CHECK POINT SOFTWARE TECHNOLOGIES LTD
Form 20-F
April 28, 2016
Table of Contents

UNITED STATES

SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 20-F

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

OR

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

For the fiscal year ended December 31, 2015

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 000-28584

CHECK POINT SOFTWARE TECHNOLOGIES LTD.

(Exact name of Registrant as specified in its charter)

ISRAEL

(Jurisdiction of incorporation or organization)

5 Ha Solelim Street, Tel Aviv 6789705, Israel

(Address of principal executive offices)

John Slavitt, Esq.

General Counsel

Check Point Software Technologies, Inc.

959 Skyway Road, Suite 300

San Carlos, CA 94070 U.S.A.

Tel: (650) 628-2110

Fax: (650) 649-1975

(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 exchange on which registered
Ordinary shares, NIS 0.01 nominal value	NASDAQ Global Select Market

Securities registered or to be registered pursuant to Section 12(g) of the Act. None

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

Indicate the number of outstanding shares of each of the issuer s classes of capital or common stock as of December 31, 2015. 174,901,523 Ordinary Shares, nominal value NIS 0.01 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 x 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 x

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 x 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 x No ¨

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, or a non-accelerated filer. See definitions of accelerated filer and large accelerated filer in Rule 12b-2 of the Exchange Act.

Large Accelerated filer x Accelerated filer ¨ Non-accelerated filer ¨

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

x 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 x

Table of Contents

Currency of Presentation and Certain Defined Terms

In this Annual Report on Form 20-F, references to U.S. or United States are to the United States of America, its territories and possessions; and references to Israel are to the State of Israel. References to $, dollar or U.S. dollar a to the legal currency of the United States of America; references to NIS or Israeli shekel are to the legal currency of Israel; references to Euro are to the legal currency of the European Union; and references to Swedish Krona are to the legal currency of the Kingdom of Sweden. Our financial statements are presented in U.S. dollars and are prepared in conformity with accounting principles generally accepted in the United States of America, or U.S. GAAP.

All references to we, us, our or Check Point shall mean Check Point Software Technologies Ltd., and, unless specifically indicated otherwise or the context indicates otherwise, our consolidated subsidiaries.

Forward-Looking Statements

Some of the statements contained in this Annual Report on Form 20-F are forward-looking statements that involve risks and uncertainties. The statements contained in this Annual Report on Form 20-F that are not purely historical are forward-looking statements within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended, including, without limitation, statements regarding: our expectations for our business, trends related to our business and the markets in which we operate and into which we sell products; future amounts and sources of our revenue; our future costs and expenses; the adequacy of our capital resources; our expectations with respect to share repurchases by us and dividend payments by us; our ongoing relationships with our current and future customers and channel partners; and our other expectations, beliefs, intentions and strategies. In some cases, you can identify forward-looking statements by terminology, such as may, will, could, should, expects, plans, anticipates, believes, intends, estimates, predicts, potential, negative of these terms or other comparable terminology. These statements are subject to known and unknown risks, uncertainties and other factors, which may cause our actual results to differ materially from those implied by the forward-looking statements. Many of these risks, uncertainties and assumptions are described in the risk factors set forth in Item 3 Key Information Risk Factors and elsewhere in this Annual Report on Form 20-F. All forward-looking statements included in this Annual Report on Form 20-F, are based on information available to us on the date of the filing. We undertake no obligation to update or revise any of the forward-looking statements after the date of the filing, except as required by applicable law.

Table of Contents

TABLE OF CONTENTS

PART I

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

Selected Financial Data

We prepare our historical consolidated financial statements in accordance with U.S. GAAP. The selected financial data, set forth in the table below, have been derived from our audited historical financial statements for each of the years from 2011 to 2015. The selected consolidated statement of income data for the years 2013, 2014 and 2015, and the selected consolidated balance sheet data at December 31, 2014 and 2015, have been derived from our audited consolidated financial statements set forth in Item 18 Financial Statements. The selected consolidated statement of income data for the years 2011 and 2012, and the selected consolidated balance sheet data at December 31, 2011, 2012, and 2013, have been derived from our previously published audited consolidated financial statements, which are not included in this Annual Report on Form 20-F. These selected financial data should be read in conjunction with our consolidated financial statements, as set forth in Item 18, and are qualified entirely by reference to such consolidated financial statements.

Table of Contents

	Year ended December 31,				
	2015	2014	2013	2012	2011
	(in thousands)				
Consolidated Statements of Income Data:					
Revenues	$ 1,629,838	$ 1,495,816	$ 1,394,105	$ 1,342,695	$ 1,246,986
Operating expenses (*):					
Cost of revenues	189,057	176,541	162,634	159,161	175,683
Research and development	149,279	133,300	121,764	111,911	110,147
Selling and marketing	359,804	306,363	276,067	255,345	253,800
General and administrative	91,981	78,558	72,735	69,743	65,182
Restructuring and other acquisition related costs					
Total operating expenses	790,121	694,762	633,200	596,160	604,812
Operating income	839,717	801,054	760,905	746,535	642,174
Financial income, net	34,073	28,762	34,931	40,332	41,040
Income before taxes on income	873,790	829,816	795,836	786,867	683,214
Taxes on income	187,924	170,245	143,036	166,867	139,248
Net income	$ 685,866	$ 659,571	$ 652,800	$ 620,000	$ 543,966
Basic earnings per ordinary share	$ 3.83	$ 3.50	$ 3.34	$ 3.04	$ 2.63
Shares used in computing basic earnings per ordinary share	179,218	188,487	195,647	203,918	206,917
Diluted earnings per ordinary share	$ 3.74	$ 3.43	$ 3.27	$ 2.96	$ 2.54
Shares used in computing diluted earnings per ordinary share	183,619	192,300	199,487	209,170	213,922

(*) Including pre-tax charges for stock based compensation, amortization of intangible assets and acquisition related expenses in the following items:

Amortization of intangible assets and acquisition related expenses					
Cost of revenues	$ 1,808	$ 240	$ 612	$ 3,982	$ 31,171
Research and development	6,146				
Selling and marketing	3,267	1,866	2,408	3,046	12,754
Stock-based compensation					
Cost of revenues	$ 1,585	$ 1,090	$ 1,048	$ 829	$ 967
Research and development	11,544	9,284	9,001	8,594	7,471
Selling and marketing	16,351	13,339	11,193	9,677	7,888
General and administrative	46,822	39,456	29,870	26,187	23,509

	December 31,				
	2015	2014	2013	2012	2011
	(in thousands)				
Consolidated Balance Sheet Data:					

Working capital	$ 678,981	$ 780,825	$ 617,520	$ 1,061,143	$ 1,007,533
Total assets	5,069,880	4,948,818	4,886,437	4,544,885	4,128,063
Shareholders equity	3,531,866	3,637,559	3,602,097	3,346,309	3,073,091
Capital stock	988,105	859,898	775,691	693,986	631,282

Table of Contents

Risk Factors

An investment in our ordinary shares involves a high degree of risk. The risks and uncertainties described below are not the only ones we face. Additional risks and uncertainties that we are unaware of, or that we currently believe are not material, also may become important factors that affect us. If any of the following risks materialize, our business, financial condition, results of operations and prospects could be materially harmed. In that event, the market price of our ordinary shares could decline and you could lose part or all of your investment.

Risks Related to Our Business and Our Market

If the market for information and network security solutions does not continue to grow, our business will be adversely affected

The market for information and network security solutions may not continue to grow. Continued growth of this market will depend, in large part, upon:

- the continued expansion of Internet usage and the number of organizations adopting or expanding intranets;
- the continued adoption of cloud infrastructure by organizations;
- the ability of the infrastructures implemented by organizations to support an increasing number of users and services;
- the continued development of new and improved services for implementation across the Internet and between the Internet and intranets;
- the adoption of data security measures as it pertains to data encryption and data loss prevention technologies;
- government regulation of the Internet and governmental and non-governmental requirements and standards with respect to data security and privacy; and
- general economic conditions in the markets in which we, our customers and our suppliers operate.

In 2015, global and regional economies around the world and financial markets, remained volatile as a result of a multitude of factors, including adverse credit conditions, changes in economic activity, concerns about inflation and deflation, fluctuating energy costs, decreased consumer confidence, reduced capital spending, adverse business conditions and liquidity concerns and other factors. During this period, many organizations limited their expenditures and a significant portion of such organizations have remained reluctant to increase expenditures. If challenging economic conditions continue or worsen, it may cause our customers to reduce or postpone their technology spending significantly, which could result in reductions in sales of our products, longer sales cycles, slower adoption of new technologies and increased price competition.

Further, if the necessary infrastructure or complementary products and services are not developed in a timely manner and, consequently, the enterprise security, data security, Internet or intranet markets fail to grow or grow more slowly than we currently anticipate, our business, operating results and financial condition may be materially adversely affected. Additional details are provided in Item 4 Information on Check Point.

We may not be able to successfully compete, which could adversely affect our business and results of operations

The market for information and network security solutions is intensely competitive and we expect that competition will continue to increase in the future. Our competitors include Cisco Systems, Inc., Juniper Networks, Inc., Fortinet Inc., SonicWall Inc. (owned by Dell Inc.), Palo Alto Networks, Inc., WatchGuard Technologies, Inc., McAfee, Inc. (owned by Intel Corporation), Sourcefire, Inc. (owned by Cisco Systems Inc.), and other companies in the network security space. We also compete with several other companies, including Microsoft Corporation, Symantec Corporation, International Business Machines Corporation, Hewlett-Packard, FireEye, Inc. and Websense Inc. with respect to specific products that we offer. There are hundreds of small and large companies that offer security products and services that we may compete with from time to time.

Some of our current and potential competitors have various advantages over us, including longer operating histories; access to larger customer bases; significantly greater financial, technical and marketing resources; a broader portfolio of products, applications and services; and larger patent and intellectual property portfolios. As a result, they may be able to adapt better than we can to new or emerging technologies and changes in customer requirements, or to devote greater resources to the promotion and sale of their products. Furthermore, some of our competitors with more diversified product portfolios and larger customer bases may be better able to withstand a reduction in spending on information and network security solutions, as well as a general slowdown or recession in economic conditions in the markets in which they operate. In addition, some of our competitors have greater financial resources than we do, and they have offered, and in the future may offer, their products at lower prices than we do, or may bundle security products with their other offerings, which may cause us to lose sales or to reduce our prices in response to competition.

Table of Contents

In addition, consolidation in the markets in which we compete may affect our competitive position. This is particularly true in circumstances where customers are seeking to obtain a broader set of products and services than we are able to provide.

The markets in which we compete also include many niche competitors, generally smaller companies at a relatively early stage of operations, which are focused on specific Internet and data security needs. These companies specialized focus may enable them to adapt better than we can to new or emerging technologies and changes in customer requirements in their specific areas of focus. In addition, some of these companies can invest relatively large resources on very specific technologies or customer segments. The effect of these companies activities in the market may result in price reductions, reduced gross margins and loss of market share, any of which will materially adversely affect our business, operating results and financial condition.

Further, vendors of operating system software, networking hardware or central processing units, or CPUs, may enhance their products to include functionality that is currently provided by our products. The widespread inclusion of similar functionality to that which is offered by our solutions, as standard features of operating system software and networking hardware could significantly reduce the demand for our products, particularly if the quality of such functionality were comparable to that of our products. Furthermore, even if the network or application security functionality provided as standard features by operating systems software and networking hardware is more limited than that of our solutions, a significant number of customers may elect to accept more limited functionality in lieu of purchasing additional products.

We may not be able to continue competing successfully against our current and future competitors, and increased competition may result in price reductions, reduced gross margins and operating margins, reduced net income, and loss of market share, any of which will materially adversely affect our business, operating results and financial condition. For additional information, see Item 4 Information on Check Point.

If we fail to enhance our existing products, develop or acquire new and more technologically advanced products, or fail to successfully commercialize these products, our business and results of operations will suffer

The information and network security industry is characterized by rapid technological advances, changes in customer requirements, frequent new product introductions and enhancements, and evolving industry standards in computer hardware and software technology. In particular, the markets for data security, Internet and intranet applications are rapidly evolving. As a result, we must continually change and improve our products in response to changes in operating systems, application software, computer and communications hardware, networking software, programming tools, and computer language technology. We must also continually change our products in response to changes in network infrastructure requirements, including the expanding use of cloud computing. Further, we must continuously improve our products to protect our customers data and networks from evolving security threats.

Our future operating results will depend upon our ability to enhance our current products and to develop and introduce new products on a timely basis; to address the increasingly sophisticated needs of our customers; and to keep pace with technological developments, new competitive product offerings, and emerging industry standards. Our competitors introduction of products embodying new technologies and the emergence of new industry standards may render our existing products obsolete or unmarketable. While we have historically been successful in developing, acquiring, and marketing new products and product enhancements that respond to technological change and evolving industry standards, we may not be able to continue to do so. In addition, we may experience difficulties that could delay or prevent the successful development, introduction, and marketing of these products, as well as the integration of acquired products. Furthermore, our new products or product enhancements may not adequately meet the requirements of the marketplace or achieve market acceptance. In some cases, a new product or product enhancements

may negatively affect sales of our existing products. If we do not respond adequately to the need to develop and introduce new products or enhancements of existing products in a timely manner in response to changing market conditions or customer requirements, our business, operating results and financial condition may be materially adversely affected. For additional information, see Item 4 Information on Check Point and under the caption We may not be able to successfully compete, which could adversely affect our business and results of operations in this Item 3 Key Information Risk Factors.

If our products fail to protect against attacks and our customers experience security breaches, our reputation and business could be harmed

Hackers and other malevolent actors are increasingly sophisticated, often affiliated with organized crime and operate large scale and complex attacks. In addition, their techniques change frequently and generally are not recognized until launched against a target. 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 customers high-value business data, our business and reputation will suffer.

Table of Contents

In addition, an actual or perceived security breach or theft of the sensitive data of one of our customers, regardless of whether the breach is attributable to the failure of our products, could adversely affect the market s perception of our security products. Despite our best efforts, there is no guarantee that our products will be free of flaws or vulnerabilities, and even if we discover these weaknesses we may not be able to correct them promptly, if at all. Our customers may also misuse our products, which could result in a breach or theft of business data.

Product defects may increase our costs and impair the market acceptance of our products and technology

Our products are complex and must meet stringent quality requirements. They may contain undetected hardware or software errors or defects, especially when new or acquired products are introduced or when new versions are released. In particular, the personal computer hardware environment is characterized by a wide variety of non-standard configurations that make pre-release testing for programming or compatibility errors very difficult and time-consuming. We may need to divert the attention of our engineering personnel from our research and development efforts to address instances of errors or defects.

Our products are used to deploy and manage Internet security and protect information, which may be critical to organizations. As a result, the sale and support of our products entails the risk of product liability and related claims. We do not know whether, in the future, we will be subject to liability claims or litigation for damages related to product errors, or will experience delays as a result of these errors. Our sales agreements and product licenses typically contain provisions designed to limit our exposure to potential product liability or related claims. In selling our products, we rely primarily on shrink wrap licenses that are not signed by the end user, and for this and other reasons, these licenses may be unenforceable under the laws of some jurisdictions. As a result, the limitation of liability provisions contained in these licenses may not be effective. Although we maintain product liability insurance for most of our products, the coverage limits of these policies may not provide sufficient protection against an asserted claim. If litigation were to arise, it could, regardless of its outcome, result in substantial expense to us, significantly divert the efforts of our technical and management personnel, and disrupt or otherwise severely impact our relationships with current and potential customers. In addition, if any of our products fail to meet specifications or have reliability, quality or compatibility problems, our reputation could be damaged significantly and customers might be reluctant to buy our products, which could result in a decline in revenues, a loss of existing customers, and difficulty attracting new customers. *We are subject to risks relating to acquisitions*

We have made acquisitions in the past and we may make additional acquisitions in the future. The pursuit of acquisitions may divert the attention of management and cause us to incur various expenses in identifying, investigating, and pursuing suitable acquisitions, whether or not they are consummated.

Competition within our industry for acquisitions of businesses, technologies, assets and product lines has been, and may in the future continue to be, intense. As such, even if we are able to identify an acquisition that we would like to consummate, we may not be able to complete the acquisition on commercially reasonable terms or because the target is acquired by another company. Furthermore, in the event that we are able to identify and consummate any future acquisitions, we could:

- issue equity securities which would dilute current shareholders percentage ownership;
- incur substantial debt;

assume contingent liabilities; or

expend significant cash.

These financing activities or expenditures could harm our business, operating results and financial condition or the price of our ordinary shares. Alternatively, due to difficulties in the capital and credit markets, we may be unable to secure capital on acceptable terms, or at all, to complete acquisitions.

In addition, if we acquire additional businesses, we may not be able to integrate the acquired personnel, operations, and technologies successfully or effectively manage the combined business following the completion of the acquisition. We may also not achieve the anticipated benefits from the acquired business due to a number of factors, including:

unanticipated costs or liabilities associated with the acquisition;

incurrence of acquisition-related costs;

diversion of management s attention from other business concerns;

harm to our existing business relationships with manufacturers, distributors and customers as a result of the acquisition;

the potential loss of key employees;

use of resources that are needed in other parts of our business;

Table of Contents

use of substantial portions of our available cash to consummate the acquisition; or

unrealistic goals or projections for the acquisition.

Moreover, even if we do obtain benefits from acquisitions in the form of increased sales and earnings, there may be a delay between the time when the expenses associated with an acquisition are incurred and the time when we recognize such benefits.

We are dependent on a small number of distributors

We derive our sales primarily through indirect channels. During 2015, 2014 and 2013, we derived approximately 53%, 54% and 57%, respectively, of our sales from our ten largest distributors. In 2015, 2014 and 2013, our two largest distributors accounted for approximately 38%, 37% and 30% of our sales. We expect that a small number of distributors will continue to generate a significant portion of our sales. Furthermore, there has been an industry trend toward consolidation among distributors, and we expect this trend to continue in the near future which could further increase our reliance on a small number of distributors for a significant portion of our sales. If these distributors reduce the amount of their purchases from us for any reason, including because they choose to focus their efforts on the sales of the products of our competitors, our business, operating results and financial condition could be materially adversely affected.

Our future success is highly dependent upon our ability to establish and maintain successful relationships with our distributors. In addition, we rely on these entities to provide many of the training and support services for our products and equipment. Accordingly, our success depends in large part on the effective performance of these distributors. Recruiting and retaining qualified distributors and training them in our technology and products requires significant time and resources. Further, we have no minimum purchase commitments with any of our distributors, and our contracts with these distributors do not prohibit them from offering products or services that compete with ours. Our competitors may be effective in providing incentives to existing and potential distributors to favor their products or to prevent or reduce sales of our products. Our distributors may choose not to offer our products exclusively or at all. Our failure to establish and maintain successful relationships with distributors would likely materially adversely affect our business, operating results and financial condition.

We purchase several key components and finished products from limited sources, and we are increasingly dependent on contract manufacturers for our hardware products.

Many components, subassemblies and modules necessary for the manufacture or integration of our hardware products are obtained from a limited group of suppliers. Our reliance on sole or limited suppliers, particularly foreign suppliers, and our reliance on subcontractors involves several risks, including a potential inability to obtain an adequate supply of required components, subassemblies or modules and limited control over pricing, quality and timely delivery of components, subassemblies or modules. Although we have been successful in the past, replacing suppliers may be difficult and it is possible it could result in an inability or delay in producing designated hardware products. Substantial delays could have a material adverse impact on our business.

Managing our supplier and contractor relationships is particularly difficult during time periods in which we introduce new products and during time periods in which demand for our products is increasing, especially if demand increases more quickly than we expect. We also have extended support contracts with these suppliers and are dependent on their ability to perform over a period of years.

We are dependent on a limited number of product families

Currently, we derive the majority of our revenues from sales of integrated appliances and Internet security products, as well as related revenues from subscriptions and from software updates and maintenance. We expect that this concentration of revenues from a small number of product families will continue for the foreseeable future. Endpoint security products and associated software updates, maintenance and subscriptions represent an additional revenue source. Our future growth depends heavily on our ability to effectively develop and sell new and acquired products as well as add new features to existing products. For more details, see Item 4 Information on Check Point and Item 5 Operating and Financial Review and Prospects.

We incorporate third party technology in our products, which may make us dependent on the providers of these technologies and expose us to potential intellectual property claims

Our products contain certain technology that we license from other companies. Third party developers or owners of technologies may not be willing to enter into, or renew, license agreements with us regarding technologies that we may wish to incorporate in our products, either on acceptable terms or at all. If we cannot obtain licenses to these technologies, we may be at a disadvantage compared with our competitors who are able to license these technologies. In addition, when we do obtain licenses to third party technologies that we did not develop, we may have little or no ability to determine in advance whether the technology infringes the intellectual property rights of others. Our suppliers and licensors may not be required or may not be able to indemnify us

Table of Contents

in the event that a claim of infringement is asserted against us, or they may be required to indemnify us only up to a maximum amount, above which we would be responsible for any further costs or damages. Any failure to obtain licenses to intellectual property or any exposure to liability as a result of incorporating third party technology into our products could materially and adversely affect our business, operating results and financing condition.

We incorporate open source technology in our products which may expose us to liability and have a material impact on our product development and sales

Some of our products utilize open source technologies. These technologies are licensed to us under varying license structures, including the General Public License. If we have improperly used, or in the future improperly use software that is subject to such licenses with our products, in such a way that our software becomes subject to the General Public License, we may be required to disclose our own source code to the public. This could enable our competitors to eliminate any technological advantage that our products may have over theirs. 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 impact our business, results of operations and financial condition.

We are the defendants in various lawsuits and have been subject to tax disputes and governmental proceedings, which could adversely affect our business, results of operations and financial condition

As a global company we are subject to taxation in Israel, the United States and various other countries and states, and accordingly attempt to utilize an efficient operating model to structure 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 different parts of the world.

In 2015, the Organization for Economic Co-operation and Development, or OECD, published final proposals under its Base Erosion and Profit Shifting, or BEPS, Action Plan. The BEPS Action Plan includes fifteen Actions to address BEPS in a comprehensive manner and represents a significant change to the international corporate tax landscape. These proposals, if adopted by countries, may increase tax uncertainty and adversely affect our provision for income taxes.

In addition, we are subject to the continuous examination of our income tax returns by tax authorities around the world. It is possible that tax authorities may disagree with certain positions we have taken and any adverse outcome of such a review or audit could have a negative effect on our financial position and operating results. We regularly assess the likelihood of adverse outcomes resulting from these examinations to determine the adequacy of our provision for income taxes, but the determination of our worldwide provision for income taxes and other tax liabilities requires significant judgment by management, and there are transactions where the ultimate tax determination is uncertain. Although we believe that our estimates are reasonable, the ultimate tax outcome may differ from the amounts recorded in our consolidated financial statements and may materially affect our financial results in the period or periods for which such determination is made. There can be no assurance that the outcomes from continuous examinations will not have an adverse effect on our business, financial condition and results of operations.

We are the defendant in various other lawsuits, including employment-related litigation claims, construction claims and other legal proceedings in the normal course of our business. Litigation and governmental proceedings can be expensive, lengthy and disruptive to normal business operations, and can require extensive management attention and resources, regardless of their merit. We will continue to vigorously assert and protect their interests in these lawsuits. While we currently intend to defend the aforementioned matters vigorously, we cannot predict the results of complex legal proceedings, and an unfavorable resolution of a lawsuit or proceeding could materially adversely affect our business, results of operations and financial condition. See also Item 8 Financial Information under the caption Legal

Proceedings.

In November 2013, we reached a settlement agreement (the Settlement Agreement), with the Israeli Tax Authorities (ITA) for years 2002 through 2011 and accordingly, we and the ITA notified the court that they have reached an agreement outside of the court and obtained the court s approval (see Note 12 of our Consolidated Financial Statements).

Class action litigation due to stock price volatility or other factors could cause us to incur substantial costs and divert our management s attention and resources

In the past, following periods of volatility in the market price of a public company s securities, securities class action litigation has often been instituted against that company. Companies such as ours in the technology industry are particularly vulnerable to this kind of litigation as a result of the volatility of their stock prices. We have been named as a defendant in this type of litigation in the past. Any litigation of this sort could result in substantial costs and a diversion of management s attention and resources.

Table of Contents

We may not be able to successfully protect our intellectual property rights

We seek to protect our proprietary technology by relying on a combination of statutory as well as common law copyright and trademark laws, trade secrets, confidentiality procedures and contractual provisions as indicated below in the section entitled Proprietary Rights in Item 4 Information on Check Point. We have certain patents in the United States and in several other countries, as well as pending patent applications. We cannot assure you that pending patent applications will be issued, either at all or within the scope of the patent claims that we have submitted. In addition, someone else may challenge our patents and these patents may be found invalid. Furthermore, others may develop technologies that are similar to or better than ours, or may work around any patents issued to us. Despite our efforts to protect our proprietary rights, others may copy aspects of our products or obtain and use information that we consider proprietary. In addition, the laws of some foreign countries do not protect our proprietary rights to the same extent as the laws of the United States, Israel or Sweden. Our efforts to protect our proprietary rights may not be adequate and our competitors may independently develop technology that is similar to our technology. If we are unable to secure, protect and enforce our intellectual property rights, such failure could harm our brand and adversely impact our business, financial condition and results of operations.

If a third-party asserts that we are infringing its intellectual property, whether successful or not, it could subject us to costly and time-consuming litigation or expensive licenses, which could harm our business

There is considerable patent and other intellectual property development activity in our industry. Our success depends, in part, upon our ability not to infringe upon the intellectual property rights of others. Our competitors, as well as a number of other entities and individuals, own or claim to own intellectual property relating to our industry. From time to time, third parties have brought, and continue to bring, claims that we are infringing upon their intellectual property rights, and we may be found to be infringing upon such rights. In addition, third-parties have in the past sent us correspondence claiming that we infringe upon their intellectual property, and in the future we may receive claims that our products infringe or violate their intellectual property rights. Furthermore, we may be unaware of the intellectual property rights of others that may cover some or all of our technology or products. Any claims or litigation could cause us to incur significant expenses and, if successfully asserted against us, could require that we pay substantial damages or royalty payments, prevent us from selling our products, or require that we comply with other unfavorable terms. In addition, we may decide to pay substantial settlement costs and/or licensing fees in connection with any claim or litigation, whether or not successfully asserted against us. Even if we were to prevail, any disputes or litigation regarding intellectual property matters could be costly and time-consuming and divert the attention of our management and key personnel from our business operations. As such, third-party claims with respect to intellectual property may increase our cost of goods sold or reduce the sales of our products, and may have a material and adverse effect on our business.

We are exposed to various legal, business, political and economic risks associated with international operations; these risks could increase our costs, reduce future growth opportunities and affect our operating results

We operate our business primarily from Israel, we sell our products worldwide, and we generate a significant portion of our revenue outside the United States. We intend to continue to expand our international operations, which will require significant management attention and financial resources. In order to continue to expand worldwide, we will need to establish additional operations, hire additional personnel and recruit additional channel partners, internationally. To the extent that we are unable to do so effectively, our growth is likely to be limited and our business, operating results and financial condition may be materially adversely affected.

Our international sales and operations subject us to many potential risks inherent in international business activities, including, but not limited to:

technology import and export license requirements;

costs of localizing our products for foreign countries, and the lack of acceptance of localized products in foreign countries;

trade restrictions;

imposition of or increases in tariffs or other payments on our revenues in these markets;

greater difficulty in protecting intellectual property;

difficulties in managing our overseas subsidiaries and our international operations;

declines in general economic conditions;

political instability and civil unrest which could discourage investment and complicate our dealings with governments;

difficulties in complying with a variety of foreign laws and legal standards and changes in regulatory requirements;

Table of Contents

expropriation and confiscation of assets and facilities;

difficulties in collecting receivables from foreign entities or delayed revenue recognition;

recruiting and retaining talented and capable employees;

differing labor standards;

increased tax rates;

potentially adverse tax consequences, including taxation of a portion of our revenues at higher rates than the tax rate that applies to us in Israel;

fluctuations in currency exchange rates and the impact of such fluctuations on our results of operations and financial position; and

the introduction of exchange controls and other restrictions by foreign governments.

These difficulties could cause our revenues to decline, increase our costs or both. This is also specifically tied to currency exchange rates which has an impact on our financial statements based on currency rate fluctuations.

Compliance with new and changing corporate governance and public disclosure requirements adds uncertainty to our compliance policies and increases our costs of compliance

Changing laws, regulations and standards relating to accounting, corporate governance and public disclosure, including the Sarbanes-Oxley Act of 2002, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank), new SEC regulations, new amendments to the Israeli Companies Law and NASDAQ Global Select Market rules are creating increased compliance costs and uncertainty for companies like ours. These new or changed laws, regulations and standards may lack specificity and are subject to varying interpretations. For example, certain provisions of Dodd-Frank are currently in the process of being implemented through regulatory action, and recently implemented provisions of Dodd-Frank remain subject to evolving application and interpretation by regulatory authorities. The implementation of these laws and their application in practice may evolve over time as new guidance is provided by regulatory and governing bodies. This could result in continuing uncertainty regarding compliance matters and higher costs of compliance as a result of ongoing revisions to such governance standards.

In addition, continuing compliance with Section 404 of the Sarbanes-Oxley Act of 2002 and the related regulations regarding our required assessment of our internal control over financial reporting requires the commitment of significant financial and managerial resources and the report of an independent registered public accounting firm on the Company s internal control over financial reporting.

In connection with our Annual Report on Form 20-F for fiscal 2015, our management assessed our internal control over financial reporting, and determined that our internal control over financial reporting was effective as of

December 31, 2015, and our independent auditors have expressed an unqualified opinion over the effectiveness of our internal control over financial reporting as of December 31, 2015. However, we will undertake management assessments of our internal control over financial reporting in connection with each annual report, and any deficiencies uncovered by these assessments or any inability of our auditors to issue an unqualified report could harm our reputation and the price of our ordinary shares.

The SEC has also adopted rules pursuant to Dodd-Frank setting forth new disclosure requirements concerning the use of certain minerals that are mined from the Democratic Republic of Congo and adjoining countries. We have incurred and expect to continue to incur costs associated with determining whether any of our products include materials that are covered by the conflict minerals rules. In the event that our products do contain materials covered by the conflict minerals rules, we would be required to comply with applicable disclosure requirements, including conducting diligence procedures to determine the sources of certain minerals that may be used or necessary to the production of our products and, if applicable, undertake potential changes to products, processes or sources of supply as a consequence of such verification activities. In addition, if our products do contain materials covered by the conflict mineral rules, these rules could adversely affect the sourcing, supply and pricing of materials used in our products, particularly if the number of suppliers offering the minerals identified as conflict minerals sourced from locations other than the Democratic Republic of Congo and adjoining countries is limited. It is also possible that we may face reputational harm if we determine that certain of our products contain minerals not determined to be conflict free and/or we are unable to alter our products, processes or sources of supply to avoid such materials.

If we fail to comply with new or changed laws or regulations, our business and reputation may be harmed.

Table of Contents

A small number of shareholders own a substantial portion of our ordinary shares, and they may make decisions with which you or others may disagree

As of January 31, 2016, our directors and executive officers owned approximately 26.6% of the voting power of our outstanding ordinary shares, or 29.8% of our outstanding ordinary shares if the percentage includes options currently exercisable or exercisable within 60 days of January 31, 2016. The interests of these shareholders may differ from your interests and present a conflict. If these shareholders act together, they could exercise significant influence over our operations and business strategy. For example, although these shareholders hold considerably less than a majority of our outstanding ordinary shares, they may have sufficient voting power to influence matters requiring approval by our shareholders, including the election and removal of directors and the approval or rejection of mergers or other business combination transactions. In addition, this concentration of ownership may delay, prevent or deter a change in control, or deprive a shareholder of a possible premium for its ordinary shares as part of a sale of our company.

We may be required to indemnify our directors and officers in certain circumstances

We have entered into agreements with each of our directors and senior officers to insure, indemnify and exculpate them against some types of claims, subject to dollar limits and other limitations. Subject to Israeli law, these agreements provide that we will indemnify each of these directors and senior officers for any of the following liabilities or expenses that they may incur due to an act performed or failure to act in their capacity as our director or senior officer:

Monetary liability imposed on the director or senior officer in favor of a third party in a judgment, including a settlement or an arbitral award confirmed by a court.

Reasonable legal costs, including attorneys fees, expended by a director or senior officer as a result of an investigation or proceeding instituted against the director or senior officer by a competent authority; provided, however, that such investigation or proceeding concludes without the filing of an indictment against the director or senior officer and either:

No financial liability was imposed on the director or senior officer in lieu of criminal proceedings, or

Financial liability was imposed on the director or senior officer in lieu of criminal proceedings, but the alleged criminal offense does not require proof of criminal intent.

Reasonable legal costs, including attorneys fees, expended by the director or senior officer or for which the director or senior officer is charged by a court:

In an action brought against the director or senior officer by us, on our behalf or on behalf of a third party,

In a criminal action in which the director or senior officer is found innocent, or

In a criminal action in which the director or senior officer is convicted, but in which proof of criminal intent is not required.

Our cash balances and investment portfolio have been, and may continue to be, adversely affected by market conditions and interest rates

We maintain substantial balances of cash and liquid investments, for purposes of acquisitions and general corporate purposes. Our cash, cash equivalents, short-term bank deposits and marketable securities totaled $3,615 million as of December 31, 2015. 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 an important component of our net income. The outlook for our financial income is dependent on many factors, some of which are beyond our control, and they include the future direction of interest rates, the amount of any share repurchases or acquisitions that we effect and the amount of cash flows from operations that are available for investment. We rely on third-party money managers to manage the majority of our investment portfolio in a risk-controlled framework. Our investment portfolio throughout the world is invested primarily in fixed-income securities and is affected by changes in interest rates which continue to be low. Interest rates are highly sensitive to many factors, including governmental monetary policies and domestic and international economic and political conditions. In a low or declining interest rate environment, borrowers may seek to refinance their borrowings at lower rates and, accordingly, prepay or redeem securities we hold more quickly than we initially expected. This action may cause us to reinvest the redeemed proceeds in lower yielding investments. Any significant decline in our financial income or the value of our investments as a result of the low interest rate environment, falling interest rates, deterioration in the credit rating of the securities in which we have invested, or general market conditions, could have an adverse effect on our results of operations and financial condition.

Table of Contents

We generally buy and hold our portfolio positions, while minimizing credit risk by setting maximum concentration limit per issuer and credit rating. Our investments consist primarily of government and corporate debentures. Although we believe that we generally adhere to conservative investment guidelines, the continuing turmoil in the financial markets may result in impairments of the carrying value of our investment assets. We classify our investments as available-for-sale. Changes in the fair value of investments classified as available-for-sale are not recognized to 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. Had we reported all the accumulated changes in the fair values of our investments into income, our reported net income for the year ended December 31, 2015, would have decreased by $4 million.

Currency fluctuations may affect the results of our operations or financial condition

Our functional and reporting currency is the U.S. dollar. We generate a majority of our revenues and expenses in U.S. dollars. In 2015, we incurred approximately 41% of our expenses in foreign currencies, primarily Israeli Shekels and Euros. Accordingly, changes in exchange rates may have a material adverse effect on our business, operating results and financial condition. The exchange rates between the U.S. dollar and certain foreign currencies have fluctuated substantially in recent years and may continue to fluctuate substantially in the future. We expect that a majority of our revenues will continue to be generated in U.S. dollars for the foreseeable future and that a significant portion of our expenses, including personnel costs, as well as capital and operating expenditures, will continue to be denominated in the currencies referred to above. The results of our operations may be adversely affected in relation to foreign exchange fluctuations. During 2015, we entered into forward contracts to hedge against some of the risk of foreign currency exchange rates fluctuations resulting in changes in future cash flow from payments of payroll and related expenses denominated in Israeli Shekels. As of December 31, 2015, we had outstanding forward contracts that hedge against changes in foreign currency exchange rates of $26 million.

We entered into forward contracts to hedge the exchange impacts on assets and liabilities denominated in Israeli Shekels and other currencies. As of December 31, 2015, we had outstanding forward contracts that did not meet the requirement for hedge accounting, in the amount of $319 million. We use derivative financial instruments, such as foreign exchange forward contracts, to mitigate the risk of changes in foreign exchange rates on accounts receivable and forecast cash flows denominated in certain foreign currencies. We may not be able to purchase derivative instruments adequate to fully insulate ourselves from foreign currency exchange risks and over the past year we have incurred losses as a result of exchange rate fluctuations on exposures that have not been covered by our hedging strategy.

Additionally, our hedging activities may also contribute to increased losses as a result of volatility in foreign currency markets. If foreign exchange currency markets continue to be volatile, such fluctuations in foreign currency exchange rates could materially and adversely affect our profit margins and results of operations in future periods. Also, the volatility in the foreign currency markets may make it difficult to hedge our foreign currency exposures effectively.

The imposition of exchange or price controls or other restrictions on the conversion of foreign currencies could also have a material adverse effect on our business, results of operations and financial condition.

Our business and operations are subject to the risks of earthquakes, fire, floods and other natural catastrophic events, as well as manmade problems such as power disruptions or terrorism

Our headquarters in the United States, as well as certain of our research and development operations, are located in the Silicon Valley area of Northern California, a region known for seismic activity. We also have significant operations in other regions that have experienced natural disasters. A significant natural disaster occurring at our facilities in Israel

or the U.S. or elsewhere, or where our channel partners are located, could have a material adverse impact on our business, operating results and financial condition. In addition, acts of terrorism could cause disruptions in our or our customers businesses or the economy as a whole. Further, we rely on information technology systems to communicate among our workforce located worldwide. Any disruption to our internal communications, whether caused by a natural disaster or by manmade problems, such as power disruptions or terrorism, could delay our research and development efforts. To the extent that such disruptions result in delays or cancellations of customer orders, our research and development efforts or the deployment of our products, our business and operating results would be materially and adversely affected.

Table of Contents

Third parties might attempt to gain unauthorized access to our network or seek to compromise our products and services.

We regularly face attempts by others to gain unauthorized access through the Internet or to introduce malicious software to our information technology (IT) systems. Additionally, malicious hackers may attempt to gain unauthorized access and corrupt the processes of hardware and software products that we manufacture and services we provide. We or our products are a frequent target of computer hackers and organizations that intend to sabotage, take control of, or otherwise corrupt our manufacturing or other processes and products. We are also a target of malicious attackers who attempt to gain access to our network or data centers or those of our customers or end users; steal proprietary information related to our business, products, employees, and customers; or interrupt our systems or those of our customers or others. We believe such attempts are increasing in number. From time to time we encounter intrusions or attempts at gaining unauthorized access to our products and network. To date, none have resulted in any material adverse impact to our business or operations. While we seek to detect and investigate all unauthorized attempts and attacks against our network and products, and to prevent their recurrence where practicable through changes to our internal processes and tools and/or changes or patches to our products, we remain potentially vulnerable to additional known or unknown threats. Such incidents, whether successful or unsuccessful, could result in our incurring significant costs related to, for example, rebuilding internal systems, reduced inventory value, providing modifications to our products and services, defending against litigation, responding to regulatory inquiries or actions, paying damages, or taking other remedial steps with respect to third parties. Publicity about vulnerabilities and attempted or successful incursions could damage our reputation with customers or users, and reduce demand for our products and services.

We may need to change our pricing models to compete successfully.

The intense competition we face in the sales of our products and services and general economic and business conditions can put pressure on us to change our prices. If our competitors offer deep discounts on certain products or services or develop products that the marketplace considers more valuable, we may need to lower prices or offer other favorable terms in order to compete successfully. Any such changes may reduce margins and could adversely affect operating results. Additionally, the increasing prevalence of cloud and SaaS delivery models offered by us and our competitors may unfavorably impact pricing in both our on-premise enterprise software business and our cloud business, as well as overall demand for our on-premise software product and service offerings, which could reduce our revenues and profitability. Our competitors may offer lower pricing on their support offerings, which could put pressure on us to further discount our product or support pricing.

We are subject to governmental export and import controls that could subject us to liability or impair our ability to compete in international markets.

Because we incorporate encryption technology into our products, certain of our products are subject to U.S. export controls and may be exported outside the U.S. only with the required export license or through an export license exception. If we were to fail to comply with U.S. export licensing requirements, U.S. customs regulations, U.S. economic sanctions, or other laws, we could be subject to substantial civil and criminal penalties, including fines, incarceration for responsible employees and managers, and the possible loss of export or import privileges. Obtaining the necessary export license for a particular sale may be time-consuming and may result in the delay or loss of sales opportunities. Furthermore, U.S. export control laws and economic sanctions prohibit the shipment of certain products to U.S. embargoed or sanctioned countries, governments, and persons. Even though we take precautions to ensure that we comply with all relevant regulations, any failure by us or any partners to comply with such regulations could have negative consequences for us, including reputational harm, government investigations, and penalties.

In addition, various countries regulate the import of certain encryption technology, including through import permit and license requirements, and have enacted laws that could limit our ability to distribute our products or could limit our end-customers ability to implement our products in those countries. Changes in our products or changes in export and import regulations may create delays in the introduction of our products into international markets, prevent our end-customers with international operations from deploying our products globally or, in some cases, prevent or delay the export or import of our products to certain countries, governments, or persons altogether. Any change in export or import regulations, economic sanctions or related legislation, shift in the enforcement or scope of existing regulations, or change in the countries, governments, persons, or technologies targeted by such regulations, could result in decreased use of our products by, or in our decreased ability to export or sell our products to, existing or potential end-customers with international operations. Any decreased use of our products or limitation on our ability to export to or sell our products in international markets would likely adversely affect our business, financial condition, and operating results.

Risks Related to Our Operations in Israel

Potential political, economic and military instability in Israel, where our principal executive offices and our principal research and development facilities are located, may adversely affect our results of operations

We are incorporated under the laws of the State of Israel, and our principal executive offices and principal research and development facilities are located in Israel. Accordingly, political, economic and military conditions in and surrounding Israel may directly affect our business. Since the State of Israel was established in 1948, a number of armed conflicts have occurred between Israel and its Arab neighbors. Terrorist attacks and hostilities within Israel; the hostilities between Israel and Hezbollah and between Israel and Hamas; as well as tensions between Israel and Iran, have also heightened these risks, including an escalation in terrorist

Table of Contents

attacks since October 2015 and extensive hostilities from July to August 2014 along Israel s border with the Gaza Strip, which resulted in missiles being fired from the Gaza Strip into Israel. Our principal place of business is located in Tel Aviv, Israel, which is approximately 40 miles from the nearest point of the border with the Gaza Strip. There can be no assurance that attacks launched from the Gaza Strip will not reach our facilities, which could result in a significant disruption of our business. In addition, there are significant ongoing hostilities in the Middle East, particularly in Syria and Iraq, which may impact Israel in the future. Any hostilities involving Israel, a significant increase in terrorism or the interruption or curtailment of trade between Israel and its present trading partners, or a significant downturn in the economic or financial condition of Israel, could materially adversely affect our operations. Ongoing and revived hostilities or other Israeli political or economic factors could materially adversely affect our business, operating results and financial condition. In addition, there have been increased efforts by activists to cause companies and consumers to boycott Israeli goods based on Israeli government policies. Such actions, particularly if they become more widespread, may adversely impact our ability to sell our products.

Recent uprisings and armed conflicts in various countries in the Middle East and North Africa are affecting the political stability of those countries. This instability may lead to deterioration of the political and trade relationships that exist between the State of Israel and these countries. In addition, this instability may affect the global economy and marketplace, including as a result of changes in oil and gas prices.

Our operations may be disrupted by the obligations of our personnel to perform military service

Many of our employees in Israel are obligated to perform annual military reserve duty in the Israel Defense Forces, in the event of a military conflict, could be called to active duty. Our operations could be disrupted by the absence of a significant number of our employees related to military service or the absence for extended periods of military service of one or more of our key employees. Military service requirements for our employees could materially adversely affect our business, operating results and financial condition.

The tax benefits available to us require us to meet several conditions, and may be terminated or reduced in the future, which would increase our taxes.

For the year ended December 31, 2015, our effective tax rate was 21.5%. We have benefited or currently benefit from a variety of government programs and tax benefits that generally carry conditions that we must meet in order to be eligible to obtain any benefit. Our tax expenses and the resulting effective tax rate reflected in our financial statements may increase over time as a result of changes in corporate income tax rates, other changes in the tax laws of the countries in which we operate or changes in the mix of countries where we generate profit.

If we fail to meet the conditions upon which certain favorable tax treatment is based, we would not be able to claim future tax benefits and could be required to refund tax benefits already received. Additionally, some of these programs and the related tax benefits are available to us for a limited number of years, and these benefits expire from time to time.

Any of the following could have a material effect on our overall effective tax rate:

- Some programs may be discontinued,

- We may be unable to meet the requirements for continuing to qualify for some programs,

These programs and tax benefits may be unavailable at their current levels,

Upon expiration of a particular benefit, we may not be eligible to participate in a new program or qualify for a new tax benefit that would offset the loss of the expiring tax benefit, or

We may be required to refund previously recognized tax benefits if we are found to be in violation of the stipulated conditions.

Additional details are provided in Item 5 Operating and Financial Review and Products under the caption Taxes on income , in Item 10 Additional Information under the caption Israeli taxation, foreign exchange regulation and investment programs and in Note 12 to our Consolidated Financial Statements.

Provisions of Israeli law and our articles of association may delay, prevent or make difficult an acquisition of us, prevent a change of control, and negatively impact our share price

Israeli corporate law regulates acquisitions of shares through tender offers and mergers, requires special approvals for transactions involving directors, officers or significant shareholders, and regulates other matters that may be relevant to these types of transactions. Furthermore, Israeli tax considerations may make potential acquisition transactions unappealing to us or to some of our shareholders. For example, Israeli tax law may subject a shareholder who exchanges his or her ordinary shares for shares in a foreign corporation, to taxation before disposition of the investment in the foreign corporation. These provisions of Israeli law may delay, prevent or make difficult an acquisition of our company, which could prevent a change of control and, therefore, depress the price of our shares.

Table of Contents

In addition, our articles of association contain certain provisions that may make it more difficult to acquire us, such as the provision which provides that our board of directors may issue preferred shares. These provisions may have the effect of delaying or deterring a change in control of us, thereby limiting the opportunity for shareholders to receive a premium for their shares and possibly affecting the price that some investors are willing to pay for our securities.

Additional details are provided in Item 10 Additional Information under the caption Articles of Association and Israeli Companies Law Anti-takeover measures.

As a foreign private issuer whose shares are listed on the NASDAQ Global Select Market, we may follow certain home country corporate governance practices instead of certain NASDAQ requirements.

As a foreign private issuer whose shares are listed on the NASDAQ Global Select Market, we are permitted to follow certain home country corporate governance practices instead of certain requirements of the NASDAQ Stock Market Rules. For example, we follow our home country law, instead of the NASDAQ Stock Market Rules, which require that we obtain shareholder approval for the establishment or amendment of certain equity based compensation plans and arrangements. Under Israeli law and practice, in general, the approval of the board of directors is required for the establishment or amendment of equity based compensation plans and arrangements, unless the arrangement is for the benefit of a director or a controlling shareholder, in which case compensation committee or audit committee and shareholder approval are also required. A foreign private issuer that elects to follow a home country practice instead of NASDAQ requirements must submit to NASDAQ in advance a written statement from an independent counsel in such issuer s home country certifying that the issuer s practices are not prohibited by the home country s laws. In addition, a foreign private issuer must disclose in its annual reports filed with the Securities and Exchange Commission each such requirement that it does not follow and describe the home country practice followed by the issuer instead of any such requirement. Accordingly, our shareholders may not be afforded the same protection as provided under NASDAQ s corporate governance rules.

ITEM 4. INFORMATION ON CHECK POINT

Overview

Check Point s mission is to secure the Internet. Check Point was founded in 1993, and has since developed technologies to secure communications and transactions over the Internet by enterprises and consumers. Two decades ago, risks and threats were limited and securing the Internet was relatively simple. A firewall and an antivirus solution generally provided adequate security for business transactions and communications over the Internet. Today, enterprises require many (in some cases 15 or more) point solutions to secure their information technology (IT) networks from the multitude of threats and potential attacks and are facing an increasingly complex IT security infrastructure.

Check Point s core competencies are developing security solutions to protect business and consumer transactions and communications over the Internet, and reducing the complexity in Internet security. We strive to solve the security maze by bringing more, better and simpler security solutions to our customers.

Check Point develops, markets and supports a wide range of products and services for IT security. We offer our customers an extensive portfolio of network security, endpoint security, data security and management solutions. Our solutions operate under a unified security architecture that enables end-to-end security with a single line of unified security gateways, and allow a single agent for all endpoint security that can be managed from a single unified management console. This unified management allows for ease of deployment and centralized control and is

supported by, and reinforced with, real-time security updates.

Check Point was an industry pioneer with our FireWall-1 and our patented Stateful Inspection technology. Check Point extended its IT security innovation with the development of our Software Blade architecture. Our dynamic Software Blade architecture delivers secure, flexible and simple solutions that can be customized to meet the security needs of any organization or environment.

Our products and services are sold to enterprises, service providers, small and medium sized businesses and consumers. Our Open Platform for Security framework allows customers to extend the capabilities of our products and services with third-party hardware and security software applications. Our products are sold, integrated and serviced by a network of partners worldwide. Check Point customers include tens of thousands of businesses and organizations of all sizes. Check Point s award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

Table of Contents

Business Highlights

Details regarding the important events in the development of our business since the beginning of 2015 are provided in Item 5 Operating and Financial Review and Prospects under the caption Overview.

We were incorporated as a company under the laws of the State of Israel in 1993 under the name of Check Point Software Technologies Ltd. Our registered office and principal place of business is located at 5 Ha Solelim Street, Tel Aviv 6789705 Israel. The telephone number of our registered office is 972-3-753-4555. Our company s web site is www.checkpoint.com. The contents of our web site are not incorporated by reference into this Annual Report on Form 20-F.

This Annual Report on Form 20-F is available on our web site. If you would like to receive a printed copy via mail, please contact our Investor Relations department at 959 Skyway Road, Suite 300, San Carlos, CA 94070, U.S.A., Tel.: 650-628-2050, email: ir@us.checkpoint.com.

Our agent for service of process in the United States is CT Corporation System, 818 West Seventh Street, Los Angeles, CA 90017 U.S.A.; Tel: 213-627-8252.

Cyber Security Industry Today

Organizations of all sizes will continue to face a challenging threat landscape. With countless new connections formed every day, the world is more globally linked than ever. Cloud, mobility, virtualization and the Internet of Things (IoT) are changing the way customers deploy and consume technology. Enterprises have more opportunities than ever before to innovate and compete more effectively and efficiently. However, the network edges in their infrastructure are blurring and boundaries between entities are disappearing, which increases the risk of cyberattacks. Specific trends within this dynamic include:

Growth in Remote Connectivity. The proliferation of smartphones and the growing number of people who work remotely and conduct business through mobile devices has expanded the need to safeguard and manage the access to information. Whether remote or mobile, workers need constant connectivity to the enterprise network. In 2015, Check Point discovered significant vulnerabilities in applications such as WhatsApp and in the Android operating system which allowed applications to gain illegitimate privileged access rights within hundreds of millions of mobile devices. Because of this trend toward remote connectivity, enterprises will need to ensure security across all points of their infrastructure and deploy mobile-specific security solutions.

Cloud Computing and Network Virtualization. Cloud computing, or Internet-based computing, provides shared servers which provide resources, software and data storage to computers and other devices on demand, and drives the need for enterprise security for both on-premises and in-the-cloud infrastructures. New virtual environments and public and private clouds jeopardize enterprises overall security posture if they are not deployed within the appropriate security infrastructure. These are complex environments to manage and secure due to multiple network layers. Deploying virtualized security solutions are crucial to ensuring that attacks are immediately contained before they spread across virtualized server and network environments.

Overall Complexity within the Enterprise IT infrastructure. Another key trend affecting IT security is the increasing complexity of deploying, managing and monitoring the many technologies needed to fully secure the enterprise IT network. This trend creates two challenges for enterprises: how to cost-effectively manage a patch-work of point product solutions, and how to ensure that no gaps are left in the infrastructure. To solve these problems, enterprises seek out single-architecture solutions with simplified management in an effort to keep the security infrastructure

robust, yet simple to manage and adaptable to on-going changes.

Increased Data Privacy and Compliance Regulation. The increasing number of governmental regulations around the world regarding data privacy and compliance is also impacting enterprise security. Enterprises need to put in place data security technologies to prevent violations of applicable laws regarding data privacy and protection and to avoid experiencing data loss or data theft, which could cause enterprises to suffer reputational harm and governmental sanctions, fines and penalties. Data has long been a prime target for hackers seeking financial information, intellectual property, and insider business information and authentication credentials. In 2015, we saw attacks on BlueCross, Morgan Stanley and Anthem . These attacks exposed personal health and financial data on millions of consumers.

Emergence of Social Engineering. As security solutions improve and are more thoroughly deployed throughout enterprises, attackers attempt to bypass security mitigations and restrictions by hacking the human mind , in other words, by deceiving employees into providing credentials, sending infected files or clicking on an infected link. Many of the attacks in 2015 have taken root within the attack s target through social engineering and phishing techniques. Specific security policies, increased segmentation of the infrastructure and multi-layer defense solutions will be needed to prevent these types of attacks.

Table of Contents

Increase in Sophistication of Threats and Attacks. Today s threats use sophisticated technology, the internet and deception to acquire sensitive information and to disrupt business operations. Many of these threats contain new, unknown signatures when they reach their targets. These new unknown signatures deploy and cause damage to their target immediately. Commonly called zero-day threats , these threats present unique challenges to the enterprise. Enterprises need to put in place multi-layer defenses to prevent, detect and extract threats before they cause damage.

Increase in the Number of Attacks and Potential Targets. By 2020, estimates indicate that there will be one billion smart meters, over one million smart light bulbs, over 50% of the consumers will utilize wearable technology and more than five major car manufacturers will have smart, driverless cars. Wearables can be hacked to record conversations, cars can be hacked to compromise safety and smart meters can be hacked to access information. Critical infrastructures such as SCADA and IOS are increasingly targeted as they are older infrastructures not originally designed with cybersecurity in mind. Manufacturers of these products will need more robust security solutions, and enterprises that are connected to these types of products through the ecosystem will need to consider how to prevent these devices might be leveraged to gain access to their infrastructure.

Check Point Legacy and Vision

Since its inception, Check Point s pure focus has been on IT security. Adapting to customers changing needs, the company has developed numerous technologies to secure the use of the Internet by corporations and consumers when transacting and communicating. Today, Check Point is the largest pure security vendor globally. Making Internet communications and critical data secure, reliable and available everywhere has been and continues to be our ongoing vision. We are committed to staying focused on real customer needs and to developing new and innovative security solutions that redefine the security landscape. An interconnected, digital economy is here to stay, empowering business leaders to invent, to inspire and to drive positive change throughout the world.

Innovative leaders seize opportunities that emerge from change. They constantly question every assumption. These leaders rely on the latest SaaS or IoT platforms to speed their time to market. They add partners from around the world to their supply chain to ensure they get the best suppliers and the best prices. They deploy beta applications in mobile environments to speed time to market. These leaders push the envelope, but not at the expense of security, performance, or their ability to compete in the market.

The ecosystem is rapidly changing, and is less and less controlled. Digital assets are harder to track and control. Infrastructure is no longer in one place as boundaries disappear. Hackers are innovating just as quickly as enterprises are and are finding new ways to attack our connected world. More and more malware is being put into our ecosystem that traditional security techniques are powerless to prevent. Increasingly, vulnerabilities are exploited, brands are damaged, assets are stolen, and our personal safety is at risk.

Business leaders today must stay One Step Ahead of things they cannot see, know or control. To be one step ahead, enterprises must have visibility to tomorrow s threats, not just the threats of today. They can no longer rely on continuously integrating layers of point solutions that result in complex mosaics that still contain gaps in the infrastructure. Enterprises need to be able to prevent attacks at every stage, from start to finish. They need to contain threats and extract them the second they are detected. To be One Step Ahead they need access to a global intelligence network and leverage it for real-time protection. These leaders need to protect every point in the infrastructure, from mobile to cloud to virtual and physical, from one location, while being flexible and adapting to change.

Organizations around the world rely on Check Point to protect their brand, assets and data from cyberattacks. For more than 20 years, Check Point s single architecture, comprehensive management and integrated threat intelligence, combined with the most advanced prevention and extraction solutions, have yielded the highest malware catch rate in

the industry, thereby enabling millions of users to safely and productively accelerate their businesses.

With a legacy of industry firsts and continuous innovation, Check Point gives business leaders the freedom to invent, inspire and compete securely in the ever changing digital economy.

Check Point Technology Leadership in 2015

Gartner

Number One Worldwide Firewall Equipment Market Share 2014

Leader Enterprise Network Firewall Market Quadrant 2015

Leader Unified Threat Management Magic Quadrant 2015

Leader Mobile Data Protection Magic Quadrant 2015

Number One Worldwide Firewall Equipment Market Share 2015 1st. 2nd, 3rd Quarter

Table of Contents

IDC

Top Position Worldwide Combined Firewall & UTM Appliance Market 2014

Top Position Worldwide Combined Firewall and UTM Appliance Market 2015 1st. 2nd, 3rd Quarter

NSS Breach Detection Systems Results: Check Point s Next Generation Threat Prevention Solution received a recommended rating in the NSS Labs Breach Detection Systems (BDS) group test. Check Point received a 100 percent catch rate of HTTP, 100 percent catch rate for email and 100 percent catch rate for drive by malware.

Common Criteria Certification: Check Point was awarded Common Criteria (CC) certification for R77.30, following a rigorous third-party evaluation and testing process.

Best Product of 2015: Check Point SandBlast was named Coolest Security Product of 2015 by *CRN Magazine*.

Product Strategy

In an effort to simultaneously address the need for scalable security solutions and the retention of initial investments, Check Point introduced the Software Blade architecture in February 2009. The architecture provides customers with the ability to tailor their security gateways based on their specific needs at any time. It offers enterprises a common platform to deploy independent, modular and interoperable security applications or Software Blades such as firewall, virtual private network (VPN), intrusion prevention system (IPS), Application Control, Anti-Bot, antivirus, data loss prevention (DLP), policy management, event analysis, or multi-domain management. The new architecture allows customers to select the exact security they need from a library of over 20 Software Blades, and to combine these blades into a single, centrally-managed solution. Customers can easily extend their security solutions by adding new Software Blades without the need to purchase additional hardware. This allows our customers to deploy security dynamically, when needed, with lower total cost of ownership, full integration, and on a single management console. Check Point also offers these software blades grouped into functional packages to address specific security issues. The four packages offered are Next Generation Firewall, Next Generation Threat Prevention, Next Generation Secure Web Gateway and Next Generation Data Protection.

Threat Prevention software blades are fed by a cloud based threat intelligence knowledge base, introduced in 2012, the Check Point ThreatCloud . The ThreatCloud, the first collaborative network to fight cybercrime, gathers threat data from an innovative worldwide network of threat sensors and distributes threat intelligence to security gateways around the globe. Today, ThreatCloud scans more than 250 million addresses for bot discovery, keeps track of over 11 million malware signatures and has detected over 5.5 million malware infested sites. On average, thousands of Check Point gateways detect more than 700,000 malwares every day. The ThreatCloud powers the Threat Prevention software blades by feeding threat updates directly to customers gateways, enabling them to enforce pre-emptive protection against advanced threats, such as bots, Advanced Persistent Threats (APTs) and other forms of sophisticated malware.

In 2015, Check Point continued its track record of innovation through strategic acquisitions and new product introductions:

February: Hyperwise Acquisition: Unique CPU-Level threat prevention technology.
March:

	SandBlast Threat Extraction Technology: Providing zero malware in zero second protection.
April:	Lacoon Mobile Security Acquisition: Advanced threat prevention for mobile devices.
May:	1200R SCADA Appliance: Securing industrial control systems and critical infrastructure.
July:	Check Point vSEC: Private cloud security solution for VMware NSX environments.
July:	ZoneAlarm 2016: Consumer endpoint security software.
August:	Check Point Protect: Mobile Threat Prevention Solution for smartphones.
September:	SandBlast Threat Prevention: Evasion Resistant Sandboxing and Threat Extraction

Check Point continued its commitment to inspecting and discovering vulnerabilities that exist in various platforms, applications and devices for the sole purpose of ensuring that all consumers of technology, whether they are currently Check Point customers or not, have important information regarding security vulnerabilities. In 2015, we published a number of vulnerability reports, including:

Volatile Cedar: Campaign allowing attackers to monitor a victim s actions and steal data.

2015 Check Point Security Report: Report revealed that 96% of organizations are using high-risk applications and that there was an increase in security incidents across all categories.

Magento eCommerce Platform: Critical RCE (remote code execution) vulnerability found in eBay s Magento web ecommerce platform, affecting nearly 200,000 online shops.

Table of Contents

WhatsApp Web Vulnerabilities: Vulnerabilities discovered that exploit the WhatsApp Web logic and put up to 200 million users at risk.

Certifi-gate Vulnerability in Android: Allows applications to gain illegitimate privileged access rights and exists in hundreds of millions of devices.

BrainTest related Mobile Malware: Malware, packaged within an Android game app called BrainTest, affected between 200,000 and one million users.

EZCast Vulnerability: HDMI dongle-based TV streamer that converts non-connected TVs into smart TVs allowing hacker s ability to gain unauthorized access to an EZCast subscriber s home network.

Rocket Kitten: Uncovered Iranian-linked cyber-espionage global campaign.

Check Point Product Offerings

Check Point continues to develop new innovations based on the Software Blade Architecture, providing customers with flexible and simple solutions that can be fully customized to meet the exact security needs of any organization. Check Point 3D Security uniquely combines policy, people and enforcement for greater protection of information assets and helps organizations implement a blueprint for security that aligns with business needs. Our products provide end-to-end security from the enterprise to the cloud to your mobile worker s personal devices. We prevent and mitigate cyber-attacks and limit the data theft that often results from these threats. Our unified security management solution delivers extensibility and ease of use. Check Point keeps customers one step ahead with industry leading security products for Threat Prevention, Mobility, Firewalls, Security Management and more. Our products protect individuals, SMBs and large data center enterprises.

Next Generation Firewalls. Check Point provides customers of all sizes with the latest data and network security protection in an integrated next generation firewall platform, reducing complexity and lowering the total cost of ownership. Offerings include the following:

a. Data Center & Enterprise

Enterprises deploy security along well defined boundaries at the perimeter and internally within software defined data centers. Our next generation firewall solutions for protecting both north-south and east-west traffic include:

Check Point Appliances. Our data center and enterprise network security appliances combine high-performance, multi-core capabilities with fast networking technologies to provide the highest level of security. By consolidating multiple security technologies into a single security gateway, these appliances are designed to deliver advanced and integrated security solutions to meet all of your business security needs.

Integrated Appliance Solutions. Check Point Integrated Appliance Solutions (IAS) offer flexibility and choice for data center and enterprise network security. Powered by Fujitsu and Blue Coat, these appliances provide integrated software and hardware bundles and direct support

that are customized to organizations exact specifications.

Public and Private Cloud. Enterprises seeking the availability, scalability and cost reduction are shifting more and more applications to cloud computing models. Check Point vSEC products provide integrated security and expertise to help customers build secure cloud infrastructure today and protect future deployments.

b. Small Business and Branch

Check Point has an affordable, easy to use and effective solution to secure small businesses and branch offices. This includes turn-key appliances and a Cloud Managed Security Service option, giving you the freedom to focus on growing your business.

600 Appliance. Available in three models to match the number of users protected, the 600 Appliance is ideal for small offices with a staff of 50 employees or fewer. You can manage the appliance via simplified web-based local management, or centrally via our Cloud Managed Security Service

1100 Appliance. Available in three models to match the number of users protected, the 1100 Appliance is ideal for branch offices with a staff of 50 employees or fewer. Small businesses can manage the appliance via simplified web-based local management, or centrally via our enterprise security management product.

Table of Contents

Cloud Managed Security Service. This cost-effective, enterprise-class security solution is managed by experts, leaving small businesses free to focus on growing their business instead of managing their security. Our partners offer this service with an attractive and predictable pricing structure that makes security budget and planning simple and affordable.

2200 Appliance. With its multi-core technology and six 1-gigabit Ethernet ports, the 2200 Appliance can easily secure any branch or small office. The appliance includes our enterprise security management product for up to two gateways.

c. **Consumer and Home**

Check Point s ZoneAlarm products are used by more than 90 million people to provide integrated threat protection to safeguard all of their PCs and mobile devices. Offerings include an a fully integrated Extreme Security Suite, an Internet Security Suite, AV + Firewall or PRO Firewall option so consumers choose the level of protection they need.

Next Generation Threat Prevention. The growing frequency and sophistication of cyber security threats makes protecting organizations more important than ever. Check Point Next Generation Threat Prevention delivers a multi-layered line of defense and extensive security intelligence coverage to help combat threats of today, and tomorrow. Our Threat Prevention products fall into the following five categories:

a. **Sandblast Zero Day Protection**: Attackers have become more creative, reaching corporate resources with modern and complex malware attacks. Check Point SandBlast Zero-Day Protection combines innovative technologies to proactively protect against even the most dangerous targeted attacks and unknown malware, while ensuring quick delivery of safe content.

b. **Threat Prevention Appliances and Software**. To combat today s sophisticated cyberattacks and meet enterprise requirements, customers need a multi-layered approach to threat prevention. Check Point s cyber security threat prevention solutions enable detection and prevention of known vulnerabilities and advanced threats dedicated threat prevention appliances or specialized Software Blades to give customers maximum flexibility in designing their security solution.

c. **Threat Intelligence**. In the constant fight against malware, threat intelligence and rapid response capabilities are vital. Check Point helps keep customers up and running with comprehensive intelligence to proactively stop threats, manage security services to monitor your network and incident response to quickly respond to and resolve attacks. Our ThreatCloud IntelliStore, Incident Response and Managed Security Services provide tools to help organizations stay one step ahead of attackers and mitigate future risks

d. **Web Security**. Web-borne malware is more clever than ever. Check Point Web Security solutions provide real-time protection for secure use of the web and educate users on web-use policy.

e. **Distributed denial-of-service.** DDoS attacks can be unleashed by anyone, but with a little preparation, customers can prevent service disruptions caused by DDoS. Check Point DDoS-P (DDoS Protection) uses a hybrid of dedicated on-premises and cloud-based resources to defend against volumetric, application, reflective and resource exhaustive DDoS attacks

Security Management. As network complexity grows, so does the difficulty of applying complete, consistent security management policies and efficient processes to investigate events and oversee resolution. Check Point offers a variety of smart management solutions designed to tackle the security management challenges of today and tomorrow.

a. **Policy Management**. With many and varied network affiliated devices to manage, organizations find strict policy enforcement time consuming and challenging. We offer centralized policy management solutions that make it easy to ensure that all gateways, mobile devices and endpoint devices are in compliance and stay that way

Network Policy Management Software Blade. Comprehensive, centralized network security policy management for Check Point gateways and Software Blades, via SmartDashboard a single, unified console that provides control over even the most complex security deployments

Endpoint Policy Management Software Blade. Simplify endpoint security management by unifying all endpoint security capabilities for PC & Mac in a single console. Monitor, manage, educate and enforce policy, from an at-a-glance dashboard down to user and machine details, all with a few clicks.

Multi-Domain Security Management (Provider-1) Software Blade. Deliver more security and control by segmenting security management into multiple virtual domains. Businesses of all sizes can easily create virtual domains based on geography, business unit or security function to strengthen security and simplify management.

Table of Contents

Management Portal Software Blade. Browser-based security management access to outside groups such as support staff or auditors, while maintaining centralized control of policy enforcement. View security policies, the status of all Check Point products and administrator activity as well as edit, create and modify internal users

b. **Operations and Workflow** As network complexity grows, security management processes inevitably slow down. Our Operations and Workflow solutions are designed to accelerate security management and restore efficiency with centralized device and user management, security best practices and automated change management.

Compliance Software Blade. Monitor management, Software Blades and security gateways to constantly validate that your Check Point environment is configured in the best way possible. The Check Point Compliance Software Blade provides 24/7 security monitoring, security alerts on policy violations, and out-of-the-box audit reports.

SmartProvisioning Software Blade. Provide centralized administration and security provisioning of Check Point devices. Using profiles, administrators can automate device configuration and easily roll out changes to settings to multiple, geographically distributed devices, via a single security management console.

User Directory Software Blade. Leverage LDAP servers to obtain identification and security information about network users, eliminating the risks associated with manually maintaining and synchronizing redundant data stores, and enabling centralized user management throughout the enterprise.

SmartWorkflow Software Blade. Provide a seamless and automated process for policy change management that helps administrators reduce errors and enhance compliance. Enforce a formal process for editing, reviewing, approving and auditing policy changes from a single console, for one-stop, total policy lifecycle management

c. **Monitoring and Analysis** When security events customers need well-defined follow-up procedures and visibility into critical security events impacting the organization. We facilitate greater insight and efficiency in event investigation with ongoing monitoring and customized reporting tailored to different stakeholder needs

Next Generation SmartEvent Software Blade. Real-time cyber threat visibility in the era of Big Data. Quickly search and analyze billions of data logs to identify critical security events. Gain greater network visibility with Next Generation SmartEvent on Smart-1 Appliances, and more easily manage big data security to make faster, more informed security decisions.

Logging and Status Software Blade. Transform data into security intelligence with SmartLog, an advanced log analyzer that delivers split-second search results providing real-time visibility into billions of log records over multiple time periods and domains.

Monitoring Software Blade. Present a complete picture of network and security performance, enabling fast responses to changes in traffic patterns or security events. The Software Blade centrally monitors Check Point devices and alerts to changes to gateways, endpoints, tunnels, remote users and security activities.

SmartReporter Software Blade. Increase the visibility of security threats by centralizing network security reporting of network, security and user activity into concise predefined or custom-built reports. Easy report generation and automatic distribution save time and money and allow organizations to maximize security investments.

Mobile Security. Today every business is a mobile business, with requirements to safeguard business data, provide secure mobile access to business documents and keep mobile devices safe from threats. Use of mobile devices and apps has introduced a wide range of new attack vectors and new data security challenges for IT. Mobile technology has made the network security challenge much bigger and more diverse - cybercriminals frequently optimize their attacks to exploit the technologies that people use the most. Document protection is limited on mobile devices. Employees use a wide variety of personal devices on the job, but few users realize the importance of preventing third parties from accessing their devices. Check Point Enterprise Mobile Security solutions provide the widest range of products to help secure the mobile world. Our offerings include:

a. **Mobile Threat Prevention**. Using smartphones and tablets to access critical business information on the go has many benefits, but it can also expose sensitive data to risk. Check Point Mobile Threat Prevention protects iOS and Android devices from advanced mobile threats, ensuring you can deploy and defend devices with confidence

b. **Mobile Document Protection**. Mobile security and complexity don t have to go hand in hand. Check Point Capsule is one seamless solution that addresses all mobile security needs. Capsule provides a secure business environment for mobile device use and protects business documents wherever they go.

Table of Contents

Endpoint Security. Check Point Endpoint Security combines data security, network security, threat prevention technologies and remote access VPN into one package for complete Windows and Mac OS X protection. This integrated suite allows you to manage security protection in a single console.

a. **Secure Data.** Most corporate laptops and PCs store proprietary data on their hard drives, and many users regularly work outside of a secure corporate environment. A data breach from a lost, stolen or compromised laptop can result in costly fines, lawsuits and lost revenue. Full Disk Encryption secures the entire hard drive. Media Encryption and Port Control secure removable media. Capsule Docs enables organizations to seamlessly protect documents, ensuring access for authorized users only. Remote Access VPN provides secure access to corporate resources when traveling or working remotely. Check Point data security solutions cover the following areas:

Full Disk Encryption

Media Encryption

Capsule Docs

Remote Access VPN

b. **Secure Devices**. Threats from malware like viruses, worms and bots change constantly. Users are targets of phishing emails that may contain links to websites infected with this malware. To prevent these new and emerging threats, IT departments need control and visibility into endpoint activity. We secure devices with products that address the following:

Firewall and Compliance Check

Anti-malware and Application Control

c. **Security Policy**. Check Point Endpoint Policy Management gives security administrators the power to enforce, manage, report and educate users with one console. With a customizable management dashboard, administrators have maximum visibility into the specific security areas important to the organization. They can take the steps to deploy and remediate endpoints to ensure compliance with company policy. Our products include solutions for:

Endpoint Policy Management

Endpoint Security Threat Forensics

Revenues by Category of Activity

The following table presents our revenues for the last three fiscal years by category of activity:

	Year Ended December 31,		
	2015	2014	2013
	(in thousands)		
Category of Activity:			
Products and licenses	$ 555,792	$ 520,312	$ 496,930
Subscriptions	$ 318,624	$ 265,021	$ 217,088
Software updates and maintenance	$ 755,422	$ 710,483	$ 680,087
Total revenues	$ 1,629,838	$ 1,495,816	$ 1,394,105

Our revenues for the last three fiscal years by geographic area are set out in Item 5 Operating and Financial Review and Prospects under the caption Overview.

Sales and Marketing

We leverage the expertise of over 2700 partners to deliver our security solutions to consumers and enterprises of all sizes around the world. Our network of partners accounts for 100% of our revenue and includes two-tier distributors, value-added resellers, retail and direct marketing partners, global systems integrators and managed service providers. In concert with our inside sales and channel sales teams, our direct sales teams work closely with our partner ecosystem to support pre-sales selling efforts to ensure that we stay close to customer requirements for current and future security solutions. In addition to our traditional outbound channels we leverage web-based e-commerce solutions to serve the needs of the majority of our consumer customers. To ensure integration with strategic applications within our customer ecosystem, we work with a variety of hardware and software suppliers such as, IBM, Hewlett-Packard, VMWare, Blue Coat Systems, Apple and Google.

Table of Contents

We drive awareness and preference for Check Point solutions through global media campaigns, thought leadership programs, digital marketing, social media, as well as press and analyst relations. We accelerate our innovation and technology agenda globally through frequent product launches and associated demand generation programs. In addition to our annual Check Point User Conference we host C-level, strategic IT and technical decision makers at a variety of custom events such as Cyber Day, CISO Roundtables, and local seminars. We also participate in targeted industry events such as RSA, CyberTech and Black Hat.

As of December 31, 2015, we had 1,679 employees and contractors dedicated to sales and marketing.

Support and Services

We operate a worldwide technical services organization which provides a wide range of services including the following: (i) technical customer support programs and plans, as well as (ii) certification and educational training on Check Point products; and (iii) professional services in implementing, upgrading and optimizing Check Point products, such as design planning and security implementation.

Our technical assistance centers in the United States, Israel, Canada and Japan offer support worldwide, 24-hour service, seven days per week. There are employees in additional locations supporting our call centers, as well as call centers operated by third parties (for consumer support only). As of December 31, 2015, we had 590 employees and contractors in our technical services organization, with 464 employees and contractors dedicated to customer service and support.

Our support solutions include both indirect and direct offerings. Channel partners provide customers with installation, training, maintenance and support, while we provide high-level technical support to our channel partners. Alternatively, our customers may elect to receive support directly from us. As part of our pre-sale support to our channel partners, we employ technical consultants and systems engineers who work closely with our channel partners to assist them with pre-sale configuration, use and application support. In addition, because of the increased demand for our portfolio of security gateway appliances, from small office locations to telco grade and capacity infrastructure platforms, we have expanded our technical support offerings around the world. This includes same and next business day replacements, on-site support availability and device pre-configuration. We have also added new ThreatCloud Managed Security Services and Incident Response. These new services are focused on helping our partners and customers maximize the effectiveness of advanced protections and mitigate and remediate critical security events quickly.

Research and Product Development

We believe that our future success will depend upon our ability to enhance our existing products, and to develop, acquire and introduce new products to address the increasingly sophisticated needs of our customers. We work closely with existing and potential customers, distribution channels and major resellers, who provide significant feedback for product development and innovation. Our product development efforts are focused on providing a unified security architecture, named the Check Point Software Blade Architecture, that functions throughout all layers of the network and devices that carry data. This includes enhancements to our current family of products and the continued development of new products to respond to the rapidly changing threat landscape through the provision of services, such as network perimeter protections, protection against cyber-threats, data protection for today s mobile environments, web security and security for managed enterprise endpoints. Our technology also centrally manages all of these layers and solutions. We develop most of our new products internally and also expect to leverage the products and technologies we have acquired. We may decide, based upon timing and cost considerations that it would be more efficient to acquire or license certain technologies or products from third parties, or to make acquisitions of other

businesses. Research and development expenses were $149 million in 2015, $133 million in 2014 and $122 million in 2013. These amounts include stock-based compensation in the amount of $12 million in 2015, $9 million in 2014 and $9 million in 2013. As of December 31, 2015, we had 1,303 employees and contractors dedicated to research and development activities and quality assurance.

Competition

Information concerning competition is provided in Item 3 Key Information under the caption Risk Factors Risks Relating to Our Business and Our Market We may not be able to successfully compete.

Proprietary Rights

We rely on a combination of copyright and trademark laws, patents, trade secrets, confidentiality procedures and contractual provisions to protect our proprietary rights. We rely on trade secret, copyright laws and patents to protect our software, documentation and other written materials. These laws provide only limited protection. Further, we generally enter into confidentiality agreements with employees, consultants, customers and potential customers, and limit access and distribution of materials and information that we consider proprietary.

We have 45 U.S. patents, 34 U.S. patents pending, and additional patents issued and patent applications pending worldwide. Our efforts to protect our patent rights and other proprietary rights may not be adequate and our competitors may independently develop technology that is similar. Additional details are provided in Item 3 Key Information under the caption Risk Factors Risks Relating to Our Business and Our Market We may not be able to successfully protect our intellectual property rights.

Table of Contents

Effect of Government Regulation on our Business

Information concerning regulation is provided in Item 5 Operating and Financial Review and Products under the caption Taxes on income and in Item 10 Additional Information under the caption Israeli taxation, foreign exchange regulation and investment programs.

Organizational Structure

We are organized under the laws of the State of Israel. We wholly own the subsidiaries listed below, directly or through other subsidiaries, unless otherwise specified in the footnotes below:

NAME OF SUBSIDIARY	COUNTRY OF INCORPORATION
Check Point Software Technologies, Inc.	United States of America (Delaware)
Check Point Software (Canada) Technologies Inc.	Canada
Check Point Software Technologies (Japan) Ltd.	Japan
Check Point Software Technologies (Netherlands) B.V.	Netherlands
Check Point Holding (Singapore) PTE Ltd.	Singapore
Check Point Holding (Singapore) PTE Ltd. (Representative Office)	Indonesia
Check Point Holding (Singapore) PTE Ltd. U.S. Branch (1)	United States of America (New York)
Israel Check Point Software Technologies Ltd. China (2)	China
Check Point Holding AB (3)	Sweden
SofaWare Technologies Ltd.	Israel
Dynasec Ltd.	Israel
Check Point Advanced Threat Prevention Ltd.	Israel
Check Point Mobile Security Ltd.	Israel

(1) Branch of Check Point Holding (Singapore) PTE Ltd.
(2) Representative office of Check Point Software Technologies Ltd.
(3) Subsidiary of Check Point Holding (Singapore) PTE Ltd. (former name: Protect Data AB)

Check Point Software Technologies (Netherlands) B.V. acts as a holding company. It wholly owns the principal operating subsidiaries listed below, unless otherwise indicated in the footnotes below:

NAME OF SUBSIDIARY	COUNTRY OF INCORPORATION
Check Point Software Technologies S.A.	Argentina
Check Point Software Technologies (Australia) PTY Ltd.	Australia
Check Point Software Technologies (Austria) GmbH	Austria
Check Point Software Technologies (Belarus) LLC	Belarus
Check Point Software Technologies (Belgium) S.A.	Belgium
Check Point Software Technologies (Brazil) LTDA	Brazil
Check Point Software Technologies (Hong Kong) Ltd. (Guangzhou office) (1)	China
Check Point Software Technologies (Hong Kong) Ltd. (Shanghai office) (1)	China

Check Point Software Technologies (Czech Republic) s.r.o.	Czech Republic
Check Point Software Technologies (Denmark) ApS	Denmark
Check Point Software Technologies (Finland) Oy	Finland
Check Point Software Technologies SARL	France
Check Point Software Technologies GmbH	Germany
Check Point Software Technologies (Greece) SA	Greece
Check Point Software Technologies (Hu	