the attention of technical and management personnel. For example, see the discussion in "Item 8. Financial Information – Legal Proceedings". Any adverse outcome in litigation alleging infringement could require us to develop non-infringing technology or enter into royalty or licensing agreements. If, in such situations, we are unable to obtain licenses on acceptable terms, we may be prevented from manufacturing or selling products that infringe such intellectual property of a third party. An unfavorable outcome or settlement regarding one or more of these matters could have a material adverse effect on our business and operating results.

If our products fail to protect against malicious attacks and our end-users experience security breaches, our reputation and business could be harmed, and our operating results could be adversely impacted.

Defects may cause our products to be vulnerable to security attacks or cause them to fail to help secure networks. Data thieves are increasingly sophisticated, often affiliated with organized crime and operate large-scale and complex automated attacks. In addition, the techniques they use to access or sabotage networks change frequently and generally are not recognized until launched against a target. As a result, our products may be unable to anticipate these techniques and provide a solution in time to protect our end- users' networks. If we fail to identify and respond to new and increasingly complex methods of attack and to update our products to detect or prevent such threats in time to protect our end- users' critical business data, the integrity of our products and reputation as well as our business and operating results could suffer.

In addition, an actual or perceived security breach or theft of sensitive data of one of our end-users, regardless of whether the breach is attributable to the failure of our products or services, could adversely affect the market's perception of our security products. There is no guarantee that our products will be free of flaws or vulnerabilities. Our end- users may also misuse our products, which could result in a breach or theft of business data.

As a security provider, if our internal network system is subject to intentional disruption by cyber attackers or other data thieves, it could, among other things, harm the integrity of our products and the public perception of our products and services and consequently adversely impact our future sales.

We will not succeed with our application and network security solutions unless the marketplace is confident that we provide effective IT security protection. We provide security products, and as a result we could be an attractive target of cyber-attacks (including, among others, malware, viruses and attachments to e-mails, and other disruptive activities of individuals or groups) designed to impede the performance of our solutions, penetrate our network security or the security of our cloud platform or our internal systems, misappropriate proprietary information and/or cause other interruptions to our services. Although we have not identified any act of sabotage or unauthorized access by a third party of our network systems, if we experience an actual or perceived breach of security in our internal systems, it could adversely affect the integrity and market perception of our products and services. Furthermore, the costs to eliminate or address security threats and vulnerabilities before or after a cyber-security incident could be significant. Our remediation efforts may not be successful and could result in interruptions, delays, or cessation of service and loss of existing or potential customers. In addition, any such security breach could impair our ability to operate our business, including our ability to provide maintenance and support services to our customers. If this happens, our revenues could decline and our reputation and business could suffer.

We rely on information systems to conduct our businesses, and failure to protect these systems against security breaches and otherwise to implement, integrate, upgrade and maintain such systems in working order could have a material adverse effect on our results of operations, cash flows or financial condition.

The efficient operation of our businesses depends on our computer hardware and software systems. For instance, we rely on information systems to process customer orders, manage accounts receivable collections, manage accounts payable processes, track costs and operations, maintain client relationships and accumulate financial results. Despite our implementation of industry-accepted security measures and technology, our information systems are vulnerable to and have been in the past subject to computer viruses, attempts to insert malicious codes, unauthorized access, phishing efforts, denial-of-service attacks and other cyber attacks and we expect to be subject to similar attacks in the future as such attacks become more sophisticated and frequent. A breach of our information systems could result in decreased performance, operational difficulties and increased costs, any of which could have a material adverse effect on our business and operating results.

Our non-competition agreements with our employees may not be enforceable. If any of these employees leave us and join a competitor, our competitor could benefit from the expertise our former employees gained while working for us.

We currently have non-competition agreements with most of our employees. These agreements prohibit our employees, in the event they cease working for us, from directly competing with us or working for some of our competitors for a limited period after termination of employment. The laws of the United States, Israel and most other countries in which we have employees may limit or prohibit our ability to enforce these non-competition agreements or may allow us to enforce them only to a limited extent. In the event that we are unable to enforce any of these agreements, competitors that employ our former employees could benefit from the expertise our former employees gained while working for us.

We may be required to pay additional taxes due to tax positions that we undertook. Additional tax liabilities could materially adversely affect our results of operations and financial condition.

We operate our business in various countries, and we attempt to utilize an efficient operating model to optimize our tax payments based on the laws in the countries in which we operate. This can cause disputes between us and various tax authorities in the countries in which we operate, whether due to tax positions that we have taken in various tax returns we have filed or due to determinations we have made not to file tax returns in certain jurisdictions. In particular, not all of our tax returns are final and may be subject to further audit and assessment by applicable tax authorities. There can be no assurance that the applicable tax authorities will accept our tax positions, and if they do not, we may be required to pay additional taxes, as a result of which, our future results may be adversely affected. In the past few years, certain tax authorities which have audited our tax returns have rejected our tax positions and, while we intend to vigorously maintain our positions, we cannot be sure that our positions will be accepted and we may end up paying additional taxes, whether as a result of litigation, if ensued, or settlement negotiations.

In recent years, we have seen changes in tax laws resulting in an increase in applicable tax rates, especially increased liabilities of corporations and limitations on the ability to benefit from strategic tax planning, with these laws particularly focused on international corporations. Such legislative changes in one or more jurisdictions in which we operate may have implications on our tax liability and have a material adverse effect on our results of operations and financial condition. For example, the Organization for Economic Cooperation and Development, or the OECD, an intergovernmental organization with 35 member countries that aims to promote the economic and social well-being of people around the world, has recently introduced the base erosion and profit shifting ("BEPS") project. The BEPS project contemplates changes to numerous international tax principles, as well as national tax incentives, and these changes, if adopted by individual countries, could adversely affect our provision for income taxes. Countries have only recently begun to translate the BEPS recommendations into specific national tax laws, and it remains difficult to predict with accuracy the magnitude of any impact that such new rules may have on our financial results. The U.S. and Israel, among other countries in which we have operations, are members of the OECD.

The adoption of the recent tax reform and the enactment of additional legislation changing the United States taxation of international business activities could materially impact our financial position and results of operations.

On December 22, 2017, President Trump signed into law what is known as the "Tax Cuts and Jobs Act" (the "TCJA") that significantly reforms the Internal Revenue Code of 1986, as amended (the "Code"). The TCJA, among other things, includes changes to U.S. federal corporate and individual income tax rates. The TCJA makes significant changes to the U.S. tax law which may affect our operations and the impact of these provisions on our operations and our investors is still uncertain and may not become evident for some period of time. The application and implementation of the new provisions may require us to apply the provisions without clear guidance from the U.S. Treasury Department or the Internal Revenue Service ("IRS"). The U.S. Treasury Department and the IRS could interpret or issue guidance on how provisions of the TCJA will be applied or otherwise administered that is different from our interpretation. As part of our compliance with the changes pursuant to the TCJA, we may make adjustments to our current provision for income taxes and other items impacted by the TCJA.

In addition, due to the expansion of our international business activities, any changes in the U.S. taxation of such activities may increase our worldwide effective tax rate and adversely affect our financial position and results of operations. Further, other foreign governments may enact tax laws in response to the TCJA that could result in further changes to global taxation and materially affect our financial position and results of operations. The impact of the TCJA on holders of our securities is uncertain. We therefore recommend our stockholders to consult with their legal and tax advisors with respect to such legislation and the potential tax consequences.

Our bank deposits and investments in Israel are not insured, and our bank deposits in the United States are in excess of insured limits.

The majority of our cash and cash equivalents, and short-term and long-term bank deposits are invested in banks in Israel and, to a smaller extent, in banks in the United States. The Israeli bank deposits are not insured, while the deposits made in the United States are in excess of insured limits and are not otherwise insured. If one or more of these financial institutions were to become insolvent, the loss of these investments would have a material adverse effect on our financial condition.

If we are unable to realize our investment objectives, our financial condition and results of operations may be adversely affected.

We maintain substantial balances of cash and liquid investments, for purposes of acquisitions and general corporate purposes. Our cash, cash equivalents, short-term and long-term bank deposits and marketable securities totaled $344.3 million as of December 31, 2017. The performance of the capital markets affects the values of funds that are held in marketable securities. These assets are subject to market fluctuations and various developments, including, without limitation, rating agency downgrades that may impair their value. We expect that market conditions will continue to fluctuate and that the fair value of our investments may be affected accordingly.

Financial income is a component of our net income (loss). As of December 31, 2017, our investment portfolio, including cash and cash equivalents, deposits and marketable securities, had a carrying value of $344.3 million, compared with $320.1 million as of December 31, 2016. For the years ended December 31, 2017, 2016 and 2015, we had $4.8 million, $5.7 million and $ 5.9 million, respectively, of financial income.

The outlook for our financial income is dependent, in part, on the future direction of interest rates, exchange rates, the amount of any share repurchases or acquisitions that we make and the amount of cash flows from operations that are available for investment. The performance of the capital markets affects the values of our funds that are held in marketable securities. These assets are subject to market fluctuations and will yield uncertain returns. Due to certain market developments, including investments' rating downgrades, the fair value of these investments may decline. If market conditions continue to fluctuate, the fair value of our investments may be impacted accordingly. Although our investment guidelines stress diversification and capital preservation, our investments are subject to a variety of risks, including risks related to general economic conditions, interest rate fluctuations and market volatility.

In particular, our investment portfolios include a significant amount of interest rate-sensitive instruments, such as bonds, which, in addition to the inherent risk associated with the debt, may be adversely affected by changes in interest rates. Changes in interest rates and credit quality may also result in fluctuations in the income derived from, or the valuation of, our fixed income securities. Interest rates are highly sensitive to many factors, including governmental monetary policies, domestic and international economic and political conditions and other factors beyond our control. For example, benchmark interest rates, such as the U.S. Federal Funds Rate, are currently relatively low, which is likely to significantly impact our investment income. Increases in interest rates will decrease the value of our investments in fixed-income securities. If increases in interest rates occur during periods when we sell investments to satisfy liquidity needs, we may experience investment losses. Conversely, if interest rates decline, reinvested funds will earn less than expected.

In terms of credit risk, our investment portfolio policy is "buy and hold", while minimizing credit risk by setting maximum concentration limit per issuer and credit rating. Our investments consist primarily of government and corporate debentures and bank deposits. Although we believe that we generally adhere to conservative investment guidelines, if turmoil in the financial markets reoccurs in the future, it may result in impairments of the carrying value of our investment assets since we classify our investments in marketable securities as available-for-sale. Changes in the fair value of investments classified as available-for-sale are not recognized as income during the period, but rather are recognized as a separate component of equity until realized. Realized losses in our investments portfolio may adversely affect our financial position and results. For example, if we had reported all the changes in the fair values of our investments into income, our reported net loss would have increased by $0.4 million and $ 1.3 million during the years ended December 31, 2017 and 2016, respectively, and our reported net income would have increased by $1.0 million during the year ended December 31, 2015. Any significant decline in our financial income or the value of our investments as a result of continued low interest rates, deterioration in the credit worthiness of the securities in which we have invested, general market conditions or other factors, could have an adverse effect on our results of operations and financial condition.

Our success depends on our ability to attract, train and retain highly qualified research and development, sales, technical, customer support, operations and information technology personnel.

We may need to increase our research and development, sales and marketing, technical, support, operations and information technology staff. Our products require a sophisticated technology, marketing and sales effort targeted at several levels within a prospective customer’s organization. Accordingly, we need highly-trained research and development, sales, marketing, technical, customer support, operations and information technology personnel. Competition for such qualified personnel is intense. Consequently, we may not be able to hire or retain sufficient personnel to support our business operations, which could result in a material adverse effect on our business, financial condition and results of operations.

Risks Related to the Market for Our Ordinary Shares

Yehuda Zisapel, our chairman of the board, Nava Zisapel, and Roy Zisapel, our President, Chief Executive Officer and director, may exert significant influence in the election of our directors and over the outcome of other matters requiring shareholder approval.

As of March 25, 2018, Yehuda Zisapel, the Chairman of our Board of Directors, beneficially owned approximately 5.4% of our outstanding ordinary shares; Nava Zisapel, beneficially owned approximately 6.4% of our outstanding ordinary shares; and their son, Roy Zisapel, our President, Chief Executive Officer and director, beneficially owned approximately 5.5% of our outstanding ordinary shares (see “Item 6E – Directors, Senior Management and Employees - Share Ownership”). As a result, if these shareholders act together, they could exert significant influence on the election of our directors and on decisions by our shareholders on matters submitted to shareholder vote, including mergers, consolidations and the sale of all or substantially all of our assets. This concentration of ownership of our ordinary shares could delay or prevent proxy contests, mergers, tender offers, or other purchases of our ordinary shares that might otherwise give our shareholders the opportunity to realize a premium over the then-prevailing market price for our ordinary shares. This concentration of ownership may also adversely affect our share price.

If we are characterized as a passive foreign investment company, our U.S. shareholders may suffer adverse tax consequences.

Generally, if for any taxable year, after applying certain "look through" tax rules, (i) 75% or more of our gross income is passive income, or (ii) at least 50% of the fair market value of our assets, averaged quarterly over our taxable year, are held for the production of, or produce, passive income, we would be characterized as a passive foreign investment company, or PFIC, for U.S. federal income tax purposes. If we are classified as a PFIC, our U.S. shareholders could suffer adverse U.S. tax consequences, including having gain realized on the sale of our ordinary shares treated as ordinary income, as opposed to capital gain income, and having potentially punitive interest charges apply to such gain. Similar rules apply to certain "excess distributions" made with respect to our ordinary shares.

For our 2017 taxable year, we do not believe that we should be classified as a PFIC. There can be no assurance, however, that the IRS will not challenge this treatment, and it is possible that the IRS could attempt to treat us as a PFIC for 2017 and prior taxable years. The tests for determining PFIC status are applied annually, and it is difficult to make accurate predictions of our future income, assets and market capitalization, including the future price of our ordinary shares, all of which are relevant to the PFIC determination. Accordingly, there can be no assurance that we will not become a PFIC in future taxable years. U.S. shareholders should consult with their own U.S. tax advisors with respect to the U.S. tax consequences of investing in our ordinary shares. For a more detailed discussion of the rules relating to PFICs and related tax consequences, please see the section of this annual report entitled "Item 10 – Additional Information – Taxation — United States Federal Income Tax Considerations."

Provisions of our Articles of Association and Israeli law as well as the terms of our equity incentive plan could delay, prevent or make a change of control of us more difficult or costly, which could depress the price of our ordinary shares.

The provisions in our Articles of Association that provide that our directors, other than our external directors, are elected in three staggered classes by a majority vote of our shareholders may have the effect of delaying or making an unsolicited acquisition of our Company more difficult. Israeli corporate and tax laws, including the ability of our Board of Directors to adopt a shareholder rights plan without further shareholder approval, may also have the effect of delaying, preventing or making an acquisition of us more difficult. For example, under the Companies Law, upon the request of a creditor of either party to a proposed merger, an Israeli court may delay or prevent the merger if it concludes that there is a reasonable concern that, as a result of the merger, the surviving company will be unable to satisfy the obligations of any of the parties to the merger. In addition, our Key Employee Share Incentive Plan (1997), as amended, or the Share Incentive Plan, provides that in the event of a "Hostile Takeover" (which is defined to include, among others, an unsolicited acquisition of more than 20% of our outstanding shares), the vesting of all or a portion of our outstanding equity awards, including stock options, will accelerate, unless otherwise determined by our Board of Directors (or a committee thereof). As a result, an acquisition of our Company that triggers the said acceleration will be more costly to a potential acquirer. These provisions could cause our ordinary shares to trade at prices below the price for which third parties might be willing to pay to gain control over us. Third parties who are otherwise willing to pay a premium over prevailing market prices to gain control of us may be unwilling to do so because of these provisions. For additional information on this topic, see "Item 6C – Board Practices – Staggered Board," "Item 6E – Directors Senior Management and Employees – Share Ownership - Key Employee Share Incentive Plan" and "Item 10B – Additional Information – Memorandum and Articles of Association – Mergers and Acquisitions under Israeli Law."

Compliance with the disclosure rules regarding the use of conflict minerals may affect our relationships with suppliers and customers.

Pursuant to Section 1502 of the Dodd-Frank Act, United States publicly-traded companies, such as Radware, are required to disclose use or potential use of "conflict minerals" that are mined from the Democratic Republic of Congo or adjoining countries (collectively, "Covered Countries"). Conflict minerals are defined by the SEC as columbite-tantalite (coltan), cassiterite, gold, wolframite, or their derivatives, which are limited to tantalum, tin, and tungsten ("conflict minerals" or "3TG"). These requirements necessitate due diligence efforts to assess whether such minerals are used in our products in order to make the relevant required annual disclosures. These requirements, which were recently implemented, could adversely affect the sourcing, supply and pricing of materials used in our products.

We have conducted an analysis of our products and found that small quantities of 3TG could potentially be found in our products. The products that we manufacture are highly complex, typically containing thousands of parts from many direct suppliers. In general, we primarily rely on third-party assembly and manufacturing vendors to provide our finished products and, in this respect, these vendors typically receive components and subassemblies included in our products from other suppliers and subcontractors. We have relationships with a vast network of suppliers throughout the world and there are generally multiple tiers between the 3TG mines and our direct suppliers. Therefore, we must rely on our direct suppliers to cooperate with us and work with their own upstream suppliers or sub-contractors in order that they may provide us with accurate information about the origin of 3TG in the components we purchase from them. In particular, many of our supplier contracts have fixed durations and we cannot unilaterally impose new contract terms or flow-down requirements that would otherwise compel these suppliers to support our due diligence efforts with respect to 3TG content. Currently, we do not have sufficient information from our suppliers to determine the country of origin of the conflict minerals used in our products or the facilities used to process those conflict minerals. Therefore, we cannot exclude the possibility that some of these conflict minerals may have originated in Covered Countries and are not from recycled or scrap sources.

We may face reputational challenges that could impact future sales (1) based on the fact that we are unable to verify with sufficient accuracy the origins of all conflict minerals used in our products, or (2) if we later determine that certain of our products contain minerals not determined to be conflict free.

Additionally, there are, and will be, ongoing costs associated with complying with these disclosure requirements pursuant to Section 1502 of the Dodd-Frank Act, including due diligence to determine the sources of those minerals that may be used or necessary to the production of our products in order to make the relevant required annual disclosures.

Our share price has decreased significantly in the past and could continue to fluctuate and further decrease in the future.

The market price for our ordinary shares, as well as the prices of shares of other technology companies, has been volatile. For example, during 2017 the lowest closing price of our share was $14.38, compared to the highest closing price of our share of $20.48 during the same year (see also “Item 9A. Offer and Listing Details”). Numerous factors, many of which are beyond our control, may cause the market price of our ordinary shares to fluctuate significantly and further decrease, including:

- fluctuations in our quarterly revenues and earnings and those of our publicly-traded competitors;
- shortfalls in our operating results from levels forecast by securities analysts;
- announcements concerning us or our competitors;
- the introduction of new products and new industry standards;
- changes in pricing policies by us or our competitors;
- general market conditions and changes in market conditions in our industry;
- the general state of the securities market (particularly the technology sector); and
- political, economic and other developments in the State of Israel, the U.S. and worldwide.

Risks Related to Operations in Israel

Security and political and economic instability in the Middle East may harm our business.

We are incorporated under Israeli law and our principal offices and manufacturing and research and development facilities are located in Israel. Accordingly, our operations and financial results could be adversely affected if political, economic and military events curtailed or interrupted trade between Israel and its present trading partners or if major hostilities involving Israel should occur in the Middle East.

Since the establishment of the State of Israel in 1948, a number of armed conflicts have taken place between Israel and its Arab neighbors. A state of hostility, varying in degree and intensity, has led to security and economic problems for Israel. Since late 2000, there has also been a high level of violence between Israel and the Palestinians including during the summer of 2014, when Israel was engaged in armed conflicts with Hamas, a militia group and political party operating in the Gaza Strip. This violence has strained Israel's relationship with its Arab citizens, Arab countries and, to some extent, with other countries around the world. Since the end of 2010 several countries in the region have been experiencing increased political instability, which led to changes in government in some of these countries and the war in Syria, the effects of which are currently difficult to assess. In addition, Israel faces threats from more distant neighbors, such as Iran (which is believed to be an ally of Hamas in Gaza and Hezbollah in Lebanon) and the militant group known as the Islamic State of Iraq and Syria. This situation may potentially escalate in the future. In addition, this instability in the region may affect the global economy and marketplace. We do not believe that the political and security situation has had a material impact on our business to date; however, there can be no assurance that this will be the case for future operations. We could be adversely affected by any major hostilities, including acts of terrorism as well as cyber-attacks or any other hostilities involving or threatening Israel, the interruption or curtailment of trade between Israel and its trading partners, a significant downturn in the economic or financial condition of Israel or a significant increase in the rate of inflation. Furthermore, some neighboring countries, as well as certain companies, organizations and movements, continue to participate in a boycott of Israeli firms and others doing business with Israel or with Israeli companies as the result of the aforementioned hostilities. No predictions can be made as to whether or when a final resolution of the area's problems will be achieved or the nature thereof and to what extent the situation will impact Israel's economic development or our operations.

Some of our directors and officers as well as many of our Israeli employees are obligated to perform annual military reserve duty in Israel. We cannot assess the potential impact of these obligations on our business.

Some of our directors, officers and employees are, unless exempt, obligated to perform annual military reserve duty, depending upon their age and prior position in the army. They may also be subject to being called to active duty at any time under emergency circumstances. Our operations could be disrupted by the absence, for a significant period, of one of more of these officers or other key employees due to military service, and any disruption in our operations could harm our business. The full impact on our workforce or business if some of our officers and employees will be called upon to perform military service, especially in times of national emergency, is difficult to predict.

The exchange rate between the New Israeli Shekel against the U.S. dollar is volatile, and may negatively impact our profitability.

Most of our revenues worldwide are denominated in U.S. dollars or are dollar-linked, whereas a portion of our revenues is denominated in other currencies, including NIS. At the same time, a substantial portion of our expenses is incurred in U.S. dollars, but we incur a portion of our expenses, principally salaries and related personnel expenses, in other currencies, mainly in Israel - in NIS, in Europe - in Euros and in Asia-Pacific - in several local currencies. If the NIS increases in value relative to the dollar, as was the case in 2017, the dollar cost of our operations in Israel will increase and our dollar-measured results of operations will be adversely affected. We cannot provide assurances that we will not be materially adversely affected by exchange rate fluctuations in the future. See also "Currency exchange rates and fluctuations of exchange rates could have a material adverse effect on our results of operations" above in this section.

The tax benefits we may receive in connection with our approved enterprise, privileged or preferred enterprise programs require us to satisfy prescribed conditions and may be terminated or reduced in the future. This would increase taxes and decrease our net profit.

We have in the past benefited, and currently benefit from certain government programs and tax benefits in Israel. To remain eligible to obtain such tax benefits, we must continue to meet certain conditions. If we fail to comply with these conditions in the future, the benefits we receive could be canceled and we may have to pay certain taxes. We cannot guarantee that these programs and tax benefits will be continued in the future, at their current levels or at all. If these programs and tax benefits are ended, our tax expenses and the resulting effective tax rate reflected in our financial statements may increase and as such our business, financial condition and results of operations could be materially and adversely affected.

In the event of distribution of dividends from tax-exempt income or in conducting certain transactions that may be viewed by the Israeli tax authorities as a deemed dividend event, the amount distributed will be subject to corporate tax at the rate ordinarily applicable to the approved/privileged enterprise's income. Tax-exempt income generated under the approved/privileged enterprise program will be subject to taxes upon dividend distribution (which includes the repurchase of the Company's shares) or liquidation.

It may be difficult to enforce a U.S. judgment against us or our officers and directors and to assert U.S. securities laws claims in Israel.

We are incorporated under the laws of the State of Israel. Service of process upon us, our Israeli subsidiary, our directors and officers and the Israeli experts, if any, named in this annual report, substantially all of whom reside outside the United States, may be difficult to obtain within the United States. Furthermore, because the majority of our assets and investments, and substantially all of our directors, officers and such Israeli experts are located outside the United States, any judgment obtained in the United States against us or any of them may be difficult to collect within the United States.

We have been informed by our legal counsel in Israel that it may also be difficult to assert U.S. securities law claims in original actions instituted in Israel. Israeli courts may refuse to hear a claim based on an alleged violation of U.S. securities laws reasoning that Israel is not the most appropriate forum to bring such a claim. In addition, even if an Israeli court agrees to hear a claim, it may determine that Israeli law and not U.S. law is applicable to the claim. There is little binding case law in Israel addressing these matters. If U.S. law is found to be applicable, the content of applicable U.S. law must be proved as a fact, which can be a time-consuming and costly process. Certain matters of procedure will also be governed by Israeli law.

Subject to specified time limitations and legal procedures, under the rules of private international law currently prevailing in Israel, Israeli courts may enforce a U.S. judgment in a civil matter, including a judgment based upon the civil liability provisions of the U.S. securities laws as well as a monetary or compensatory judgment in a non-civil matter, provided that the following key conditions are met:

· subject to limited exceptions, the judgment is final and non-appealable;

- the judgment was given by a court competent under the laws of the state of the court and is otherwise enforceable in such state;
- the judgment was rendered by a court competent under the rules of private international law applicable in Israel;
- the laws of the state in which the judgment was given provide for the enforcement of judgments of Israeli courts;
- adequate service of process has been effected and the defendant has had a reasonable opportunity to present his arguments and evidence;
- the judgment and its enforcement are not contrary to the law, public policy, security or sovereignty of the State of Israel;
- the judgment was not obtained by fraud and does not conflict with any other valid judgment in the same matter between the same parties; and
- an action between the same parties in the same matter was not pending in any Israeli court at the time the lawsuit was instituted in the U.S. court.

We have obtained benefits from the Israeli Innovation Authority, which subjects us to ongoing restrictions. In addition, these benefits may not continue or in the future may be limited or restricted.

In 2016 and 2017, we received grants from the Israeli Innovation Authority (formerly known as the Office of the Chief Scientist of the Israeli Ministry of Economy), or the IIA. We have also received such grants in the past few years and may in the future apply for, non-royalty-bearing grants for research and development programs that meet specified criteria pursuant to the Law for the Encouragement of Research, Development and Technological Innovation, 1984, and the regulations promulgated thereunder, or the R&D Law. The terms of the IIA grants limit our ability to manufacture products or transfer technologies outside of Israel if such products or technologies were developed using know-how developed with or based upon IIA grants. In addition, any non-Israeli who, among other things, becomes an "interested party" in Radware (e.g., becomes a holder of 5% or more of our share capital or voting rights), is generally required to undertake to observe the law governing the grant programs of the IIA, some of the principal restrictions and penalties of which are the transferability limits described above and elsewhere in this annual report.

Further, the IIA grants may be terminated in the future or the available benefits may be reduced or impacted, including, among other possible circumstances, should we transfer certain research and development and/or manufacturing activities outside the State of Israel. The termination or curtailment of these programs or the loss or reduction of such benefits could have a material adverse effect on our business, financial condition and results of operations. In addition, the IIA may establish new guidelines regarding the R&D Law, which may affect our existing and/or future IIA programs and incentives for which we may be eligible. We cannot predict what changes, if any, the IIA may make.

ITEM 4. INFORMATION ON THE COMPANY

A. History and Development of the Company

Radware Ltd. was organized in May 1996 as a corporation under the laws of the State of Israel and commenced operations in 1997. Our principal executive offices are located at 22 Raoul Wallenberg Street, Tel-Aviv 6971917, Israel and our telephone number is 972-3-766-8666. Our website address is www.radware.com (information contained on our website is not incorporated herein by reference and shall not constitute part of this annual report).

As of September 1, 1998, we established Radware, Inc., a wholly-owned subsidiary in the United States, which conducts the sales and marketing of our products in the Americas and is our authorized representative and agent in the United States. The principal offices of Radware Inc. are located at 575 Corporate Dr., Lobby 2, Mahwah, NJ 07430 and its telephone number is 201-512-9771. We also have several wholly-owned subsidiaries world-wide handling local support and promotion activities.

In September 1999, we conducted the initial public offering of our ordinary shares and our ordinary shares commenced trading on the Nasdaq.

In December 2005, we acquired the business of V-Secure Technologies, a U.S.-based provider of behavior-based network intrusion prevention solutions. In April 2007, we acquired Covelight, a U.S.-based provider of web channel intelligence technology. In March 2009, we acquired from Nortel certain assets and liabilities related to Nortel's Layer 4-7 Application Delivery Business (Alteon). In May 2011, we established Radyoos Media Ltd., or Radyoos, our majority owned subsidiary, which was engaged in developing and operating a web-based e-commerce platform. In February 2013, we acquired Strangeloop, a Canadian-based provider of web performance acceleration solutions. In January 2017, we acquired Seculert, a company engaged in cyber-attack detection and HTTP analytics solutions and developing user and entity behavioral analysis "UEBA" solutions.

Recent Major Business Developments

Below is a summary of the major business developments in Radware since January 1, 2017:

- On September 19, 2017, we announced that we introduced a comprehensive solution for protection from network layer attacks, including increased threats stemming from Internet-of-Things (IoT) botnets.
- On June 7, 2017, we announced the new Alteon D-line of appliances and software, which was designed to address evolving market challenges around the increase in encrypted traffic.
- On January 31, 2017, we announced the acquisition of Seculert, a company engaged in cyber-attack detection and HTTP analytics solutions and developing user and entity behavioral analysis "UEBA" solutions.

For a discussion of our capital expenditures and divestitures, see “Item 5B—Operating and Financial Review and Prospects – Liquidity and Capital Resources.”

B. Business Overview

(a) Overview

We are a provider of cyber security and application delivery solutions that help our customers to secure the digital experience for users of business-critical applications in virtual, cloud and software defined data centers. Our solutions are deployed by, among others, enterprises, carriers and cloud service providers.

We offer a set of solutions that are designed to ensure application service levels are guaranteed at all times, in any operational scenario, and to optimize business operations, minimize service delivery degradation and prevent downtime.

Our solutions are offered in three main categories including products, product subscriptions and services.

(b) The Market Opportunity

General Market Overview - Cyber Security and Application Delivery

According to Frost & Sullivan, a market research firm, in their “DDoS Mitigation Global Market Analysis, Forecast to 2021” report, the total DDoS Mitigation market is estimated at nearly $1 billion in 2017 and expected to grow to $1.8 billion by 2021, representing a compound annual growth rate of 17.1%. According to Frost & Sullivan, in their “Global Web Application Firewall (WAF) Market Analysis, Forecast to 2021”, the total WAF market is estimated at approximately $700 million in 2017 and expected to grow to $1.15 billion by 2021, representing a compound annual growth rate of 13.1%.

At the same time, enterprises are moving their applications to the cloud in order to achieve flexibility, reduce capital expenses and service simplicity. This trend is reflected in the growth of both cloud applications markets and cloud security markets. Frost & Sullivan, in their aforementioned reports, estimates the cloud DDoS Protection and Cloud WAF markets to be at approximately $840 million in 2017 and expected to grow to $1.2 billion by 2021, representing a compound annual growth rate of 22.8%.

The application delivery controllers market is estimated by Gartner, in its “Forecast: Enterprise Network Equipment by Market Segment, Worldwide, 2014-2021, 3Q17 Update” report, at $2.5 billion in 2017 and expected to decrease to $2.3 billion by 2021, representing a compound annual decline rate of (2.2%). While this overall market shows mild negative slow down, according to the aforesaid Gartner report, the virtual ADC segment is expected to show a compound annual growth at a rate of 8.1% and the virtual ADC leases for MSPs is expected to show a compound annual growth rate of 12.7%.

The following sections provide more detailed information about the trends in the key markets Radware is selling to.

Market Overview –

DDoS Protection

General

We believe that in today's environment, organizations are challenged by an evolving threat of cyber-attacks that, if materialized, could reduce revenues, increase expenses and damage reputation of organizations and other users. In particular, today’s cyber-attackers use sophisticated methods, often equipped with multiple attack-vectors in the same attack campaign, aimed at shutting down or otherwise impairing the operation of datacenters and organizations’ web presence. At the same time, we believe that the simplicity of launching such cyber-attacks and variety of attack tools available are the primary reasons that more organizations are suffering from increased attacks, such as DDoS.

The DDoS protection market has significantly evolved in the past years with multiple solutions designed to defend against the DDoS threat, starting from hardware and software on-premises solutions, in-the-cloud scrubbing centers, DDoS protection managed providers and Internet service providers, or ISPs, who offer value-add DDoS protection services.

Industry Trends

As DDoS attack characteristics become more complex, organizations are increasingly adopting "hybrid" DDoS mitigation strategies consisting of on-premises appliances for manageable attacks and a cloud-based service as a fail-over option for massive volume attacks), driving new alliances and consolidation among complementary DDoS mitigation solution providers. For example, in 2015, Akamai became a competitor in the security market by acquiring Prolexic, and in 2016, F5 acquired defense.net, a DDoS mitigation scrubbing service provider, to offer a hybrid DDoS protection solution (defense.net service was later renamed F5 Silverline). The key trends we identified in this market include the following:

- While large enterprises and service providers are focused on the technology advantage of the DDoS solutions, medium-sized organizations often balance such criteria with other considerations, like cost and ease of deployment and procurement.
- Increased adoption of cloud computing, by customers as well as attackers, is creating new opportunities and expectations for DDoS mitigation solution providers.
- Need for DDoS protection solutions provided as-a-service is increasing.
- The growing frequency and intensity of DDoS attacks in recent years have directly translated to a jump in demand for DDoS mitigation solution during such period.

WAF Solutions

General

In its 2017 Magic Quadrant report for Web Application Firewalls (WAF), Gartner summarized that the WAF market is growing, driven by the adoption of cloud-based WAF service. WAF deployments are also driven by compliance requirements such as the payment cards industry (PCI) and the GDPR that will come into effect in May 2018.

Industry trends

The key trends we identified in this market include the following:

- In recent years, WAF solutions delivered as a cloud-based service directly by the vendor (cloud-based WAF service), which initially targeted midmarket or relatively smaller organizations, has gained more attention from initialtarget of midmarket organizations.

- Cloud-based WAF service grows steadily. Gartner estimates that it now represents more than 30% of the total market in 2017 and that Cloud-native solutions increasingly compete with the more mature vendors, which Internet as a Service providers are not yet as visible in inquiries, but they also offer a WAF.

ADC Solutions

General

In its 2016 Magic Quadrant report Application Delivery Controllers (ADC), Gartner summarized that ADCs are a key component within enterprise and cloud data centers to improve application availability, performance and security.

Industry Trends

The ADC market continues to be innovative as new application-centric customers are emerging and drive changes in the market, including changes in deployment, pricing and the overall vendor landscape for application delivery. The key trends we identified in this market include the following:

- Although this market emerged from load balancing in the mid-1990s, most organizations now use advanced functionality, including WAF, global load balancing and acceleration.

- As the market evolves, ADCs are becoming less hardware-centric and the demand for software-based ADCs increases. However, we believe that, at this stage, hardware-based ADCs still provide the highest level of performance and scale.
- More organizations are relying on private or hybrid cloud-based ADC solutions, especially with cloud-based applications that require cloud-based ADC solutions.
- IT and data center managers are increasingly minded to the challenges posed by network and application attacks coupled with the need to maintain the availability and integrity of services by improved resistance to cyber-attacks.
- With the increase of encrypted web communication usage (such as the use of HTTPS, a protocol for secure communication over a computer network which is widely used on the Internet) on the Internet, cyber attackers have found a new channel through which they can gain access into an enterprise network and the sensitive information it contains without being spotted. Enterprises are expecting ADC solutions to offload Secure Sockets Layer (SSL) traffic and provide visibility into SSL-encrypted traffic to various network security tools.

(c) Our Competitive Strengths and Strategies

Our Core Assets

Our solutions incorporate proprietary and innovative cyber security and application delivery technologies that help our customers to secure the digital experience for users of business-critical applications. We believe our competitive strengths are based on the following key elements:

- Innovation, proprietary technologies and thought leadership. Being one of the first companies to offer hybrid attack mitigation solutions, we have developed and commercially deployed several generations of our products and solutions. We believe this has given us significant expertise, know-how and leadership in the market for cyber-attack mitigation solutions and we take part in many technology communities, standard organizations and open source projects. At the same time, we continue to invest in research and development of cyber security and application delivery technologies in order to introduce new and innovative solutions, which are supported and protected by multiple patents and proprietary rights.
- Global presence. We have more than 12,500 customers worldwide and have global sales, support and marketing capabilities. For example, we offer global cloud and service infrastructure based on multiple service centers dispersed globally through service data centers in Europe, Asia, North America, South America, Africa and Australia. We currently have local presence in 19 countries around the world. As such, our Technical Assistance Centers (TAC) are located to provide 24/7 support service to our customers.

- Strategic relationships. We have global technology partner alliances with leading vendors such as Cisco Systems, Inc., Check Point Software Technologies Ltd., Hewlett Packard Enterprise HPE, Nokia Corp, IBM (International Business Machines Corporation), VMware, Inc., and Symantec Corporation. We believe these relationships enable us to increase our market reach as well as offer prospects with higher solutions value.
- Customers. Our customers include top-tier banks, stock exchanges, carriers, cloud service providers, internet service providers, retailers and higher-education institutions. We believe this portfolio of high profile customers demonstrates the advantage and recognition of our solution offerings.

Our Growth Strategy

Our growth strategy is based on several key elements:

- Focus on data center solutions. Focus on developing and selling holistic cyber security and application delivery solutions for data centers and cloud applications.
- Continue investing in cloud and security. We aim to offer superior and innovative security solutions and cloud-based solutions and expand our portfolio in these two dimensions. We also intent to invest in go-to-market efforts related to cloud and security.
- Increase our market footprint. We believe that a significant market opportunity exists to sell our solutions with the complementary products and services provided by other organizations with whom we wish to collaborate. To that end, we have already established strategic relationships with various third parties, including leading global-class partners, such as Check Point, Cisco and Nokia. We intend to further increase our market footprint through OEMs, global system integrations and collaboration with leading cloud and CDN providers.
- Pursue acquisitions and investments. In order to achieve our business objectives, we may evaluate and pursue the acquisition of, or significant investments in, other complementary companies, technologies, products and/or businesses that enable us to enhance and increase our technological capabilities and expand our products and service offerings.

(d) Our Solutions

General

We are a provider of cyber security and application delivery solutions cyber security and application delivery technologies that help our customers to secure the digital experience for users of business-critical applications in virtual, cloud and software defined data centers. Our solutions are deployed, among others, by enterprises, carriers and cloud service providers.

Our solutions are offered in three main categories:

- Products – We offer a range of physical appliances and virtual appliances (software-based products) for enterprise and carrier data centers, which typically deploy on-premises solutions as part of their IT and application infrastructure.
- Product subscriptions – We offer subscriptions for value-add features and capabilities on top of our products offering. The subscriptions are typically offered as yearly activation licenses.
- Services – We offer cloud services and managed services to our customers. Our services are typically offered as a recurring monthly fee.

<u>Our Products</u>

Our product offering currently consists of the following key products:

- o DefensePro Attack Mitigation Device. DefensePro® is a real-time network attack prevention device that protects the user's application infrastructure against network and application downtime, application vulnerability exploitation, malware spread, network anomalies, information theft and other emerging network attacks.
- o AppWall Web Application Firewall. AppWall® is a WAF appliance that secures web applications. It enables PCI compliance by mitigating web application security threats and vulnerabilities to prevent data theft and manipulation of sensitive corporate and customer information. AppWall incorporates Web application security filtering technologies to effectively detect threats, block attacks and report events.
- o DefenseFlow Cyber Command and Control application. DefenseFlow® is a network-wide cyber command and control application that helps service providers to automate network security incidents response. DefenseFlow acts as a cyber-defense control-plane that collects and analyzes multiple sources of security telemetries and, based on this information, applies designated intelligent security actions. DefenseFlow enables service providers to handle large amounts of customers efficiently and with minimal errors.
- o Alteon® D Line Application Delivery Controller/Load Balancer. Alteon D Line is our next generation ADC. It provides advanced, end-to-end local and global load balancing capabilities for Web, cloud and mobile based applications. Alteon D Line is built from the ground up to allow application SLA. Alteon D Line innovatively leverages several next-generation services, bundling FastView Web Performance Optimization (WPO), HTTP/2.0 Gateway, Application Performance Monitoring (APM), AppWall Web Application Firewall (WAF), Authentication Gateway, Advanced Denial of Service (ADoS), bandwidth management, as well as SSL off-loading and SSL inspection security gateway – a feature that enables organizations to oversee outgoing encrypted traffic and filter using content security gateways. All Alteon D Line platforms are designed with comprehensive fault isolation of each ADC instance (vADC). Our vADC per application approach, along with the ability to scale up or scale out, is offered on all our Alteon D Line platforms and form factors including ADC-VX, Alteon Virtual Appliance (VA), Alteon VA for NFV and Alteon VA for cloud environment.

- o LinkProof NG Multi-homing. LinkProof® NG is a next-generation multi-homing and enterprise gateway solution that allows service level availability and continuous connectivity of enterprise and cloud-based applications. It is an application-aware multi-homing and link load balancing module that delivers 24/7 continuous connectivity and service level assurance, improved performance and cost-effective scalability of bandwidth for corporate and cloud-based applications.
- o FastView - Web Performance Optimization and Acceleration. FastView® is a web performance optimization (WPO) module that enables faster websites and web-based applications. It combines the power of its Web performance optimization (WPO) module and technology, together with an embedded HTTP/2 gateway. Each one of those modules provides a different set of capabilities that accelerate the delivery of web applications to all types of end-user devices and browsers (e.g. desktops/mobile, etc.). FastView transforms front-end optimization (FEO) from a lengthy and complex process to an automated function. This FEO is performed in real time, accelerating web application response time out-of-the-box. FastView is also available in other modes, including for SAP applications (primarily designed to accelerate SAP applications for the customer's global workforce, partners and customers) and as a cloud-based service.
- o APSolute Vision - APSolute Vision is the network management tool and network monitoring tool for the Radware family of cyber security and application delivery solutions. It provides Radware's customers immediate visibility to health, real-time status, performance and security of Radware products from one central, unified console (even if you have multiple data centers).
- o Application Performance Monitoring (APM) - APM allows our customers to detect application performance issues – before their end users customer do. APM ensures Web application performance meets the und user's expectations and consistently delivers business SLA. It provides complete visibility into our customers' applications' performance with a breakdown by application, location or specific transaction.
- o vDirect - vDirect is our service orchestration and automation engine, designed for software-defined data centers and clouds. With vDirect, customers can automate their data centers across all of Radware devices. In addition, vDirect integrates the Radware devices with leading network virtualization and orchestration solutions such as VMware vCloud Director, VMware vCenter Orchestrator, VMware vFabric Application Director Cloud Management, VMware NSX, Cisco ACI, OpenStack and others.

Our Product Subscriptions

Our product subscription offering currently consists of the following key subscription-based products:

- o Alteon Perform Subscription. The perform subscription is available on top of the Alteon D-line base product offering, adding features such as Operator Tool Box (for automated solution management), Application Performance Monitoring (APM), FastView (for web applications acceleration), Advanced Routing and LinkProof (for link load balancing).

- o Alteon Secure Subscription. The Secure subscription is available on top of the Alteon D-line Perform Subscription, adding features such as AppWall web application firewall, Application Authentication Gateway (AAG) and SSL Inspection (for inspection of encrypted internet traffic).
- o Security Updates Subscription (SUS). Our SUS service consists of periodic updates, emergency updates, and custom filters, which are supported by our own security operations center for vulnerability and exploit detection; security risk assessment; and threat mitigation support services. The service provides immediate and ongoing security updates to protect customers against the latest threats. The service is available for DefensePro and AppWall products.
- o Fraud Feed Subscription. This subscription-based service provides protection from fraud and phishing attacks. This includes protecting network users from financial fraud, information theft, and zero-minute malware spread. By subscribing to this service, customers receive updates about malicious fraud and phishing sites that are downloaded automatically to DefensePro every defined period, and block access to malicious sites from within the organization.
- o Cloud DDoS Protection Service. Our Cloud DDoS Protection Services provide a full range of enterprise-grade DDoS protection services in the cloud. Based on our DDoS protection technology, it aims to offer organizations wide security coverage, accurate detection and short time to protect from today’s dynamic and evolving DDoS attacks. We offer a multi-vector DDoS attack detection and mitigation service, handling attacks at the network layer, server-based attacks, and application-layer DDoS attacks. The solution includes protection against volumetric and non-volumetric attacks, SYN flood attacks, "low & slow" attacks, HTTP floods, SSL-based attacks and more.

Our Cloud DDoS Service is offered in multiple deployment options to meet an organization’s specific needs:

- § Hybrid Cloud DDoS service –integrates with our on-premises DDoS protection device in its data center. Recommended for organizations that can deploy an on-premises device in its data center.
- § Always-On Cloud DDoS Service (provides always-on protection where traffic is always routed through Radware's cloud security POPs (Points of Presence) with no on-premises device required for detection and mitigation. Recommended for organizations that have applications hosted in the cloud or those that are not able to deploy an on-premises attack mitigation device in their data center.
- § On-Demand Cloud DDoS Service - protects against Internet pipe saturation and is activated when the attack threatens to saturate the organization’s Internet pipe. Recommended for organizations that are looking for the lowest cost solution and are less sensitive to real-time detection of DDoS attacks.

- Cloud WAF Service - Our Cloud WAF Service provides enterprise-grade, continuously adaptive web security protection and is based on our ICSA Labs certified web application firewall. Cloud WAF includes full coverage of OWASP Top-10 threats, advanced attacks and zero-day attack protection. It automatically adapts the protections to evolving threats and protected assets.
- Cloud Malware Protection Service – Our Cloud Malware Protection service defends organizations against zero-day malware by analyzing data collected from a global community of 2 million users using patented machine learning algorithms to detect previously unknown malware based on their unique behavior patterns.
- Content Delivery Network (CDN) Service – Our CDN service provides content to end-users from the nearest location to optimize user experience, shorten website response times, and offload customer compute capacity. The CDN service uses a globally distributed network of high capacity, high-speed cache servers leveraging advanced caching techniques. Our CDN Service is based on a strategic cooperation with Verizon Digital Media Services' CDN.
- Cloud Web Acceleration Service. Our Cloud Web Acceleration Service speeds up web applications by up to 40% is designed to eliminate the need to continuously invest development resources in code optimization per browser or device type. Based on our FastView technology, Cloud Web Acceleration Service continuously monitors the web application and automatically optimizes its content for faster delivery to the end user, according to device type and web browser.

<u>Our Services</u>

Our service offering currently consists of the following key services:

- Emergency Response Team (ERT) Service. Our ERT team provides 24x7 security and product expert support for hands-on attack mitigation assistance from a single point of contact. The ERT provides expertise needed by the customer during prolonged, multi-vector attacks. This includes working closely with customers to decide on the diversion of traffic during volumetric attacks, assisting with capturing files, analyzing the situation and ensuring the best mitigation options are implemented.
- Emergency Response Team (ERT) Premium Service. The ERT Premium service is an extended set of security and operational support services that allow customers to fully outsource the monitoring and management of their organization's security to a team of security experts. ERT Premium is a managed service designed to proactively prevent emergencies, neutralize security risks, and safeguard operations from irreparable damages, thus assuring SLA and business continuity.
- Customer Support and Maintenance Services. The technical support and maintenance services consists of initial installation, set-up and ongoing support of our products, trains distributors and customers to use our products and provides software updates and product upgrades for our products. In addition, our technical team trains and certifies our distributors to provide limited technical support in each of the geographical areas in which our products are sold, and is directly responsible for remote support.

Recent Product Activities

During 2017, our key activities regarding our products and services offering consisted of the following:

- We have added Cloud Malware Protection, a cloud-based service that defends organizations against zero-day malware by analyzing data collected from a global community of millions of users using patented machine learning algorithms to detect previously unknown malware based on their unique behavior patterns. The Cloud Malware protection service is based on the acquisition of Seculert, a SaaS cloud-based provider of protection against enterprise network breach and data exfiltration.
- We have further expanded our global cloud security network by adding new scrubbing centers in South Africa, Japan, South Korea, Australia and England. Our cloud security nodes achieve now over 3.5Tbps of global mitigation capacity, enabling to segregate clean and attack traffic with dedicated scrubbing centers, and block attack traffic near origin. These nodes serve our cloud WAF offering, our DDOS cloud offering, or both.
- We have launched DDoS Protection for applications hosted on Amazon Web Services and Microsoft Azure public clouds. Radware's new Cloud DDoS Service provides organizations that host their applications on a mix of on-premises and public cloud environments with unified DDoS protection that offers consistent security policies and a single pane-of-glass. This includes a single emergency response team and focal point, a unified web security portal, single reporting tool and single DDoS protection technology across premise- and cloud-based protections.

We have launched a new line of DefensePro products to offer a full range of next generation protection platforms that includes:

- DefensePro VA – a virtual appliance with mitigation capacity of up to 20Gbps. Best for organizations operating in a virtualized environment and Software Defined Data Centers (SDDC) as well as for cloud hosting providers looking to scale protection to their customers.
- DefensePro 20 – Supporting 2Gbps through 12Gbps of legitimate traffic with up to 20Gbps mitigation capacity. Best fit for small and medium size enterprises.

- DefensePro 60 - Supporting 10Gbps through 40Gbps of legitimate traffic with up to 60Gbps mitigation capacity. Designed for large data center protection deployed by large enterprises, eCommerce and service providers.
- DefensePro 200 & 400 – Radware’s largest devices offering up to 200Gbps and 400Gbps mitigation capacity respectively. Best fit for carriers, scrubbing centers and service providers looking for a single platform to handle very high volume attacks.
- We have launched a new set of DNS service protections, protecting against large scale attacks originating from IoT botnets that target the availability of web based services through paralyzing the DNS service.
- We have launched the new Alteon D-line of appliances and software, which was designed to address evolving market challenges around the increase in encrypted traffic, the increase in encrypted attacks and malware, and the growing needs for data center automation. We have introduced new SSL process capacity across the complete suite of Alteon D line of hardware and virtual appliances with SSL connection speeds up to 98,000 CPS (2K RSA) and 48,000 CPS (256-bit ECC) and up to 40G of SSL throughput.
- We have launched Alteon VA for Microsoft Azure public cloud. Alteon VA for Azure targets enterprises that need to incorporate an application delivery solution in their cloud deployment. It comes with integrated migration tools that make cloud migration simple and easy to execute.
- Technology partnerships and integrations.

  - We have continued our investment in the OEM agreement with Cisco for DDoS Mitigation, providing our virtual DefensePro appliance for Cisco’s next generation Firewalls (Firepower 4100 series and Firepower 9000 series).
  - We have continued our investment in integrating Radware solutions with Cisco next generation and software defined data center (SDDC) technologies through vDirect, our software-based management orchestration plug-in for Cisco SDDC solutions.

(e) Sales and Marketing

Sales. We market and sell our products primarily through indirect sales channels that consist of distributors and resellers located in the Americas (including the U.S., Canada and Central and Latin America), Europe, Africa, Asia and Australia. In addition, we generate direct sales to select customers mainly in the United States. Our direct sales channels are supported by our sales and marketing managers who are also responsible for recruiting potential distributors and resellers and for initiating and managing marketing projects in their assigned regions. The sales managers are supported by our internal sales support staff that help generate and qualify leads for the sales managers. As of December 31, 2017, we had a total of 186 sales and marketing personnel, of which 70 persons were employed in the Americas with locations in various countries, mainly in the United States. We have subsidiaries and representative offices and branches in several countries (see Item 4.C. – Organizational Structure), which promote and market our products and provide customer support in their respective regions.

Marketing. Our marketing strategy is to enhance brand recognition and maintain our reputation as a provider of technologically advanced, quality cyber security and application delivery solutions to help drive demand for our products. We seek to build upon our marketing and branding efforts globally to achieve greater worldwide sales. Our sales force and marketing efforts are principally directed at developing brand awareness, generating demand and providing support to our distributors/resellers to promote sales. We participate in major trade shows, regionally-based events/seminars and offer support to our distributors and resellers who participate in these events. We also invest in online and search engine advertising campaigns, global public relations and regionalized field marketing campaigns. In addition to our independent marketing efforts, we invest in joint marketing efforts with our distributors, VARs and other companies that have formed strategic alliances with us.

We have entered into co-marketing and reseller arrangements with companies in other complementary sectors in order to broaden our customer base by selling joint solutions comprised of such complementary products. As an example, application vendors may sell our Alteon® to their customers in conjunction with their application in order to load-balance and optimize the application availability and performance. We established such co-marketing and reseller arrangements with, among others: Xura (previously Comverse); Hewlett Packard Enterprise; IBM; Microsoft Corporation; Oracle Corporation; SAP AG.; Juniper Networks, Inc.; VMWare, Inc.; Red Hat Limited; NEC Corporation; Verint Americas, Inc.; Cisco Systems Inc.; Nokia Networks and Ericsson Inc. However, there is no assurance that the above co-marketing and strategic alliance agreements would result in a substantial increase in our revenues.

Strategic Alliances and OEM Agreements. We have entered into strategic alliances and OEM agreements with other software and hardware vendors, as well as mutual channel information sharing arrangements, where products can either be branded with our name or the vendor’s name. We believe that these companies have significant customer relationships and offer products which complement our products.

For example, we entered into an agreement with Check Point Software Technologies Ltd., whereby certain of Check Point’s appliances will be based on our attack mitigation solutions; in 2015, we entered into an OEM agreement with Cisco for DDoS Mitigation, providing our virtual DefensePro appliance for Cisco Firepower 9300 series and Firepower 4100 series; and in early 2017, our strategic relationship with Nokia was expanded to include the reselling of our security solutions as part of Nokia’s offerings to carriers.

We plan to further invest in the development of strategic alliances in order to provide greater access to our target markets and enhance our brand name. We have also entered into OEM agreements with several software vendors, in which we incorporate such vendors’ software into our products to create additional value to our customers.

(f) Customers and End-Users

With the exception of our limited direct sales to selected customers, we sell our products through distributors or resellers who then sell our products to end users.

We have a globally diversified end-user base, consisting of corporate enterprises, including banks, insurance companies, manufacturing and retail companies, government agencies and media companies, and service providers, such as telecommunication carriers, internet service providers, cloud service providers and application service providers. Customers in these different vertical markets deploy Radware products for availability, performance and security of their applications from headquarters to branch offices.

In 2017, approximately 46% of our sales were in the Americas (principally in the United States), 27% were in Europe, Middle East and Africa ("EMEA") and 27% in Asia-Pacific, compared to 43%, 27% and 30%, respectively, in 2016, and 41%, 29% and 30%, respectively, in 2015. Other than the United States, which accounted for 37% of our total revenues in 2017, no other single country accounted for more than 10% of our sales for 2017.

In 2017, approximately 56% of our sales derived from product sales and 44% derived from service sales, same as in 2016 and 63% and 37%, respectively, in 2015. We believe that this reflects our strong product installed base that drives a demand for our support and managed services and maintenance, as well as a decline in our product sales.

In 2017, approximately 66% of our sales derived from the enterprise market and 34% derived from the carrier market, compared to approximately 69% and 31%, respectively, in 2016 and 71% and 29%, respectively, in 2015.

As of December 31, 2017, 2016 and 2015, no single customer accounted for more than 10% of our sales or more than 10% of our trade receivables balance.

For additional details regarding the breakdown of our revenues by geographical distribution and by activity, see "Item 5A – Operating and Financial Review and Prospects – Operating Results".

(g) Seasonality

Our quarterly operating results have been, and are likely to continue to be, influenced by seasonal fluctuations in our sales and by seasonal purchasing patterns of some of our customers. Some of our customers plan their annual purchasing budget at the beginning of each year which causes operating results in our first quarter of the year to be typically lower than other quarters. In addition, our operating results in the fourth quarter tend to be higher than other quarters as some of our customers tend to make greater capital and operational expenditures as well as expenditures relating to service renewals towards the end of their own fiscal years, thereby increasing orders for our products, support and subscription services in the fourth quarter.

(h) Customer Support Services

Our technical team, which consisted of 244 employees worldwide as of December 31, 2017, supports our sales force during the sales process, assists our customers and distributors with the initial installation, set-up and ongoing support of our products, trains distributors and customers to use our products and provides software updates and product upgrades for our products. In addition, our technical team trains and certifies our distributors to provide limited technical support in each of the geographical areas in which our products are sold, and is directly responsible for remote support. Our Certainty Support Program provides offerings which allow customers to automatically obtain new software versions of their products and obtain optimized performance by purchasing any of the following optional offerings: extended warranty, software updates, 24x7 help-desk (directly to our customers and through our distributors), on-site support and unit replacement. Some of our on-site services are provided by third party contractors.

(i) Research and Development

We place considerable emphasis on research and development to expand the capabilities of our existing products, develop new products and improve our existing technologies and capabilities. We believe that our future success will depend upon our ability to maintain our technological expertise, enhance our existing products and introduce, on a timely basis, new commercially viable products that will continue to address the needs of our customers. Accordingly, we intend to continue devoting a significant portion of our personnel and financial resources to research and development. In order to identify market needs and to define appropriate product specifications, as part of the product development process we seek to maintain close relationships with current and potential distributors, customers and vendors in related industry sectors.

As of December 31, 2017, our research and development staff consisted of 320 employees and 61 subcontractors. Research and development activities take place mainly at our facilities in Israel, Vancouver, Canada; and North Carolina, United States and our sub-contractor in Bangalore, India. We employ established procedures for the required management, development and quality assurance of our new product developments. Our research and development organization is divided into Security, Application Delivery, Cloud Malware and Management groups. Within those groups the organization is divided according to our existing product solutions. Each product group is headed by a group leader and includes team leaders and engineers. Each group has a dedicated quality assurance team. In addition, we have an infrastructure department responsible for the development of our platforms which are the basis for all products, serving all product groups, which consist of a senior group leader, group leaders, team leaders, and engineers. The heads of all research and development divisions report to either the Chief Operating Officer or the Chief Technology Officer.

See also below under "Government Regulations – Israeli Innovation Authority.”

(j) Manufacturing and Suppliers

Our quality assurance testing, final integration, packaging and shipping operations as well as part of our final assembly activities are primarily performed at our facility in Jerusalem, Israel. All of our products are Underwriters Laboratories (UL) and ISO 9001:2008 compliant and some of them have also achieved significant industry certifications, such as DefensePro (for the Common Criteria Evaluation & Validation Scheme (CCEVS) EAL4+ through the National Security Agency (NSA) program) and AppWall (ICSA certification for Web Application Firewall).

We rely on third-party manufacturing vendors to provide our finished products. In this respect, these vendors primarily provide us with manufacturing assembly services in order to deliver the finished goods while we perform the final integration of the products. All components and subassemblies included in our products are supplied to the manufacturing vendors by several suppliers and subcontractors. Each of the manufacturing vendors monitors each stage of the components production process, including the selection of components and subassembly suppliers. Thereafter, each of the manufacturing vendors makes the final assembly in their own facility. Our primary manufacturing vendors are ISO 9001 certified, indicating that each of their manufacturing processes adhere to established quality standards.

In 2017, we primarily relied on two ODMs to manufacture and to supply our hardware platforms, whereby approximately 47% of our direct product costs were from one of these vendors and 34% were from the other vendor. There are also two additional vendors from whom we buy components for main accessories – in 2017, we purchased 8% of such accessories from one of these vendors and 4% from the other.

We conduct a business continuity plan (BCP) with all our vendors to ensure an immediate recovery in case of crisis that might jeopardize the supply of our products. However, if we are unable to continue to acquire those platforms or components from these platform manufacturers and vendors on acceptable terms, or should any of these suppliers cease to supply us with such platforms or components for any reason, we may not be able to identify and integrate an alternative source of supply in a timely fashion or at the same costs. Any transition to one or more alternate suppliers would likely result in delays, operational problems and increased costs, and may limit our ability to deliver our products to our customers on time for such transition period, although we believe we have levels of inventory that will assist us to transition to alternate suppliers smoothly.

(k) Proprietary Rights

We rely on patent, trademark and trade secret laws, as well as confidentiality agreements and other contractual arrangements with our employees, distributors and others to protect our technology. We have a policy that requires our employees to execute employment agreements, including confidentiality and non-competition provisions.

We have registered trademarks for, among others, Radware®; Radware Logo: ®; OnDemand Switch®; Alteon®; APSolute®; LinkProof®; DefensePro®; CID®; SIPDirector®; AppDirector®; AppXcel®; AppXML®; AppWall®; APSolute Insite®; Triangulation®; SmartNat®; StringMatch Engine®; Web Server Director®; Fireproof®; SecureFlow®; APSolute Vision®; VAdapter®; vDirect®; Alteon VA®; AppShape®; FastView®; DefenseFlow®; TeraVIP®; Virtual Director®; DefensePipe®;"ADC Fabric®"; CyberStack® and "Virtual DefensePro® and we have trademark applications pending for, among others, "ADC-VX"™; VADI™ (Virtual Application Delivery Infrastructure) and "Inflight"™, ". We own registered U.S. copyrights in all of our primary software product lines.

We have registered patents in the United States and Canada for, among others, our triangle redirection method used for the global load balancing in our AppDirector product; our mechanism for efficient management and optimization of multiple links used in our LinkProof product; our method for load balancing by global proximity used in our AppDirector product; our method for controlling traffic on links between autonomous Border Gateway Protocol (BGP) systems; the stateful distribution of copied SSL traffic; the transparent inspection of encrypted client traffic; our passive monitoring and event detection mechanisms used for business event monitoring in our Inflight product; the activation of multiple virtual services on a switching platform; the behavioral analysis and detection of zero-day and DoS network attack patterns in our DefensePro product; our hypertext transfer protocol (HTTP) DoS attack mitigation behavioral mechanisms in our DefensePro; a geographically based traffic distribution; a generic proximity based site selection for global load balancing; an internal hardware connectivity plane architecture; a specific proximity based site selection for global load balancing of HTTP transactions implemented in our Alteon products; and additional patents in the SDN field, around a new concept of cyber control and automation for our DefenseFlow Product.

We have pending patent applications and provisional patents in connection with several methods and features used in our products or that we plan to implement in the future, such as advanced algorithms for cyber detection defending against new kinds of attacks (Burst and IoT related attacks, detection of attacks within AWS etc.), patent applications around the cyber control and automation (DefenseFlow) and around ADC for SDDC adapted for containerized environments. In 2017, we continued to add new capabilities covered by such patent applications to our lines of security, namely new algorithms to fight against new attack surfaces resulting from IoT, and added new capabilities to defeat application floods against workloads that are hosted in public clouds such as AWS and Azure. Our new patent applications allowed us extended the surface of the DefenseFlow to control, manage and automate attack mitigation across all domains: scrubbing centers, enterprise data-centers and cloud data-centers. The notion of DefenseFlow client was extended to DetectPro which has been develop as a software based programmable detector with flexible form factors and deployment modes, to extend our detection footprints across new domains such as: micro-perimeters and edge-compute. Another domain that we have added new capabilities covered by patent applications is integration of our Alteon load-balancer with micro-services. We have integrated Alteon as a front-end service to automatically learn the Kubernetes eco-system and auto-configure itself based on the ever-changing containerized application environment. These applications may not result in any patent being issued, and, if issued, the patents may not provide adequate protection against competitive technology and may not be held valid and enforceable if challenged. In addition, other parties may assert rights as inventors of the underlying technologies, which could limit our ability to fully exploit the rights conferred by any patent that we receive. See “Item 8. Financial Information – Legal Proceedings” for a discussion of intellectual property litigation. Our competitors may be able to design around a patent we receive and other parties may obtain patents that we would need to license or circumvent in order to exploit our patents.

The protective steps we have taken may be inadequate to deter misappropriation of our technology and information. We may be unable to detect the unauthorized use of, or take appropriate steps to enforce, our intellectual property rights. Some of the countries in which we sell our products do not protect intellectual property to the same extent as the United States and Israel. In addition, our competitors may independently develop technologies that are substantially equivalent or superior to our technology. Any licenses for intellectual property that might be required for our services or products may not be available on reasonable terms.

(l) Competition

The cyber security and application delivery market is highly competitive and we expect competition to intensify in the future. We may lose market share if we are unable to compete effectively with our competitors, which include equipment manufacturers and service providers.

Our principal competitors are:

- Equipment manufacturers (DDoS Protection): Netscout Systems Corp. (through Arbor Networks); and A10 Networks, Inc.
- Equipment manufacturers (ADC): F5 Networks, Inc., or F5; Citrix Systems, Inc.; and A10 Networks, Inc.
- Equipment manufacturers (WAF): Imperva; F5; Akamai.
- Cloud service providers (DDoS protection and Cloud WAF): Akamai (Prolexic); Imperva (through Incapsula, Inc.); Neustar and Verisign;
- Cloud service providers (ADC): Amazon Web Services; Microsoft Azure.

We expect to continue to face additional competition as new participants enter the market or extend their portfolios into related technologies. Larger companies with substantial resources, brand recognition and sales channels may also form alliances with or acquire competing providers of application delivery or application and network security solutions and emerge as significant competitors.

Competition may result in lower prices or reduced demand for our products and a corresponding reduction in our ability to recover our costs as well as increased costs associated with sales and marketing expenses to maintain or increase market share which may impair our ability to increase profitability. Furthermore, the dynamic market environment, which is demonstrated by the above acquisitions, poses a challenge in predicting market trends and expected growth. We believe that our success will depend primarily on our ability to provide more technologically advanced and cost-effective application delivery and application and network security solutions, and more responsive customer service and support, than our competitors. However, we cannot assure you that the products we offer will compete successfully with those of our competitors. Furthermore, should competition intensify, we may have to reduce the prices of our products which will negatively impact our business and financial condition. See also above under “Business Overview – Our Competitive Strengths and Strategies”.

(m) Government Regulations

Environmental Regulations

Our activities in Europe require that we comply with European Union Directives with respect to product quality assurance standards and environmental standards. The “RoHs” and RoHs II Directives require products sold in Europe to meet certain design specifications, which exclude the use of hazardous substances. Directive 2002/96/EC on Waste Electrical and Electronic Equipment (known as the “WEEE” Directive) requires producers of electrical and electronic equipment to register in different European countries and to provide collection and recycling facilities for used products. We are currently in compliance with the RoHs and WEEE regulations and ISO 14001 standards (re Environmental Management Systems).

Israeli Innovation Authority

From time to time, eligible participants may receive grants under programs of the IIA. Grants received are generally repaid through a mandatory royalty based on revenues from the sale of products (and ancillary services) incorporating know-how developed, in whole or in part, with the grants. This governmental support is conditioned upon the participant’s ability to comply with certain applicable requirements and conditions specified in the IIA’s programs and the R&D Law.

Under the R&D Law, research and development programs that meet specified criteria and are approved by the Research Committee of the IIA are eligible for grants usually of up to 66% of certain approved expenditures of such programs, as determined by said committee. In exchange, the recipient of such grants is required to pay the IIA royalties from the revenues derived from products incorporating know-how developed within the framework of each such program or derived therefrom (including ancillary services in connection therewith), up to an aggregate of 100% of the dollar-linked value of the total grants received in respect of such program, plus interest.

The R&D Law also provides that know-how developed under an approved research and development program or rights associated with such know-how (1) may not be transferred to third parties in Israel without the approval of the IIA (such approval is not required for the sale or export of any products resulting from such research or development) and (2) may not be transferred to any third parties outside Israel, except in certain special circumstances and subject to the IIA’s prior approval, which approval, if any, may generally be obtained, in the following cases: (a) the grant recipient pays to the IIA a portion of the sale price paid in consideration for such IIA-funded know-how (according to certain formulas, which may result in repayment of up to 600% of the grant amounts plus interest), or (b) the grant recipient receives know-how from a third party in exchange for its IIA-funded know-how. Such approval is not required for the export of any products resulting from such research or development.

The R&D Law imposes reporting requirements with respect to certain changes in the ownership of a grant recipient. The law requires the grant recipient and its controlling shareholders and foreign interested parties to notify the IIA of any change in control of the recipient or a change in the holdings of the means of control of the recipient and requires a non-Israel interested party to undertake to the IIA to comply with the R&D Law. In addition, the rules of the IIA may require additional information or representations in respect of certain of such events. For this purpose, “control” is defined as the ability to direct the activities of a company other than any ability arising solely from serving as an officer or director of the company. A person is presumed to have control if such person holds 50% or more of the means of control of a company. “Means of control” refers to voting rights or the right to appoint directors or the chief executive officer. An “interested party” of a company includes a holder of 5% or more of its outstanding share capital or voting rights, its chief executive officer and directors, someone who has the right to appoint its chief executive officer or at least one director, and a company with respect to which any of the foregoing interested parties owns 25% or more of the outstanding share capital or voting rights or has the right to appoint 25% or more of the directors. Accordingly, any non-Israeli who acquires 5% or more of our ordinary shares will be required to notify us that it has become an interested party and to sign an undertaking to comply with the R&D Law.

The Israeli authorities have indicated in the past that the government may further reduce or abolish the IIA grants in the future. Even if these grants are maintained, we cannot presently predict what would be the amounts of future grants, if any, that we might receive. In addition, an amendment to the R&D Law that became effective on January 1, 2016, provides the IIA with authority to establish new guidelines regarding the R&D Law, which may affect our existing and/or future IIA programs and incentives for which we may be eligible. We cannot predict what changes, if any, the IIA may make.

During 2012-2014 we received grants from the IIA to fund certain other research and development projects as part of our participation in the MAGNET Consortium Program, which is a program that sponsors innovative generic industry-oriented technologies to strengthen the country’s technological expertise and enhance competitiveness. These grants do not bear any royalty repayment obligations. In 2012, 2013 and 2014 we received $0.3 million, $0.4 million, and $0.3 million respectively, in IIA grants under such MAGNET programs.

In 2017 and 2016, we were qualified to participate in three projects funded by the IIA to develop generic technology relevant to the development of our products. We were eligible to receive grants constituting between 30% and 50% of certain research and development expenses relating to these projects. The grants under these projects are not required to be repaid by way of royalties. Grants for the years ended December 31, 2016 and 2017 were $ 0.9 million and $ 0.6 million, respectively.

C. Organizational Structure

We have a wholly-owned subsidiary in the United States, Radware Inc., which conducts the sales and marketing of our products in the United States. We also have subsidiaries in Australia, France, Germany, the United Kingdom, Italy, Japan, Singapore, Korea, Canada, India, Israel, China and Hong Kong, most of which typically conduct the sales and marketing of our products in their respective locations. We have also established representative offices in Taiwan and Spain. Our subsidiaries include:

Name of Subsidiary	Country of Incorporation
Radware Inc.	New Jersey, United States of America
Radware UK Limited	United Kingdom
Radware France	France
Radware Srl	Italy
Radware GmbH	Germany
Nihon Radware KK	Japan
Radware Australia Pty. Ltd.	Australia
Radware Singapore Pte. Ltd.	Singapore
Radware Korea Ltd.	Korea
Radware Canada Inc.	Canada
Radware India Pvt. Ltd.	India
Radware China Ltd.	China
Radware (Hong Kong) Limited	Hong Kong
Radyoos Media Ltd.*	Israel
Seculert Ltd.**	Israel
Radware Canada Holdings Inc.	Canada
Radware Iberia, S.L.U.	Spain

* We own 91% of this subsidiary. All other listed subsidiaries are wholly owned.

** Seculert Ltd. was merged into Radware on December 31, 2017.

Yehuda Zisapel, one of our co-founders and shareholders, is the Chairman of our Board of Directors and the father of Roy Zisapel, our President, Chief Executive Officer and director. Individually or together with his brother, Zohar Zisapel, and with Nava Zisapel, Yehuda Zisapel is also a founder, director and/or principal shareholder of several other companies which, together with our Company and our subsidiaries listed above are known as the RAD-Bynet Group. These companies include, among others:

AB-NET Communications Ltd.	Ceragon Networks Ltd.	
Ace – Assured Customer Experience Ltd.	Internet Binat Ltd.	
Binat Business Ltd.	Nuance Hearing Ltd.	
BYNET Data	Packetlight Networks Ltd.	RADWIN Ltd.
Communications Ltd.	RAD-Bynet Properties and Services (1981) Ltd.	SecurityDam Ltd.
BYNET Electronics Ltd.	Radbit Computers, Inc.	Silicom Ltd.
BYNET SEMECH (outsourcing) Ltd.	RADCOM Ltd.	
Bynet Software Systems Ltd.	RAD Data Communications Ltd.	
Bynet System Applications Ltd.	Radiflow Ltd.	

The RAD-Bynet Group also includes several other holdings, real estate companies, biotech and pharmaceutical companies and the above list does not constitute a complete list of the holdings of Messrs. Yehuda and Zohar Zisapel.

In addition to engaging in other businesses, members of the RAD-Bynet Group are actively engaged in designing, manufacturing, marketing and supporting data communications products, none of which currently compete with our products. Some of the products of members of the RAD-Bynet Group are complementary to, and may be used in connection with, our products. See also “Item 7B – Major Shareholders and Related Party Transactions - Related Party Transactions”.

D. Property, Plants and Equipment

General. We operate from leased premises mainly in Tel Aviv and Jerusalem in Israel and New Jersey in the United States. We also lease premises in several locations in Europe and Asia-Pacific for the activities of our subsidiaries, representative offices and branches. Our aggregate annual rent expenses under these leases were approximately $6.2 million in 2017 compared to $5.4 in 2016.

We believe that the following offices and facilities are suitable and adequate for our operations as currently conducted and as currently foreseen. In the event that additional or substitute offices and facilities are required, we believe that we could obtain such offices and facilities at commercially reasonable rates.

Israel. Our headquarters and principal administrative, finance, research and development and marketing operations are located in approximately 100,000 square feet of leased office space in Tel Aviv, Israel, in two buildings: one, consisting of approximately 40,000 square feet, with a lease expiring in June 2020; and the second consisting of approximately 60,000 square feet, with a lease expiring in June 2020. These facilities are leased from companies owned by Yehuda, Nava and Zohar Zisapel. For more information see – "Item 7 - Major Shareholders and Related Parties Transactions."

In addition, we lease approximately 3,600 square feet of space in Jerusalem for development facilities from a company owned by Yehuda, Nava and Zohar Zisapel. The lease expires in August 2020. We also sublease approximately 15,000 square feet for warehousing in Jerusalem from a company owned by Yehuda, Nava and Zohar Zisapel. The lease expires in August 2019. For more information, see "Item 7 - Major Shareholders and Related Parties Transactions."

Other locations. In the United States, we lease approximately 16,900 square feet of property, consisting of approximately 12,700 square feet of office space and 4,200 square feet of warehouse space, in Mahwah, New Jersey from a company owned by Yehuda, Nava and Zohar Zisapel. The lease expires in December 2018. For more information, see – "Item 7 - Major Shareholders and Related Party Transactions."

We lease approximately 3,800 square feet of property for our research and development facilities in North Carolina, the lease for which will expire in September 2018. In addition, we lease approximately 5,700 square feet of property in Sunnyvale, California, the lease for which will expire in December 2021.

We lease facilities for the operation of our subsidiaries and representative offices in several locations in Europe and Asia-Pacific, all from unrelated third parties.

ITEM 4A. UNRESOLVED STAFF COMMENTS

None.

ITEM 5. OPERATING AND FINANCIAL REVIEW AND PROSPECTS

Our discussion and analysis of our financial condition and results of operation are based upon our consolidated financial statements, which have been prepared in accordance with generally accepted accounting principles in the United States. Our operating and financial review and prospects should be read in conjunction with our financial statements, accompanying notes thereto and other financial information appearing elsewhere in this annual report.

A. Operating Results

Overview

We are a provider of cyber security and application delivery solutions designed to secure the user digital experience for business-critical applications in virtual, cloud and software defined data centers. Our solutions are deployed by enterprises, carriers and cloud service providers. We began selling our products in 1997, and currently have local offices, subsidiaries or branches in 19 countries in Asia-Pacific, Europe and the Americas.

We sell through sales channels such as resellers and distributors whereas most of our direct sales are to strategic customers.

Most of our revenues are generated in dollars or are dollar-linked and the majority of our expenses are incurred in dollars and, as such, the dollar is our functional currency. Our consolidated financial statements are prepared in dollars and in accordance with U.S. GAAP.

Our revenues are derived from sales of our products and services:

- We recognize product revenue when persuasive evidence of an arrangement exists, delivery has occurred, the fee is fixed or determinable, no further obligation exists and collectability is probable. We recognize revenues from product subscriptions, ratably over the subscription period.
- Revenues from post-contract customer support and service subscriptions, which represents mainly software update subscriptions, help-desk support and unit repairs or replacements, are recognized ratably over the contract or subscription period.

We operate in one reportable market segment and our revenues are attributed to geographic areas based on the location of the end-users.

In the years ended December 31, 2017, 2016 and 2015, revenues derived from sales of the Company’s products constituted approximately 56%, 56% and 63%, respectively, of our total revenues, with the remaining revenues being derived from services. A significant portion of our revenues is derived from repeat product sales to existing customers, and we expect that repeat product sales will continue to account for a significant portion of such revenues in the future. As our installed base of products grows, service revenues are also generally expected to increase.

On January 30, 2017 we acquired Seculert. The consideration to acquire Seculert was $10 million in cash and additional contingent consideration of up to $10 million, based on certain milestones to be achieved. The derived goodwill from this acquisition is attributable to additional capabilities of the Company to expand its products portfolio. Goodwill generated from this business combination is primarily attributable to synergies between the Company's and Seculert's respective products and services.

We recorded IPR&D, technology and goodwill in amount of $7.1 million, $2.2 million and $2.1 million, respectively. The estimated useful life of the IPR&D and technology is approximately 9 years.

For our recording of our IPR&D, technology and goodwill and estimated payments of the contingency milestones see also Note 1(c) and Note 4 to our consolidated financial statements included elsewhere in this annual report.

Critical Accounting Policies

In many cases, the accounting treatment of a particular transaction is specifically dictated in U.S. GAAP and does not require management's judgment in its application. There are also areas in which management's judgment in selecting among available alternatives would produce a materially different result. Our management has reviewed these critical accounting policies and related disclosures with our Audit Committee. See note 2 to our consolidated financial statements included elsewhere in this annual report, which contains additional information regarding our accounting policies and other disclosures required by U.S. GAAP.

Our management believes that the significant accounting policies which affect its more significant judgments and estimates used in the preparation of its consolidated financial statements and which are the most critical to aid in fully understanding and evaluating our reported financial results include the following:

- Revenue recognition;
- Investment in marketable securities;
- Goodwill;
- Impairment of long lived assets and intangible assets subject to amortization;
- Stock-based compensation; and
- Income taxes.

Revenue Recognition. We derive revenues mainly from sales of products and services:

- We recognize product revenue in accordance with Accounting Standards Codification, or ASC, No. 605, "Revenue Recognition", when persuasive evidence of an arrangement exists, delivery has occurred, the fee is fixed or determinable, no further obligation exists and collectability is probable. We recognize revenues from product subscriptions, ratably over the subscription period.
- Revenues from PCS and service subscriptions, which represents mainly software update subscriptions, help-desk support and unit repairs or replacements, are recognized ratably over the term of the agreement, which is typically between one year and three years.

Our products are sold partially through distributors and resellers, all of which are considered end-users.

Our products and services generally qualify as separate units of accounting. As such, revenues from multiple element arrangements that include products, PCS and subscriptions are separated into their various elements using the relative selling price method. The estimated selling price for each deliverable is based on its vendor specific objective evidence ("VSOE"), if available, third party evidence ("TPE") if VSOE is not available, or estimated selling price ("ESP") if neither VSOE nor TPE is available.

We determine the best estimated selling price ("ESP") in multiple-element arrangements as follows: VSOE for post-contract customer support is determined based on the price charged when such element is sold separately (renewals). The price may vary in the territories and vertical markets in which we conduct business. Price is determined by using a consistent percentage of our product price lists, in the same territories and markets.

For the product and subscriptions, we determine the ESP based on management estimated selling price by considering several external and internal factors including, but not limited to, pricing practices including discounting, margin objectives, and competition. The determination of ESP is made through consultation with and approval of management, taking into consideration the pricing model and go-to-market strategy.

We record a provision for estimated sale returns and stock rotation granted to customers on products in the same period the related revenues are recorded in accordance with ASC No. 605. These estimates are based on historical sales returns, stock rotations and other known factors. Such provisions amounted to $ 1.7 million and $1.0 million as of December 31, 2017 and 2016, respectively.

Deferred revenues include unearned amounts received under post-contract customer support and subscription agreements, and are classified in short and long-term based on their contractual term. Deferred revenues amounts which represent uncollected amounts are offset against account receivables.

Investment in Marketable Securities. We account for investments in marketable securities in accordance with ASC No. 320, "Investments- Debt and equity Securities". Management determines the appropriate classification of our investments at the time of purchase and reevaluates such determinations at each balance sheet date.

We classified all of our debt and equity securities as available-for-sale securities. Available-for-sale securities are carried at fair value, with the unrealized gains and losses reported in "accumulated other comprehensive income (loss)" in shareholders' equity. Realized gains and losses on sales of investments are included in financial income, net and are derived using the specific identification method for determining the cost of securities.

The amortized cost of debt securities is adjusted for amortization of premiums and accretion of discounts to maturity. Such amortization together with interest and dividends on securities are included in financial income, net.

We recognize an impairment charge when a decline in the fair value of our investments below the cost basis is judged to be other-than-temporary. The factors considered in making such a determination include the duration and severity of the impairment, the reason for the decline in value, the potential recovery period and our intent to sell, including whether it is more likely than not that we will be required to sell the investment before recovery of cost basis. For securities that are deemed other-than-temporarily impaired, the amount of impairment recognized in the statement of income is limited to the amount related to credit losses, while impairment related to other factors is recognized in other comprehensive income. During the years 2017, 2016 and 2015, we did not record any other-than-temporary impairment loss with respect to our marketable securities.

Goodwill. Goodwill represents the excess of the purchase price in a business combination over the fair value of the net tangible and intangible assets acquired. Under ASC 350 "Intangibles – Goodwill and Other" ("ASC 350"), goodwill is not amortized, but rather is subject to an annual impairment test. ASC 350 requires goodwill to be tested for impairment at least annually or between annual tests in certain circumstances, and written down when impaired. Goodwill is tested for impairment by comparing the fair value of the reporting unit with its carrying value.

ASC 350 allows an entity to first assess qualitative factors to determine whether it is necessary to perform the two-step quantitative goodwill impairment test. If the qualitative assessment does not result in a more likely than not indication of impairment, no further impairment testing is required. If it does result in a more likely than not indication of impairment, the two-step impairment test is performed. Alternatively, ASC 350 permits an entity to bypass the qualitative assessment for any reporting unit and proceed directly to performing the first step of the goodwill impairment test.

We operate in one operating segment, and this segment comprises our single reporting unit. We perform assessment of qualitative factors during the fourth quarter of each fiscal year, or more frequently if impairment indicators are present. This analysis determined that no indicators of impairment existed for 2017, 2016 and 2015.

Impairment of long lived assets and intangible assets subject to amortization. Property and equipment and intangible assets subject to amortization are reviewed for impairment in accordance with ASC No. 360, "Accounting for the Impairment or Disposal of Long-Lived Assets," whenever events or changes in circumstances indicate that the carrying amount of an asset may not be recoverable. Recoverability of assets to be held and used is measured by a comparison of the carrying amount of an asset to the future undiscounted cash flows expected to be generated by the assets. If such assets are considered to be impaired, the impairment to be recognized is measured by the amount by which the carrying amount of the assets exceeds the fair value of the assets.

Intangible assets acquired in a business combination are recorded at fair value at the date of acquisition. Following initial recognition, intangible assets are carried at cost less any accumulated amortization and any accumulated impairment losses. The useful lives of intangible assets are assessed to be either finite or indefinite. Intangible assets that are not considered to have an indefinite useful life are amortized over their estimated useful lives, which range from five to nine years. Some of the acquired customer arrangements are amortized over their estimated useful lives in proportion to the economic benefits realized. This accounting policy results in accelerated amortization of such customer arrangements as compared to the straight-line method. All other intangible assets are amortized over their estimated useful lives on a straight-line basis.

During 2017, 2016 and 2015, no impairment losses were recorded.

Stock-based compensation. We account for stock-based compensation in accordance with ASC No. 718, "Compensation-Stock Compensation". ASC No. 718 requires companies to estimate the fair value of equity-based payment awards on the date of grant using an option-pricing model. The value of the portion of the award that is ultimately expected to vest is recognized as an expense over the requisite service periods in our consolidated statement of income.

We recognize compensation expenses for the value of our awards based on the accelerated attribution method over the requisite service period of each of the awards, net of estimated forfeitures. ASC No. 718 requires forfeitures to be estimated at the time of grant and revised, if necessary, in subsequent periods if actual forfeitures differ from those estimates. Estimated forfeitures are based on actual historical pre-vesting forfeitures.

ASC No. 718 requires the cash flows resulting from the tax deductions in excess of the compensation costs recognized for those stock options to be classified as financing cash flows.

We selected the Black-Scholes-Merton option pricing model to account for the fair value of our stock-options awards with only service conditions and whereas the fair value of the restricted stocks awards is based on the market value of the underlying shares at the date of grant. The option-pricing model requires a number of assumptions, of which the most significant are the expected stock price volatility and the expected option term. Expected volatility was calculated based upon actual historical stock price movements over an historical period equivalent to the option's expected term. The expected option term represents the period of time that options are expected to be outstanding. Expected term of options is based on historical experience. The risk-free interest rate is based on the yield from U.S. treasury bonds with an equivalent term. We have historically not paid dividends and have no foreseeable plans to pay dividends.

During 2016, we approved the repricing of 667,750 stock options for several employees and senior management, previously granted under the Stock Option Plans. As a result, the exercise price of the options was lowered to a price per share lower than the original grant exercise price, but a higher price than the known share’s closing price on Nasdaq on the modification date. There was no change in the number of shares subject to each option, vesting or other terms of the options. The incremental expense for the repricing of the options is approximately $1.2 million. For the year ended December 31, 2016, we recorded expenses totaling $0.4 million associated with the repricing.

Income Taxes. We account for income taxes in accordance with ASC No. 740, "Income Taxes". This statement prescribes the use of the liability method whereby deferred tax assets and liability account balances are determined based on differences between financial reporting and tax bases of assets and liabilities and are measured using the enacted tax rates and laws that will be in effect when the differences are expected to reverse. We provide a valuation allowance, if necessary, to reduce deferred tax assets to their estimated realizable value if it is more likely than not that a portion or all of the deferred tax assets will not be realized. Deferred tax liabilities and assets are classified as non-current in accordance with Accounting Standard Update, or ASU, No. 2015-17 (see also Note 2(ab) to our consolidated financial statements included elsewhere in this annual report). ASC No. 740 contains a two-step approach to recognizing and measuring a liability for uncertain tax positions. The first step is to evaluate the tax position taken or expected to be taken in a tax return by determining if the weight of available evidence indicates that it is more likely than not that, on an evaluation of the technical merits, the tax position will be sustained on audit, including resolution of any related appeals or litigation processes. The second step is only addressed if the first step has been satisfied (i.e. the position is more likely than not to be sustained) otherwise a full liability in respect of a tax position not meeting the more likely than not criteria is recognized. The second step is to measure the tax benefit as the largest amount that is more than 50% likely to be realized upon ultimate settlement. We accrue interest and penalty, if any related to unrecognized tax benefits in its taxes on income. Although we believe we have adequately reserved for our uncertain tax positions, no assurance can be given that the final tax outcome of these matters will not be different. We adjust these reserves in light of changing facts and circumstances, such as the closing of a tax audit, the refinement of an estimate or changes in tax laws. To the extent that the final tax outcome of these matters is different than the amounts recorded, such differences will impact the provision for income taxes in the period in which such determination is made. The provision for income taxes includes the impact of reserve provisions and changes to reserves that are considered appropriate, as well as the related interest and penalties.

Accounting for tax positions requires judgments, including estimating reserves for potential uncertainties. We also assess our ability to utilize tax attributes, including those in the form of carry forwards for which the benefits have already been reflected in the financial statements. We do not record valuation allowances for deferred tax assets that we believe are more likely than not to be realized in future periods. While we believe the resulting tax balances as of December 31, 2017 and 2016 are appropriately accounted for, the ultimate outcome of such matters could result in favorable or unfavorable adjustments to our consolidated financial statements and such adjustments could be material. See Note 12 to our consolidated financial statements included elsewhere in this annual report for further information regarding income taxes. We have filed or are in the process of filing local and foreign tax returns that are subject to audit by the respective tax authorities. The amount of income tax we pay is subject to ongoing audits by the tax authorities, which often result in proposed assessments. See “Results of Operations – Taxes” below.

While we believe that we have adequately provided for any reasonably foreseeable outcomes related to tax audits and settlement, our future results may include favorable or unfavorable adjustments to our estimated tax liabilities in the period the assessments are made or resolved, audits are closed or when statutes of limitation on potential assessments expire.

New Accounting Pronouncements Not Yet Effective

In May 2014, the Financial Accounting Standards Board, or the FASB, issued ASU No. 2014-09, "Revenue from Contracts with Customers (Topic 606)", or ASU No. 2014-09, a new standard related to revenue recognition and, thereafter, issued related subsequent updates or, collectively, the New Revenue Standard. Under the New Revenue Standard, revenue is recognized when a customer obtains control of promised goods or services and is recognized in an amount that reflects the consideration, which the entity expects to receive in exchange for those goods or services. In addition, the New Revenue Recognition Standard requires disclosure of the nature, amount, timing, and uncertainty of revenue and cash flow arising from contracts with customers. The New Revenue Standard permits two methods of modification: retrospectively to each prior reporting period presented (the so-called "full retrospective method"), or retrospectively with the cumulative effect of initially applying the guidance recognized at the date of initial application (the so-called "modified retrospective method"). We have adopted the New Revenue Standard, effective January 1, 2018, using the modified retrospective method applied to those contracts, which were not substantially completed as of January 1, 2018. The cumulative adjustment will decrease our retained earnings by $0.1 million to the opening accumulated balance.

We expect that the most significant impact of the New Revenue Standard on us will relates to the way we account for sales commission expenses. We have also considered the impact of the guidance in ASC No. 340-40, "Other Assets and Deferred Costs", in light of the New Revenue Standard. Under ASC No. 340-40, we may be required to capitalize and amortize certain incremental costs of obtaining a contract, such as the maintenance portion of sales commission costs. The cumulative impact to our retained earnings as of January 1, 2018 will increase our opening accumulated balance by approximately $10.2 million.

Adoption of the New Revenue Standard had no impact to cash from or used in operating, investing or financing activities on our consolidated statement of cash flows.

Recently Issued Accounting Pronouncements

In February 2016, the FASB issued ASU No. 2016-02, Leases (Topic 842), which changes the current lease accounting standard by requiring the recognition of lease assets and lease liabilities for all leases, including those currently classified as operating leases. This new standard is to be applied under a modified retrospective application to the earliest reporting period presented for reporting periods beginning after December 15, 2018. Early adoption is permitted. We are currently evaluating the potential impact of this new standard on our financial statements.

In June 2016, the FASB issued ASU No. 2016-13, "Financial Instruments—Credit Losses (Topic 326): Measurement of Credit Losses on Financial Instruments". This new standard requires financial assets measured at amortized cost be presented at the net amount expected to be collected, through an allowance for credit losses that is deducted from the amortized cost basis. This standard will be effective for the Company beginning January 1, 2020, with early application permitted. We are evaluating the impact of adopting this new accounting standard on our consolidated financial statements.

In January 2017, FASB issued ASU No. 2017-01, "Business Combinations (Topic 805) Clarifying the Definition of Business". ASU No. 2017-01 clarifies the definition of a business with the objective of adding guidance to assist entities with evaluating whether transactions should be accounted for as acquisitions (or disposals) of assets or businesses. The update to the standard is effective for interim and annual periods beginning after December 15, 2017, and applied prospectively. We do not expect the adoption of this standard will have a material impact on the consolidated financial statements.

In January 2017, the FASB issued ASU No. 2017-04, "Simplifying the Test for Goodwill Impairment (Topic 350)". This standard eliminates the second step from the goodwill impairment test, and instead requiring an entity to recognize a goodwill impairment charge for the amount by which the goodwill carrying amount exceeds the reporting unit's fair value. This standard is effective for interim and annual goodwill impairment tests in fiscal years beginning after December 15, 2019 with early adoption permitted. This standard must be applied on a prospective basis. We are currently evaluating the potential effect of the standard on our consolidated financial statements.

In May 2017, the FASB issued ASU 2017-09, changing the terms or conditions of a share-based payment award must be accounted for as modifications. Entities will apply the modification accounting guidance if the value, vesting conditions or classifications of the award changes. The standard also clarifies that a modification to an award could be significant and therefore require disclosure, even if modification accounting is not required. Therefore, an entity will have to make all of the disclosures about modifications that are required today, in addition to disclosing that the compensation expense has not change. This standard is effective for interim and fiscal years beginning after December 15, 2017 with early adoption permitted. This standard must be applied on a prospective basis. We do not expect the adoption of this standard will have a material impact on our consolidated financial statements.

For information with respect to ASU No. 2014-09 and other recent accounting pronouncements, see Note 2(aa) and Note 2(ab) to our consolidated financial statements included in this annual report.

Results of Operations

The following discussion of our results of operations for the years ended December 31, 2017, 2016 and 2015, including the following tables, which present selected financial information data in dollars and as a percentage of total revenues, are based upon our statements of operations contained in our financial statements for those periods, and the related notes, included in this annual report.

The following table sets forth, for the periods indicated, certain financial data concerning our operating results:

	2017	2016	2015
	(U.S. $ in thousands)		
Revenues:			
Products	$117,968	$110,186	$136,793*
Services	93,401	86,399	79,773 *
	211,369	196,585	216,566
Cost of revenues:			
Products	30,862	27,320	29,159
Services	8,754	8,375	9,041
	39,616	35,695	38,200
Gross profit	171,753	160,890	178,366
Operating expenses, net:			
Research and development, net	59,003	51,732	49,987
Sales and marketing	108,744	103,774	93,347
General and administrative	17,577	18,133	17,033
Other income	(6,900)	-	-
Total operating expenses	178,424	173,639	160,367
Operating income (loss)	(6,671)	(12,749)	17,999
Financial income, net	4,830	5,741	5,867
Income (loss) before taxes on income	(1,841)	(7,008)	23,866
Taxes on income	(5,652)	(1,651)	(5,297)
Net income (loss)	(7,493)	(8,659)	18,569

The breakdown between product and service revenues for 2015 was reclassified to include most subscription revenues in product revenues rather than allocating some to product and some to service revenues, which has resulted in a change to previously published figures for the period ended December 31, 2015.

The following table sets forth, for the periods indicated, certain financial data expressed as a percentage of our total revenues:

	2017	2016	2015
Revenues:			
Products	56 %	56 %	63 %
Services	44	44	37
	100	100	100
Cost of Revenues:			
Products	15	14	13
Services	4	4	4
	19	18	18
Gross profit	81	82	82
Operating expenses, net:			
Research and development, net	28	26	23
Sales and marketing	51	53	43
General and administrative	8	9	8
Other income	(3)	-	-
Total operating expenses	84	88	74
Operating income (loss)	(3)	(6)	8
Financial income, net	2	3	3
Income (loss) before taxes on income	(1)	(3)	11
Taxes on income	(3)	(1)	(2)
Net income (loss)	(4)%	(4)%	9 %

Comparison of Years Ended December 31, 2017, 2016 and 2015

Revenues.

Our revenues are derived from sales of our products and services. We recognize product revenue when persuasive evidence of an arrangement exists, delivery has occurred, the fee is fixed or determinable, no further obligation exists and collectability is probable. Subscriptions revenues and post-contract customer support, which represents mainly software update subscriptions, help-desk support and unit repairs or replacements, are recognized ratably over the contract or subscription period.

We operate in one reportable market segment and our revenues are attributed to geographic areas based on the location of the end-users.

Sales in 2017 were $211.4 million compared with sales of $196.6 million in 2016, an increase of 7.5%.

Sales in 2016 were $196.6 million compared with sales of $216.6 million in 2015, a decrease of 9%.

The following table provides a breakdown of our revenues (dollars in thousands) by type of revenues both in dollars and as a percentage of total revenues for the past three fiscal years, as well as the percentage change between such periods:

	2017		2016		2015		% Change 2017 vs. 2016	% Change 2016 vs. 2015
Products	117,968	56 %	110,186	56 %	136,793*	63 %	7 %	(19)%
Services	93,401	44 %	86,399	44 %	79,773 *	37 %	8 %	8 %
Total	211,369	100%	196,585	100%	216,566	100%	8 %	(9)%

*The breakdown between product and service revenues for 2015 was reclassified to include most subscription revenues in product revenues rather than allocating some to product and some to service revenues, which has resulted in a change to previously published figures for the period ended December 31, 2015.

The following table shows a breakdown of our total revenues (dollars in thousands) by geographical distribution both in dollars and as a percentage of total revenues for the past three fiscal years, as well as the percentage change between such periods:

	2017		2016		2015		% Change 2017 vs. 2016	% Change 2016 vs. 2015
North, Central and South America (principally the United States)(*)	97,901	46 %	84,733	43 %	88,685	41 %	16 %	(4)%
EMEA (Europe, the Middle East and Africa)	56,589	27 %	53,724	27 %	62,689	29 %	5 %	(14)%
Asia-Pacific	56,879	27 %	58,128	30 %	65,192	30 %	(2)%	(11)%
Total	211,369	100%	196,585	100%	216,566	100%	8 %	(9)%

(*) For the years ended December 31, 2017, 2016 and 2015, our revenues from the United States were $78.5 million, $68.0 million and $69.1 million, respectively, representing 37%, 35% and 32% of total revenues for these years, respectively.

Other than the United States, no other single country accounted for more than 10% of our sales for the years ended December 31, 2017, 2016 and 2015.

In 2017, our product revenues increased by 7%, to $118.0 million, compared to $110.2 million in 2016. The increase in our product revenues is mainly attributed to an increase in our product sales and greater contribution from our previous years' subscription deferred revenues which matured into revenues in 2017.

In 2017, our service sales increased by 8% to $93.4 million, compared to $86.4 million in 2016. This increase in service sales is mainly attributed to renewals of existing support contracts and sales of new support contracts.

During 2017, our revenues from the enterprise market represented approximately 66%, whereas revenues from the carrier market represented approximately 34% of our revenues, compared to 69% and 31%, respectively, in 2016.

Our revenues in the Americas increased in 2017 by $13.0 million compared to 2016, or 16% year-over-year, mainly due to greater demand for cloud based security solutions. Revenues from the EMEA region increased by 5% compared to 2016. Revenues in Asia-Pacific region decreased by 2% due to change in our sales model which is reflected by the shift to subscription sales which resulted lower revenue recognition.

In 2016, our product sales decreased by 19%, to $110.2 million, compared to $136.8 million in 2015. The decrease in our product sales is attributed to a gradual change in our sales model which is reflected by the shift to subscription sales format as well as challenging conditions in our international business.

In 2016, our service sales increased by 8% to $86.4 million, compared to $79.8 million in 2015. This increase in service sales is attributed primarily to (1) the continued growth of our installed base and (2) an increase in our service offerings.

During 2016, our revenues (excluding revenues derived from the Radyoos web-based e-commerce platform) from the enterprise market represented approximately 69%, whereas revenues from the carrier market represented approximately 31% of our revenues, compared to 71% and 29%, respectively, in 2015.

Our revenues in the Americas in 2016 decreased by $4.0 million compared to 2015, or 4% year-over-year, mainly as a result of the shift to subscription sales format which resulted in a longer period for revenue recognition. The EMEA region experienced a decline of 14% compared to 2015. The decrease was primarily due to lower products revenue resulting from the shift to subscription sales as well as a result of overall soft market conditions. Revenues from the Asia-Pacific region decreased by $7.1 million, or 11% year- over-year, mainly due to challenging conditions in some of the major countries, mainly in China, Japan and Australia.

Cost of Revenues.

Cost of revenues refers to both products and service revenues and consists primarily of the cost of circuit boards and other components required for the assembly of our products, salaries and related personnel expenses for those engaged in the final assembly and in providing support and maintenance service of our products, amortization of acquired technology and other overhead costs.

The following table sets forth a breakdown of our cost of revenues between products and services for the periods indicated, in absolute figures (dollars in thousands) and as a percentage of the relative product and services revenues:

	2017		2016		2015	
Cost of Products	30,862	26.2%	27,320	24.8%	$29,159	21.3%
Cost of Services	8,754	9.4 %	8,375	9.7 %	9,041	11.3%
Total	39,616	18.7%	35,695	18.2%	$38,200	17.6%

Cost of products sales as a percentage of products sales increased from 24.8% in 2016 to 26.2% in 2017. Cost of products sales in 2017 and 2016 included amortization of intangible assets in the amount of $1.1 and $1.0 million, respectively. Our cost of products sales as a percentage of products sales, excluding amortization of intangible assets, represented approximately 25.2% of products sales in 2017, compared to 23.9% in 2016. The increase in cost of products sales as a percentage of products sales is mainly due to different sales mix of our products, cost of operating our cloud infrastructure and expanding our global logistic footprint to support our global maintenance and support commitments.

Cost of sales related to services as a percentage of service revenues in 2017 was 9.4% compared to 9.7% in 2016.

Cost of products sales as a percentage of products sales increased year-over-year from 21.3% in 2015 to 24.8% in 2016. Cost of products sales in 2016 and 2015 included amortization of intangible assets in the amount of $1.0 and $1.1 million, respectively. Our cost of products sales as a percentage of products sales, excluding amortization of intangible assets, represented approximately 23.9% of products sales in 2016, compared to 20.5% in 2015. The increase in cost of products sales as a percentage of products sales is mainly due to different sales mix of our products coupled with stronger competition in some of the regions.

Cost of sales related to services as a percentage of service revenues in 2016 was 9.7% compared to 11.3% in 2015. The reason for the decrease is mainly due to the fact that a major portion of the cost of services is fixed (mainly salaries of technical personnel) while the increase in sales did not correlate into the same rate of increase in costs.

Operating Expenses.

The following table sets forth a breakdown of our operating expenses (dollars in thousands) for the periods indicated as well as the percentage change between such periods:

2017	2016	2015	% Change 2017 vs. 2016