QUALYS, INC.
Form 10-K
March 05, 2013
Table of Contents

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

_____

FORM 10-K

_____

x Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934
For the Annual Period Ended December 31, 2012
or
o Transition Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934
For the transition period from to
Commission file number 001-35662

_____

QUALYS, INC.
(Exact name of registrant as specified in its charter)

_____

Delaware	77-0534145
(State or other jurisdiction of incorporation or organization)	(I.R.S. Employer Identification Number)

1600 Bridge Parkway, Redwood City, California 94065
(Address of principal executive offices, including zip code)
(650) 801-6100
(Registrant’s telephone number, including area code)

_____

Securities registered pursuant to section 12(b) of the Act:

Title of each class	Name of each exchange on which registered
Common stock, $0.001 par value per share	NASDAQ Stock Market

Securities registered pursuant to section 12(g) of the Act: None
Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes o No x
Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes o 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 o
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 during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files). Yes x No o
Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K(§229.405 of this chapter) is not contained herein, and will not be contained, to the best of registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this From 10-K or any amendment to this Form 10-K. x
Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or a smaller reporting company. See the definitions of “large accelerated filer,” “accelerated filer” and “smaller reporting

company" in Rule 12b-2 of the Exchange Act. (Check one):

Large accelerated filer o	Accelerated filer o	Non-accelerated filer x (Do not check if a smaller reporting company)	Smaller reporting company o

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes o No x

The registrant's common stock began trading on the NASDAQ Stock Market on September 28, 2012. As of December 31, 2012, the aggregate market value of voting shares of common stock held by non-affiliates of the registrant was $216.6 million based on the last reported sale price of the registrant's common stock on December 31, 2012. Shares of common stock held by each executive officer and director and by each person who owns 5% or more of the outstanding common stock have been excluded in that such persons may be deemed to be affiliates. This determination of affiliate status is not necessarily a conclusive determination for other purposes.

The number of shares of the Registrant's common stock outstanding as of February 28, 2013 was 31,547,650 shares.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's Proxy Statement for its 2013 Annual Meeting of Stockholders are incorporated by reference in Part III of this Annual Report on Form 10-K where indicated. Such proxy statement will be filed with the Securities and Exchange Commission within 120 days of the registrant's fiscal year ended December 31, 2012.

Table of Contents

Qualys, Inc.
TABLE OF CONTENTS

Table of Contents

PART I

Forward-Looking Statements

In addition to historical information, this Annual Report on Form 10-K contains “forward-looking” statements within the meaning of the federal securities laws, which statements involve substantial risks and uncertainties. Forward-looking statements generally relate to future events or our future financial or operating performance. In some cases, it is possible to identify forward-looking statements because they contain words such as “anticipates,” “believes,” “contemplates,” “continue,” “could,” “estimates,” “expects,” “future,” “intends,” “likely,” “may,” “plans,” “potential,” “predic “should,” “target” or “will,” or the negative of these words or other similar terms or expressions that concern our expectations, strategy, plans or intentions. Forward-looking statements contained in this Annual Report on 10-K include, but are not limited to, statements about:

- our financial performance, including our revenues, costs, expenditures, growth rates, operating expenses and ability to generate positive cash flow to attain and sustain profitability;
- anticipated technology trends, such as the use of cloud solutions;
- our ability to adapt to changing market conditions;
- economic and financial conditions, including volatility in foreign exchange rates;
- our ability to diversify our sources of revenues;
- the effects of increased competition in our market;
- our ability to effectively manage our growth;
- our anticipated investments in sales and marketing and research and development;
- maintaining and expanding our relationships with channel partners;
- our ability to maintain, protect and enhance our brand and intellectual property;
- costs associated with defending intellectual property infringement and other claims;
- our ability to attract and retain qualified employees and key personnel;
- our ability to successfully enter new markets and manage our international expansion; and
- other factors discussed in this Annual Report on Form 10-K in the sections titled “Risk Factors,” “Management's Discussion and Analysis of Financial Condition and Results of Operations” and “Business.”

We have based the forward-looking statements contained in this Annual Report on Form 10-K primarily on our current expectations and projections about future events and trends that we believe may affect our business, financial condition, results of operations and prospects. The outcome of the events described in this forward-looking statements is subject to risks, uncertainties, assumptions, and other factors including those described in Part I, Item 1A (Risk Factors) of this Annual Report. Moreover, we operate in a very competitive and rapidly changing environment. New risks and uncertainties emerge from time to time, and it is not possible for us to predict all risks and uncertainties that could have an impact on the forward-looking statements used herein. We cannot provide assurance that the results, events, and circumstances reflected in the forward-looking statements will be achieved or occur, and actual results, events or circumstances could differ materially from those described in the forward-looking statements.

You should not rely on forward-looking statements as predictions of future events. Except as required by law, neither we nor any other person assumes responsibility for the accuracy and completeness of the forward-looking statements, and we undertake no obligation to update any forward-looking statements to reflect events or circumstances after the date of such statements.

Qualys, the Qualys logo and QualysGuard, and other trademarks and service marks of Qualys appearing in this Annual Report on Form 10-K are the property of Qualys. This Annual Report on Form 10-K also contains trademarks and trade names of other businesses that are the property of their respective holders. We have omitted the ® and ™ designations, as applicable, for the trademarks used in this Annual Report on Form 10-K.

3

Table of Contents

Item 1. Business

Overview

We are a pioneer and leading provider of cloud security and compliance solutions that enable organizations to identify security risks to their IT infrastructures, help protect their IT systems and applications from ever-evolving cyber attacks and achieve compliance with internal policies and external regulations. Our cloud solutions address the growing security and compliance complexities and risks that are amplified by the dissolving boundaries between internal and external IT infrastructures and web environments, the rapid adoption of cloud computing and the proliferation of geographically dispersed IT assets. Our integrated suite of security and compliance solutions delivered on our QualysGuard Cloud Platform enable our customers to identify their IT assets, collect and analyze large amounts of IT security data, discover and prioritize vulnerabilities, recommend remediation actions and verify the implementation of such actions. Organizations use our integrated suite of solutions delivered on our QualysGuard Cloud Platform to cost-effectively obtain a unified view of their security and compliance posture across globally-distributed IT infrastructures.

IT infrastructures are more complex and globally-distributed today than ever before, as organizations of all sizes increasingly rely upon myriad interconnected information systems and related IT assets, such as servers, databases, web applications, routers, switches, desktops, laptops, other physical and virtual infrastructure, and numerous external networks and cloud services. In this environment, new and evolving technologies intended to improve organizations' operations can also increase vulnerability to cyber attacks, which can expose sensitive data, damage IT and physical infrastructures, and result in serious financial or reputational consequences. In addition, the rapidly increasing amount of data and devices in IT environments makes it more difficult to identify and remediate vulnerabilities in a timely manner. The predominant approach to IT security has been to implement multiple disparate security products that can be costly and difficult to deploy, integrate and manage and may not adequately protect organizations. As a result, we believe there is a large and growing opportunity for comprehensive cloud security and compliance solutions.

We designed our QualysGuard Cloud Platform to transform the way organizations secure and protect their IT infrastructures and applications. Our cloud platform offers an integrated suite of solutions that automates the lifecycle of asset discovery, security assessments, and compliance management for an organization's IT infrastructure and assets, whether they reside inside the organization, on their network perimeter or in the cloud. Since inception, our solutions have been designed to be delivered through the cloud and to be easily and rapidly deployed on a global scale across a broad range of industries, enabling faster implementation and lower total cost of ownership than traditional on-premise enterprise software products. Our customers, ranging from some of the largest organizations to small businesses, are all served from our globally-distributed cloud platform, enabling us to rapidly deliver new solutions, enhancements and security updates.

We were founded and incorporated in December 1999 with a vision of transforming the way organizations secure and protect their IT infrastructure and applications and initially launched our first cloud solution, QualysGuard Vulnerability Management, in 2000. This solution has provided the substantial majority of our revenues to date, representing 87%, 90% and 92% of total revenues in 2012, 2011 and 2010, respectively. As this solution gained acceptance, we introduced new solutions to help customers manage increasing IT security and compliance requirements. In 2006, we added our PCI Compliance solution, and in 2008, we added our Policy Compliance solution. In 2009, we broadened the scope of our cloud services by adding Web Application Scanning. We continued our expansion in 2010, launching Malware Detection Service and Qualys SECURE Seal for automated protection of websites. On September 28, 2012, our common stock commenced trading on the NASDAQ Stock Market under the trading symbol "QLYS," and on October 3, 2012 we closed our initial public offering.

We provide our solutions through a software-as-a-service model, primarily with renewable annual subscriptions. These subscriptions require customers to pay a fee in order to access our cloud solutions. We invoice our customers for the entire subscription amount at the start of the subscription term, and the invoiced amounts are treated as deferred revenues and are recognized ratably over the term of each subscription. Historically, we have experienced significant revenue growth from existing customers as they renew and purchase additional subscriptions. Revenues

from customers existing at or prior to December 31, 2011 grew $7.8 million to $84.0 million during 2012. We expect this trend to continue.

Table of Contents

Our QualysGuard Cloud Platform is currently used by over 6,150 organizations in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. Our revenues increased from $65.4 million in 2010 to $76.2 million in 2011, and reached $91.4 million in 2012. We generated net income of $0.8 million in 2010, $2.0 million in 2011, and $2.3 million in 2012. Total assets as of December 31, 2012 and 2011 were $170.3 million and $68.8 million, respectively.

Our Growth Strategy

We intend to leverage our innovation and extensive expertise to strengthen our leadership position as a trusted provider of cloud security and compliance solutions. The key elements of our growth strategy are:

- Continue to innovate and enhance our cloud platform and suite of solutions. We intend to continue to make significant investments in research and development to extend our cloud platform's functionality by developing new security solutions and further enhancing our existing suite of solutions. In 2012, we introduced several new solutions on our platform, including our Web Application Scanning and Zero-Day Risk Analyzer, and have additional solutions under development.
- Expand the use of our suite of solutions by our large and diverse customer base. With more than 6,150 customers across many industries and geographies, we believe we have a significant opportunity to sell additional solutions to our customers and expand their use of our suite of solutions. Since the majority of our customers initially deploy only one of our solutions and in select parts of their IT infrastructures, our existing customers serve as a strong source of new sales. In this regard, we have significantly expanded our sales execution and marketing functions to increase adoption of our newly developed solutions among our existing customers.
- Drive new customer growth. We are pursuing new customers by targeting key accounts and expanding our sales and marketing organization and network of channel partners. We will continue to seek to make significant investments to encourage organizations to replace their existing security products with our cloud solutions.
- Broaden our global reach. We intend to expand our relationships with key security consulting organizations, managed security service providers and value added resellers to accelerate the adoption of our cloud platform. We seek to strengthen existing relationships as well as establish new relationships to increase the distribution and market awareness of our cloud platform and target new geographic regions.
- Selectively pursue technology acquisitions to bolster our capabilities and leadership position. We may explore acquisitions that are complementary to and can expand the functionality of our cloud platform. We may also seek to acquire technology teams to supplement our own team and increase the breadth of our cloud security and compliance solutions.

Our Platform

Our QualysGuard Cloud Platform consists of a suite of IT security and compliance solutions that leverage our shared and extensible core services and our highly scalable multi-tenant cloud infrastructure.

Our suite of solutions provides security intelligence by automating the life cycle of IT asset discovery, security assessment and compliance management. Our core services layer provides a set of advanced shared technologies that are leveraged by our suite of security and compliance solutions, which we refer to as our Core Services.

Built on our cloud platform infrastructure, our Core Services provide an integrated framework with proprietary functionalities that act as building blocks to enable efficient and scalable delivery of our customer-facing cloud solutions. Our cloud platform's infrastructure includes integrated services that deliver a highly automated and scalable scanning infrastructure capable of scanning IT systems and web applications, inside and outside corporate firewalls. The Core Services and infrastructure layers of our cloud platform deliver benefits to our entire suite of security and compliance solutions, including:

- Dynamic and interactive user interfaces with configurable report templates to present scan data with a wide range of presentation options to match a customer's needs;
- Fast searching of several extensive QualysGuard data sets, including scan results, asset data, scan profiles, users and vulnerabilities;

Table of Contents

- Asset management technology for hierarchical asset categorization via dynamic tagging and role-based customer access management; and
- Distributed scanning platform for global cloud-based environments.

We also provide open application program interfaces, or APIs, and other developer tools that allow third parties to embed our technology into their solutions and build applications on our cloud platform.

QualysGuard Cloud Suite

Our suite of solutions, which we refer to as the QualysGuard Cloud Suite, currently includes six solutions: Vulnerability Management, Web Application Scanning, Malware Detection Service, Policy Compliance, PCI Compliance and Qualys SECURE Seal. This integrated set of cloud solutions enables organizations to:

- Discover and catalogue information assets inside the organization, on the perimeter, or in the cloud;
- Manage assets on an ongoing basis to establish a trusted repository for IT system configurations and to maintain hierarchical relationships between them;
- Design policies to establish a secure and compliant IT infrastructure and automate ongoing security and compliance assessments of IT systems and applications in accordance with best practices;
- Proactively identify and help fix vulnerabilities to mitigate security risks and achieve compliance;
- Monitor and measure security and compliance through a unified user interface; and
- Distribute security and compliance reports tailored to differing customer needs, including management personnel, auditors and security professionals.

Our customers can subscribe to one or more of our security and compliance solutions based on their initial needs and expand their subscriptions over time to new areas within their organization or to additional QualysGuard solutions. We offer two editions of our QualysGuard Cloud Suite, the Enterprise edition for large and medium-sized enterprises and the Express edition for small and medium-sized businesses. QualysGuard Cloud Suite solutions are described below.

QualysGuard Vulnerability Management

QualysGuard Vulnerability Management, or QualysGuard VM, is an industry leading and award-winning solution that automates network auditing and vulnerability management across an organization, including network discovery and mapping, asset management, vulnerability reporting, and remediation tracking. Driven by our comprehensive KnowledgeBase of known vulnerabilities, QualysGuard VM enables cost-effective protection against vulnerabilities without substantial resource deployment.

QualysGuard Policy Compliance

QualysGuard Policy Compliance, or QualysGuard PC, allows customers to analyze and collect configuration and access control information from their networked devices and web applications and automatically maps this information to internal policies and external regulations in order to document compliance. QualysGuard PC is fully automated and helps reduce customers' cost of compliance without requiring the use of software agents.

QualysGuard PCI Compliance

QualysGuard PCI Compliance, or QualysGuard PCI, provides organizations that store cardholder data a cost-effective and highly automated solution to verify and document compliance with PCI DSS. QualysGuard PCI allows merchants to complete the annual PCI Self-Assessment Questionnaire, or SAQ, to perform vulnerability scanning for quarterly PCI audits and to meet the demands of PCI for web application security.

QualysGuard Web Application Scanning

QualysGuard Web Application Scanning, or QualysGuard WAS, uses the scalability of our cloud platform to allow customers to discover, catalog and scan a large number of web applications. QualysGuard WAS scans and analyzes custom web applications and identifies vulnerabilities that threaten underlying databases or bypass access controls. These web applications are often the main attack vectors for cyber attackers.

Table of Contents

QualysGuard Malware Detection Service

QualysGuard Malware Detection Service, or QualysGuard MDS, provides organizations with the ability to scan, identify and remove malware infections from their websites. QualysGuard MDS utilizes behavioral and static analysis to provide malware detection to organizations. It provides periodic scanning to monitor websites and delivers email alerts to notify customers of infections.

QualysGuard Web Application Firewall

QualysGuard Web Application Firewall, or QualysGuard WAF, currently in beta testing, delivers enterprise-grade web application security without the costs, footprint, and complexity associated with appliance-based web application firewall solutions. It is designed to protect web applications from attack vectors by enhancing default web application configurations and virtual patching. QualysGuard WAF can improve website performance by reducing page load times and optimizing bandwidth.

Qualys SECURE Seal

QualysGuard SECURE Seal helps organizations demonstrate to their online customers that they maintain a proactive security program. This solution includes scanning for the presence of malware, network and web application vulnerabilities and for SSL certificate validation. Websites that regularly perform these security scans with no critical security issues detected can display a QualysGuard SECURE Seal on their website to demonstrate to visitors that they are proactively securing their websites.

QualysGuard Core Services

Our Core Services enable integrated workflows, management and real-time analysis and reporting across all of our IT security and compliance solutions. Our Core Services include:

- Asset Tagging and Management. Enables customers to easily identify, categorize and manage large numbers of assets in highly dynamic IT environments and automates the process of inventory management and hierarchical organization of IT assets.
- Reporting and Dashboards. A highly configurable reporting engine that provides customers with reports and dashboards based on their roles and access privileges.
- Questionnaires and Collaboration. A configurable workflow engine that enables customers to easily build questionnaires and capture existing business processes and workflows to evaluate controls and gather evidence to validate and document compliance.
- Remediation and Workflow. An integrated workflow engine that allows customers to automatically generate helpdesk tickets for remediation and to manage compliance exceptions based on customer-defined policies, enabling subsequent review, commentary, tracking and escalation. This engine automatically distributes remediation tasks to IT administrators upon scan completion, tracks remediation progress and closes open tickets once patches are applied and remediation is verified in subsequent scans.
- Big Data Correlation and Analytics Engine. Provides capabilities for indexing, searching and correlating large amounts of security and compliance data with other security incidents and third-party security intelligence data. Embedded workflows enable customers to quickly assess risk and access information for remediation, incident analysis and forensic investigations.
- Alerts and Notifications. Creates email notifications to alert customers of new vulnerabilities, malware infections, scan completion, open trouble tickets and system updates.

QualysGuard Cloud Infrastructure

Our infrastructure layer, which we refer to as our Infrastructure, includes the data, data processing capabilities, software and hardware infrastructure and infrastructure management capabilities that provide the foundation for our cloud platform and allow us to automatically scale our Infrastructure and Core Services to scan millions of IPs. Each Infrastructure service is described below:

- Scalable Capacity. We have designed a modular and scalable infrastructure that leverages virtualization and cloud technologies. This allows our operations team to dynamically allocate additional capacity on-demand across our entire QualysGuard Cloud Platform to address the growth and scalability of our solutions.

Table of Contents

- Big Data Indexing and Storage. Built on top of our secure data storage model, this engine indexes petabytes of data and uses this information in real-time to execute tags or rules to dynamically update IT assets' properties, which are used in various workflows for scanning, reporting and remediation.
- QualysGuard KnowledgeBase. QualysGuard relies on our comprehensive repository, which we refer to as our KnowledgeBase, of known vulnerabilities and compliance controls for a wide range of devices, technologies and applications that powers our security and compliance scanning technology. We update our KnowledgeBase daily with signatures for new vulnerabilities, control checks, validated fixes and improvements.
- Managed Scanner Appliances. As part of our cloud platform, we host and operate a large number of globally distributed physical scanner appliances that our customers use to scan their externally facing systems and web applications. To scan internal IT assets, customers can also deploy our scanners, which are available on a subscription basis as physical appliances or downloadable virtual images, within their internal networks. Our scanner appliances self-update daily in a transparent manner using our automated and proprietary scan management technology. These scanner appliances allow us to scale our cloud platform to scan networked devices and web applications across organizations' networks around the world.

Our Customers

We market and sell our solutions to enterprises, government entities and to small and medium size businesses across a broad range of industries, including education, financial services, government, healthcare, insurance, manufacturing, media, retail, technology and utilities. As of December 31, 2012, we had over 6,150 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. In each of 2012, 2011 and 2010, no one customer accounted for more than 10% of our revenues. In 2012, 2011 and 2010, approximately 68%, 67% and 67%, respectively, of our revenues were derived from customers in the United States. We sell our solutions to enterprises and government entities primarily through our field sales force and to small and medium-sized businesses through our inside sales force. We generate a significant portion of sales through our channel partners, including managed service providers, value-added resellers and consulting firms in the United States and internationally.

Sales and Marketing

Sales

We market and sell our IT security and compliance solutions to customers directly through our sales teams as well as indirectly through our network of channel partners.

Our global sales force is organized into a field sales team, which focuses on enterprises, generally including organizations with more than 4,000 employees, and an inside sales team, which focuses on small to medium businesses, which generally include organizations with less than 4,000 employees. Both our field and inside sales teams are divided into three geographic regions, including the Americas; Europe, Middle East and Africa; and Asia-Pacific. We also further segment each of our sales teams into groups that focus on adding new customers or expanding relationships with existing customers.

Our channel partners maintain relationships with their customers throughout the territories in which they operate and provide their customers with services and third-party solutions to help meet those customers' evolving security and compliance requirements. As such, these partners offer our IT security and compliance solutions in conjunction with one or more of their own products or services and act as a conduit through which we can connect with these prospective customers to offer our solutions. Our channel partners include security consulting organizations, managed service providers and resellers, such as Computacenter UK Ltd., Dell Inc., FishNet Security, Inc., Insight Technologies, Inc., Symantec Corporation and Verizon Communications Inc.

Table of Contents

For sales involving a channel partner, the channel partner engages with the prospective customer directly and involves our sales team as needed to assist in developing and closing an order. When a channel partner secures a sale, we sell the associated subscription to the channel partner who in turn resells the subscription to the customer, with the channel partner earning a fee based on the total value of the order. Once the order is completed, we provide these customers with direct access to our solutions and other associated back-office applications, enabling us to establish a direct relationship as part of ensuring customer satisfaction with our solutions. At the end of the subscription term, the channel partner engages with the customer to execute a renewal order, with our sales team providing assistance as required. In 2012, 2011 and 2010, 40%, 38% and 33%, respectively, of our revenues were generated by channel partners.

Marketing

Our marketing programs include a variety of online marketing, advertising, conferences, events, public relations activities and web-based seminar campaigns targeted at key decision makers within our prospective customers.

We have a number of marketing initiatives to build awareness and encourage customer adoption of our solutions. We offer free trials and services to allow prospective customers to experience the quality of our solutions, to learn in detail about the features and functionality of our cloud platform, and to quantify the potential benefits of our solutions.

Customer Support

We deliver 24x7x365 customer support from centers located in Redwood City, California; Durham, North Carolina; and Slough, United Kingdom. We recruit senior level technical personnel and trained subject matter experts who work closely with engineering and operations personnel to resolve issues quickly. Our security and compliance solutions can be deployed easily and are designed to be implemented and operated without the need for any professional services. Accordingly, we do not sell any professional services. However, we do offer various training programs as part of our subscriptions to all of our customers. We believe that our customer support helps ensure customer satisfaction and is critical to retaining and expanding our customer base. In addition, we leverage the insights drawn from our customers to further improve the functionality of our security and compliance solutions.

Research and Development and Operations

We devote significant resources to maintain, enhance and add new functionality to our QualysGuard Cloud Platform and the integrated suite of solutions that we offer. Our development organization consists of agile engineering teams with substantial security expertise in specific areas of our solutions. In addition to our development teams, we have also built a sophisticated research team focused on identifying threats and developing signatures for vulnerabilities and compliance checks so that we can provide our customers with daily updates and enable them to scan their assets for the latest threats. We conduct our research and development in the United States, Brazil, China, France, India, and United Kingdom, which gives us access to some of the best research and engineering talent in the world. Our focus remains to attract engineering talent as we continue to add new solutions and improve existing ones.

Our development team works closely with our customers and partners to gain valuable insights into their environments and gather feedback for threat research, product development and innovations. We typically release updates to our solutions, including enhancements and new features multiple times a year, and we measure the quality of our scan results on a frequent basis in an effort to maintain the highest level of scan accuracy.

The modular architecture of our cloud platform enables our engineering teams to simultaneously work on different features, accelerating the delivery of new functionalities to customers. Our research and development team also works collaboratively with our technical support team to ensure customer satisfaction and with our sales team to accelerate the adoption of our solutions.

Research and development expenses were $20.2 million, $19.6 million and $15.8 million for 2012, 2011 and 2010, respectively.

Table of Contents

Manufacturing Agreement

Our physical appliances are provided by SYNNEX Corporation, or SYNNEX, pursuant to a manufacturing services agreement dated March 1, 2011. Under this agreement, SYNNEX manufactures, assembles and tests our physical scanner appliances. This agreement has an initial term of one year, which is automatically renewed for additional one-year terms, unless terminated (i) at anytime upon the mutual written agreement of us and SYNNEX, (ii) by either party upon 90 days or more written notice, (iii) upon written notice, subject to applicable cure periods, if the other party has materially breached its obligations under the agreement or (iv) by either party upon the other party seeking an order for relief under the bankruptcy laws of the United States or similar laws of any other jurisdiction, a composition with or assignment for the benefit of creditors, or dissolution or liquidation.

Data Center Agreements

Our data center operations are provided by Savvis Communications Corporation, or Savvis, pursuant to a master services agreement dated June 22, 2010, and Interoute Communications Limited, or Interoute, pursuant to a master agreement dated March 31, 2008. Under these agreements, Savvis and Interoute provide us with data center space in various locations. The Savvis agreement had an initial term of 24 months; upon the completion of this initial term, services have automatically continued to renew for successive one month periods. The provision of renewed service for such successive one month periods may be terminated by either party upon the provision of upon written notice, subject to applicable cure periods if the other party has materially breached its obligations under the agreement. As of December 31, 2012, we are seeking to negotiate a 24 month renewal under the original master services agreement. The Interoute agreement has an initial term of three years, which is automatically renewed for additional one-year terms, unless terminated (i) immediately upon written notice, subject to applicable cure periods, if the other party has materially breached its obligations, or breached certain specific obligations under the agreement or (ii) by Interoute in the event that we engage in fraud, fail to make undisputed payments or violate certain Interoute policies.

Competition

The expanding capabilities of our security and compliance solutions have enabled us to address a growing array of opportunities in the cloud IT security and compliance market. We compete with a large and broad array of established and emerging vulnerability management vendors, compliance vendors and data security vendors in a highly fragmented and competitive environment.

We compete with large public companies, such as Hewlett-Packard Company, Imperva, Inc., International Business Machines Corporation, McAfee, Inc. (a subsidiary of Intel Corporation) and Symantec Corporation, as well as private security providers including Barracuda Networks, Inc., BeyondTrust Software, Inc., Lumension Security, Inc., nCircle Network Security, Inc., NetIQ Corporation, Rapid7 LLC, Tenable Network Security, Inc. and Trustwave Holdings, Inc. We also seek to replace IT security and compliance solutions that organizations have developed internally. As we continue to extend our cloud platform’s functionality by further developing security and compliance solutions, such as web application scanning and firewalls, we expect to face additional competition in these new markets.

We believe that the principal competitive factors affecting the market for cloud security and compliance solutions include product functionality, breadth of offerings, flexibility of delivery models, ease of deployment and use, total cost of ownership, scalability and performance, customer support and extensibility of platform. We believe that our suite of solutions generally competes favorably with respect to these factors. However, many of our primary competitors have greater name recognition, longer operating histories, more established customer relationships, larger marketing budgets and significantly greater resources than we do.

Table of Contents

Intellectual Property

We rely on a combination of trade secrets, copyrights, patents and trademarks, as well as contractual protections, to establish and protect our intellectual property rights and protect our proprietary technology. We have one issued patent, several pending U.S. patent applications and an inbound license to four U.S. patents, which was obtained in connection with our acquisition of Nemean. The inbound license remains in effect until the licensed patents are no longer enforceable, unless the applicable license agreement is first terminated by us or terminated by the licensor for a breach of the agreement or if we undergo certain bankruptcy events. The licenses are currently exclusive and will remain exclusive so long as we make an appropriately-timed written election and pay an annual fixed royalty for ten years thereafter. These exclusive licenses are subject to the licensor's reservation of certain rights in the patents and subject to the U.S. government's reserved rights in the technology. We have a number of registered and unregistered trademarks. We require our employees, consultants and other third parties to enter into confidentiality and proprietary rights agreements and control access to software, documentation and other proprietary information. We view our trade secrets and know-how as a significant component of our intellectual property assets, as we have spent years designing and developing our QualysGuard Cloud Platform, which we believe differentiates us from our competitors.

Despite our efforts to protect our proprietary technology and our intellectual property rights, unauthorized parties may attempt to copy or obtain and use our technology to develop products with the same functionality as our solution. Policing unauthorized use of our technology and intellectual property rights is difficult.

We expect that software and other solutions in our industry may be subject to third-party infringement claims as the number of competitors grows and the functionality of products in different industry segments overlaps. Any of these third parties might make a claim of infringement against us at any time.

Employees

As of December 31, 2012, we had 359 full-time employees, including 123 in research and development, 137 in sales and marketing, 58 in operations and customer support and 41 in general and administrative. As of December 31, 2012, we had 264 employees in the United States and 95 employees internationally. None of our U.S. employees are covered by collective bargaining agreements. Employees in certain European countries have the benefits of collective bargaining arrangements at the national level. We believe our employee relations are good and we have not experienced any work stoppages.

Available Information

Our principal executive offices are located at 1600 Bridge Parkway, Redwood City, California 94065. The telephone number of our principal executive offices is (650) 801-6100, and our main corporate website is www.qualys.com. Information contained on, or that can be accessed through, our website, does not constitute part of this Annual Report on Form 10-K and inclusion of our website address in this Annual Report on Form 10-K is an inactive textual reference only.

We make available our Annual Reports on Form 10-K, Quarterly Reports on Form 10-Q, Current Reports on Form 8-K and amendments to those reports filed or furnished pursuant to Section 13(a) or Section 15(d) of the Securities Exchange Act of 1934, as amended, free of charge on our website, www.qualys.com as soon as reasonably practicable after they are electronically filed with or furnished to the Securities and Exchange Commission or SEC. Additionally, copies of materials filed by us with the SEC may be accessed at the SEC's Public Reference Room at 100 F Street, N.E., Washington, D.C. 20549 or at the SEC's website, www.sec.gov. For information about the SEC's Public Reference Room, contact 1-800-SEC-0330.

Item 1A. Risk Factors

An investment in our common stock involves a high degree of risk. You should carefully consider the risks and uncertainties described below, and all other information contained in this Annual Report on Form 10-K, including our consolidated financial statements and the related notes, before making a decision to invest in our common stock. Our business, operating results, financial condition, or prospects could be materially and adversely affected by any of these risks and uncertainties. In that case, the trading price of our common stock could decline, and you might lose all or part or all of your investment. In addition, the risks and uncertainties discussed below are not the only ones we face.

Our business, operating results, financial performance or prospects could also be harmed by risks and uncertainties not currently known to us or that we currently do not believe are material.

Table of Contents

We have a limited history of profitability and may not achieve or maintain profitability in the future.

We have not been consistently profitable on a quarterly or annual basis. While we have experienced significant revenue growth over recent years, we may not be able to sustain or increase our growth or return to profitability in the future. Although we had net income for each of the three years ended December 31, 2012, 2011 and 2010, we had net losses in the fourth quarter of 2011 and in the first two quarters of 2012. The net losses were primarily due to increased sales and marketing activities during those quarters as we continued to expand our worldwide customer base as well as focus on the promotion of our new solutions. We plan to continue to invest in our infrastructure, new solutions, research and development and sales and marketing, and as a result, we cannot assure you that we will maintain profitability. In addition, as a public company, we incur significant accounting, legal and other expenses that we did not incur as a private company. As a result of these increased expenditures, we will have to generate and sustain increased revenues to achieve future profitability. We may incur losses in the future for a number of reasons, including without limitation, the other risks and uncertainties described in this Annual Report on Form 10-K. Additionally, we may encounter unforeseen operating expenses, difficulties, complications, delays and other unknown factors that may result in losses in future periods. If our revenue growth does not meet our expectations in future periods, our financial performance may be harmed and we may not again achieve or maintain profitability in the future.

If the market for cloud solutions for IT security and compliance does not evolve as we anticipate, our revenues may not grow and our operating results would be harmed.

Our success depends to a significant extent on the willingness of organizations to increase their use of cloud solutions for their IT security and compliance. However, the market for cloud solutions for IT security and compliance is at an early stage relative to on-premise solutions, and as such, it is difficult to predict important market trends, including the potential growth, if any, of the market for cloud security and compliance solutions. To date, some organizations have been reluctant to use cloud solutions because they have concerns regarding the risks associated with the reliability or security of the technology delivery model associated with these solutions. If other cloud service providers experience security incidents, loss of customer data, disruptions in service delivery or other problems, the market for cloud solutions as a whole, including our solutions, may be negatively impacted. Moreover, many organizations have invested substantial personnel and financial resources to integrate on-premise software into their businesses, and as a result may be reluctant or unwilling to migrate to a cloud solution. Organizations that use on-premise security products, such as network firewalls, security information and event management products or data loss prevention solutions, may also believe that these products sufficiently protect their IT infrastructure and deliver adequate security. Therefore, they may continue spending their IT security budgets on these products and may not adopt our security and compliance solutions in addition to or as a replacement for such products.

If the market for cloud solutions for IT security and compliance does not evolve in the way we anticipate or if customers do not recognize the benefits of our cloud solutions over traditional on-premise enterprise software products, and as a result we are unable to increase sales of subscriptions to our solutions, then our revenues may not grow or may decline, and our operating results would be harmed.

If we do not successfully anticipate market needs and opportunities or are unable to enhance our solutions and develop new solutions that meet those needs and opportunities on a timely basis, we may not be able to compete effectively and our business and financial condition may be harmed.

The IT security and compliance market is characterized by rapid technological advances, changes in customer requirements, frequent new product introductions and enhancements and evolving industry standards and regulatory mandates. We must also continually change and improve our solutions in response to changes in operating systems, application software, computer and communications hardware, networking software, data center architectures,

programming tools and computer language technology.

We may not be able to anticipate future market needs and opportunities or develop enhancements or new solutions to meet such needs or opportunities in a timely manner or at all. The market for cloud solutions for IT security and compliance is relatively new, and it is uncertain whether our new solutions will gain market acceptance.

Our solution enhancements or new solutions could fail to attain sufficient market acceptance for many reasons, including:

Table of Contents

- failure to timely meet market demand for product functionality;
- inability to identify and provide intelligence regarding the attacks or techniques used by cyber attackers;
- inability to interoperate effectively with the database technologies, file systems or web applications of our prospective customers;
- defects, errors or failures;
- delays in releasing our enhancements or new solutions;
- negative publicity about their performance or effectiveness;
- introduction or anticipated introduction of products by our competitors;
- poor business conditions, causing customers to delay IT security and compliance purchases;
- easing or changing of external regulations related to IT security and compliance; and
- reluctance of customers to purchase cloud solutions for IT security and compliance.

Furthermore, diversifying our solutions and expanding into new IT security and compliance markets will require significant investment and planning, require that our research and development and sales and marketing organizations develop expertise in these new markets, bring us more directly into competition with security and compliance providers that may be better established or have greater resources than we do, require additional investment of time and resources in the development and training of our channel partners and entail significant risk of failure.

If we fail to anticipate market requirements or fail to develop and introduce solution enhancements or new solutions to satisfy those requirements in a timely manner, such failure could substantially decrease or delay market acceptance and sales of our present and future solutions and cause us to lose existing customers or fail to gain new customers, which would significantly harm our business, financial condition and results of operations.

If we fail to continue to effectively scale and adapt our platform to meet the performance and other requirements of our customers, our operating results and our business would be harmed.

Our future growth is dependent upon our ability to continue to meet the expanding needs of our customers as their use of our cloud platform grows. As these customers gain more experience with our solutions, the number of users and the number of locations where our solutions are being accessed may expand rapidly in the future. In order to ensure that we meet the performance and other requirements of our customers, we intend to continue to make significant investments to develop and implement new proprietary and third-party technologies at all levels of our cloud platform. These technologies, which include databases, applications and server optimizations, and network and hosting strategies, are often complex, new and unproven. We may not be successful in developing or implementing these technologies. To the extent that we do not effectively scale our platform to maintain performance as our customers expand their use of our platform, our operating results and our business may be harmed.

Our quarterly operating results may vary from period to period, which could result in our failure to meet expectations with respect to operating results and cause the trading price of our stock to decline.

Our operating results have historically varied from period to period, and we expect that they will continue to do so as a result of a number of factors, many of which are outside of our control, including:

- the level of demand for our solutions;
- changes in customer renewals of our solutions;
- the extent to which customers subscribe for additional solutions;
- seasonal buying patterns of our customers;
- the level of perceived threats to IT security;
- security breaches, technical difficulties or interruptions with our service;
- changes in the growth rate of the IT security and compliance market;

13

Table of Contents

- the timing and success of new product or service introductions by us or our competitors or any other changes in the competitive landscape of our industry, including consolidation among our competitors;
- the introduction or adoption of new technologies that compete with our solutions;
- decisions by potential customers to purchase IT security and compliance products or services from other vendors;
- the amount and timing of operating costs and capital expenditures related to the operations and expansion of our business;
- the timing of sales commissions relative to the recognition of revenues;
- the announcement or adoption of new regulations and policy mandates or changes to existing regulations and policy mandates;
- price competition;
- insolvency or credit difficulties confronting our customers, affecting their ability to purchase or pay for our solutions;
- changes in foreign currency exchange rates;
- general economic conditions, both domestically and in the foreign markets in which we sell our solutions; and
- future accounting pronouncements or changes in our accounting policies.

Each factor above or discussed elsewhere in this Annual Report on Form 10-K or the cumulative effect of some of these factors may result in fluctuations in our operating results. This variability and unpredictability could result in our failure to meet expectations with respect to operating results, or those of securities analysts or investors, for a particular period. In addition, a significant percentage of our operating expenses are fixed in nature and based on forecasted trends in revenues. Accordingly, in the event of shortfalls in revenues, we are generally unable to mitigate the negative impact on margins in the short term by reducing our operating expenses. If we fail to meet or exceed expectations for our operating results for these or any other reasons, the trading price of our common stock could fall and we could face costly lawsuits, including securities class action suits.

Adverse economic conditions or reduced IT spending may adversely impact our business.

Our business depends on the overall demand for IT and on the economic health of our current and prospective customers. In general, worldwide economic conditions remain unstable, and these conditions make it difficult for our customers, prospective customers and us to forecast and plan future business activities accurately, and they could cause our customers or prospective customers to reevaluate their decision to purchase our solutions. Weak global economic conditions, or a reduction in IT spending even if economic conditions improve, could adversely impact our business, financial condition and results of operations in a number of ways, including longer sales cycles, lower prices for our solutions, reduced bookings and lower or no growth.

Table of Contents

Our business depends substantially on retaining our current customers, and any reduction in our customer renewals or revenues from such customers could harm our future operating results.

We offer our QualysGuard Cloud Platform and integrated suite of solutions pursuant to a software-as-a-service model, and our customers purchase subscriptions from us that are generally one year in length. Our customers have no obligation to renew their subscriptions after their subscription period expires, and they may not renew their subscriptions at the same or higher levels or at all. As a result, our ability to grow depends in part on customers renewing their existing subscriptions and purchasing additional subscriptions and solutions. Our customers may choose not to renew their subscriptions to our solutions or purchase additional solutions due to a number of factors, including their satisfaction or dissatisfaction with our solutions, the prices of our solutions, the prices of products or services offered by our competitors, reductions in our customers' spending levels due to the macroeconomic environment or other factors. If our customers do not renew their subscriptions to our solutions, renew on less favorable terms, or do not purchase additional solutions or subscriptions, our revenues may grow more slowly than expected or decline and our results of operations may be harmed.

If we are unable to continue to attract new customers and grow our customer base, our growth could be slower than we expect and our business may be harmed.

We believe that our future growth depends in part upon increasing our customer base. Our ability to achieve significant growth in revenues in the future will depend, in large part, upon continually attracting new customers and obtaining subscription renewals to our solutions from those customers. If we fail to attract new customers our revenues may grow more slowly than expected and our business may be harmed.

Subscriptions to our QualysGuard Vulnerability Management solution generate most of our revenues, and if we are unable to continue to renew and grow subscriptions for this solution, our operating results would suffer.

We derived 87%, 90%, and 92% of our revenues from subscriptions to our QualysGuard Vulnerability Management solution for the years ended December 31, 2012, 2011 and 2010, respectively, and we expect to continue to derive a significant majority of our revenues from sales of subscriptions to this solution for the foreseeable future. As a result, the market demand for our QualysGuard Vulnerability Management solution is critical to our continued success. Demand for this solution is affected by a number of factors beyond our control, including continued market acceptance of our solution for existing and new use cases, the timing of development and release of new products or services by our competitors, technological change, and growth or contraction in our market. Our inability to renew or increase subscriptions for this solution or a decline in price of this solution would harm our business and operating results more seriously than if we derived significant revenues from a variety of solutions.

If we are unable to sell subscriptions to additional solutions, our future revenue growth may be harmed and our business may suffer.

We will need to increase the revenues that we derive from our current and future solutions other than QualysGuard Vulnerability Management for our business and revenues to grow as we expect. Revenues from our other solutions, including our Web Application Scanning, Policy Compliance, PCI Compliance, Malware Detection Service and Qualys SECURE Seal, have been relatively modest compared to revenues from our QualysGuard Vulnerability Management solution. Our future success depends in part on our ability to sell subscriptions to these additional solutions to existing and new customers. This may require more costly sales and marketing efforts and may not result in additional sales. If our efforts to sell subscriptions to additional solutions to existing and new customers are not successful, our business may suffer.

15

Table of Contents

Our security and compliance solutions are primarily delivered from two data centers, and any disruption of service at these facilities would interrupt or delay our ability to deliver our solutions to our customers which could reduce our revenues and harm our operating results.

We currently host substantially all of our solutions from two third-party data centers, located in the United States and Switzerland. These facilities are vulnerable to damage or interruption from earthquakes, hurricanes, floods, fires, cybersecurity attacks, terrorist attacks, employee negligence, power losses, telecommunications failures and similar events. The facilities also could be subject to break-ins, sabotage, intentional acts of vandalism and other misconduct. The occurrence of a natural disaster, an act of terrorism or misconduct, a decision to close the facilities without adequate notice or other unanticipated problems could result in interruptions in our services.

Our data centers are not currently redundant and we cannot rapidly move customers from one data center to another, which may increase delays in the restoration of our service for our customers if an adverse event occurs. We intend to add additional data center facilities in 2013 to provide additional capacity for our cloud platform and enable disaster recovery. These additional facilities may not be operational in the anticipated time frame and we may incur unplanned expenses.

Additionally, our existing data center facilities providers have no obligations to renew their agreements with us on commercially reasonable terms, or at all. If we are unable to renew our agreements with the facilities providers on commercially reasonable terms or if in the future we add additional data center facility providers, we may experience costs or downtime in connection with the loss of an existing facility or the transfer to, or addition of, new data center facilities.

Any disruptions or other performance problems with our solutions could harm our reputation and business and may damage our customers' businesses. Interruptions in our service delivery might reduce our revenues, cause us to issue credits to customers, subject us to potential liability and cause customers to terminate their subscriptions or not renew their subscriptions.

If we are unable to increase market awareness of our company and our new solutions, our revenues may not continue to grow, or may decline.

We have a limited operating history, particularly in certain markets and solution offerings, and we believe that we need to continue to develop market awareness in the IT security and compliance market. Market awareness of our capabilities and solutions is essential to our continued growth and success in all of our markets, particularly for the large enterprise, service provider and government markets. If our marketing programs are not successful in creating market awareness of our company and our full suite of solutions, our business, financial condition and results of operations may be adversely affected, and we may not be able to achieve our expected growth.

If our solutions fail to help our customers achieve and maintain compliance with regulations and industry standards, our revenues and operating results could be harmed.

We generate a portion of our revenues from solutions that help organizations achieve and maintain compliance with regulations and industry standards. For example, many of our customers subscribe to our security and compliance solutions to help them comply with the security standards developed and maintained by the Payment Card Industry Security Standards Council, or the PCI Council, which apply to companies that store cardholder data. Industry organizations like the PCI Council may significantly change their security standards with little or no notice, including changes that could make their standards more or less onerous for businesses. Governments may also adopt new laws or regulations, or make changes to existing laws or regulations, that could impact the demand for or value of our solutions.

If we are unable to adapt our solutions to changing regulatory standards in a timely manner, or if our solutions fail to assist with or expedite our customers' compliance initiatives, our customers may lose confidence in our solutions and could switch to products offered by our competitors. In addition, if regulations and standards related to data security, vulnerability management and other IT security and compliance requirements are relaxed or the penalties for non-compliance are changed in a manner that makes them less onerous, our customers may view government and industry regulatory compliance as less critical to their businesses, and our customers may be less willing to purchase our solutions. In any of these cases, our revenues and operating results could be harmed.

Table of Contents

If our solutions fail to detect vulnerabilities or incorrectly detect vulnerabilities, our brand and reputation could be harmed, which could have an adverse effect on our business and results of operations.

If our solutions fail to detect vulnerabilities in our customers' IT infrastructures, or if our solutions fail to identify and respond to new and increasingly complex methods of attacks, our business and reputation may suffer. There is no guarantee that our solutions will detect all vulnerabilities. Additionally, our security and compliance solutions may falsely detect vulnerabilities or threats that do not actually exist. For example, some of our solutions rely on information on attack sources aggregated from third-party data providers who monitor global malicious activity originating from a variety of sources, including anonymous proxies, specific IP addresses, botnets and phishing sites. If the information from these data providers is inaccurate, the potential for false indications of security vulnerabilities increases. These false positives, while typical in the industry, may impair the perceived reliability of our solutions and may therefore adversely impact market acceptance of our solutions and could result in negative publicity, loss of customers and sales and increased costs to remedy any problem.

In addition, our solutions do not currently extend to cover mobile devices or personal devices that employees may bring into an organization. As such, our solutions would not identify or address vulnerabilities in mobile devices, such as mobile phones or tablets, or personal devices, and our customers' IT infrastructures may be compromised by attacks that infiltrate their networks through such devices.

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 solutions, could adversely affect the market's perception of our security solutions.

Incorrect or improper implementation or use of our solutions could result in customer dissatisfaction and harm our business and reputation.

Our solutions are deployed in a wide variety of IT environments, including large-scale, complex infrastructures. If our customers are unable to implement our solutions successfully, customer perceptions of our platform may be impaired or our reputation and brand may suffer. Our customers have in the past inadvertently misused our solutions, which triggered downtime in their internal infrastructure until the problem was resolved. Any misuse of our solutions could result in customer dissatisfaction, impact the perceived reliability of our solutions, result in negative press coverage, negatively affect our reputation and harm our financial results.

As a security provider, our platform, website and internal systems may be subject to intentional disruption that could adversely impact our reputation and future sales.

Our operations involve providing IT security solutions to our customers, and as a result we could be a target of cyber attacks designed to impede the performance of our solutions, penetrate our network security or the security of our cloud platform or our internal systems, misappropriate proprietary information and/or cause interruptions to our services. If an actual or perceived breach of our network security occurs, it could adversely affect the market perception of our solutions, negatively affecting our reputation, and may expose us to the loss of information, litigation and possible liability. Such a security breach could also divert the efforts of our technical and management personnel. In addition, such a security breach could impair our ability to operate our business and provide solutions to our customers. If this happens, our reputation could be harmed, our revenues could decline and our business could suffer.

Undetected software errors or flaws in our cloud platform could harm our reputation or decrease market acceptance of our solutions, which would harm our operating results.

Our solutions may contain undetected errors or defects when first introduced or as new versions are released. We have experienced these errors or defects in the past in connection with new solutions and solution upgrades and we expect that these errors or defects will be found from time to time in the future in new or enhanced solutions after commercial release of these solutions. Since our customers use our solutions for security and compliance reasons, any errors, defects, disruptions in service or other performance problems with our solutions may damage our customers' business and could hurt our reputation. If that occurs, we may incur significant costs, the attention of our key personnel could be diverted, our customers may delay or withhold payment to us or elect not to renew, or other significant customer relations problems may arise. We may also be subject to liability claims for damages related to errors or defects in our solutions. A material liability claim or other occurrence that harms our reputation or decreases market acceptance of our solutions may harm our business and operating results.

Table of Contents

Our solutions could be used to collect and store personal information of our customers' employees or customers, and therefore privacy concerns could result in additional cost and liability to us or inhibit sales of our solutions.

We collect the names and email addresses of our customers in connection with subscriptions to our solutions. Additionally, the data that our solutions collect to help secure and protect the IT infrastructure of our customers may include additional personal information of our customers' employees and their customers. Personal privacy has become a significant issue in the United States and in many other countries where we offer our solutions. The regulatory framework for privacy issues worldwide is currently evolving and is likely to remain uncertain for the foreseeable future. Many federal, state and foreign government bodies and agencies have adopted or are considering adopting laws and regulations regarding the collection, use, disclosure and retention of personal information. In the United States, these include, for example, rules and regulations promulgated under the authority of the Federal Trade Commission, the Health Insurance Portability and Accountability Act of 1996, or HIPAA, the Gramm-Leach-Bliley Act, or GLB, and state breach notification laws. Internationally, virtually every jurisdiction in which we operate has established its own data security and privacy legal framework with which we or our customers must comply, including the Data Protection Directive established in the European Union and the Federal Data Protection Act passed in Germany.

In addition to laws and regulations, privacy advocacy and industry groups or other private parties may propose new and different privacy standards that either legally or contractually apply to us. Because the interpretation and application of privacy and data protection laws and privacy standards are still uncertain, it is possible that these laws or privacy standards may be interpreted and applied in a manner that is inconsistent with our existing data management practices or the features of our solutions. If so, in addition to the possibility of fines, lawsuits and other claims, we could be required to fundamentally change our business activities and practices or modify our solutions, which could have an adverse effect on our business. Any inability to adequately address privacy concerns, even if unfounded, or comply with applicable privacy or data protection laws, regulations and privacy standards, could result in additional cost and liability to us, damage our reputation, inhibit sales of subscriptions and harm our business.

Furthermore, the costs of compliance with, and other burdens imposed by, the laws, regulations, and privacy standards that are applicable to the businesses of our customers may limit the use and adoption of, and reduce the overall demand for, our solutions. Privacy concerns, whether valid or not valid, may inhibit market adoption of our solutions particularly in certain industries and foreign countries.

Disruptive technologies could gain wide adoption and supplant our cloud security and compliance solutions, thereby weakening our sales and harming our results of operations.

The introduction of products and services embodying new technologies could render our existing solutions obsolete or less attractive to customers. Our business could be harmed if new security and compliance technologies are widely adopted. We may not be able to successfully anticipate or adapt to changing technology or customer requirements on a timely basis, or at all. If we fail to keep up with technological changes or to convince
our customers and potential customers of the value of our solutions even in light of new technologies, our business could be harmed and our revenues may decline.

We face competition in our markets, and we may lack sufficient financial or other resources to maintain or improve our competitive position.

We compete with a large range of established and emerging vulnerability management vendors, compliance vendors and data security vendors in a highly fragmented and competitive environment. We face significant competition for each of our solutions from companies with broad product suites and greater name recognition and resources than we have, as well as from small companies focused on specialized security solutions.

18

Table of Contents

We compete with large public companies, such as Hewlett-Packard Company, Imperva, Inc., International Business Machines Corporation, McAfee, Inc. (a subsidiary of Intel Corporation), and Symantec Corporation, as well as private security providers including Barracuda Networks, Inc., BeyondTrust Software, Inc., Lumension Security, Inc., nCircle Network Security, Inc., NetIQ Corporation, Rapid7 LLC, Tenable Network Security, Inc. and Trustwave Holdings, Inc. We also seek to replace IT security and compliance solutions that organizations have developed internally. As we continue to extend our cloud platform's functionality by further developing security and compliance solutions, such as web application scanning and firewalls, we expect to face additional competition in these new markets. Our competitors may also attempt to further expand their presence in the IT security and compliance market and compete more directly against one or more of our solutions.

We believe that the principal competitive factors affecting our markets include product functionality, breadth of offerings, flexibility of delivery models, ease of deployment and use, total cost of ownership, scalability and performance, customer support and extensibility of platform. Many of our existing and potential competitors have competitive advantages, including:

- greater brand name recognition;
- larger sales and marketing budgets and resources;
- broader distribution networks and more established relationships with distributors and customers;
- access to larger customer bases;
- greater customer support resources;
- greater resources to make acquisitions;
- greater resources to develop and introduce products that compete with our solutions;
- greater resources to meet relevant regulatory requirements; and
- substantially greater financial, technical and other resources.

As a result, our competitors may be able to respond more quickly and effectively than we can to new or changing opportunities, technologies, standards or customer requirements. With the introduction of new technologies, the evolution of our service and new market entrants, we expect competition to intensify in the future.

In addition, some of our larger competitors have substantially broader product offerings and can bundle competing products and services with other software offerings. As a result, customers may choose a bundled product offering from our competitors, even if individual products have more limited functionality than our solutions. These competitors may also offer their products at a lower price as part of this larger sale, which could increase pricing pressure on our solutions and cause the average sales price for our solutions to decline. These larger competitors are also often in a better position to withstand any significant reduction in capital spending, and will therefore not be as susceptible to economic downturns.

Furthermore, our current and potential competitors may establish cooperative relationships among themselves or with third parties that may further enhance their resources and product and services offerings in the markets we address. In addition, current or potential competitors may be acquired by third parties with greater available resources. As a result of such relationships and acquisitions, our current or potential competitors might be able to adapt more quickly to new technologies and customer needs, devote greater resources to the promotion or sale of their products and services, initiate or withstand substantial price competition, take advantage of other opportunities more readily or develop and expand their product and service offerings more quickly than we do. For all of these reasons, we may not be able to compete successfully against our current or future competitors.

Table of Contents

Our business and operations have experienced rapid growth, and if we do not appropriately manage any future growth, or are unable to improve our systems and processes, our operating results may be negatively affected.

We have experienced rapid growth over the last several years. From 2010 to 2012, our revenues have grown from $65.4 million to $91.4 million, and our headcount increased from 232 employees at the beginning of 2010 to 359 employees at December 31, 2012. We rely on information technology systems to help manage critical functions such as order processing, revenue recognition and financial forecasts. To manage any future growth effectively we must continue to improve and expand our IT systems, financial infrastructure, and operating and administrative systems and controls, and continue to manage headcount, capital and processes in an efficient manner. We may not be able to successfully implement improvements to these systems and processes in a timely or efficient manner.

Our failure to improve our systems and processes, or their failure to operate in the intended manner, may result in our inability to manage the growth of our business and to accurately forecast our revenues, expenses and earnings, or to prevent certain losses. In addition, as we continue to grow, our productivity and the quality of our solutions may also be adversely affected if we do not integrate and train our new employees quickly and effectively. Any future growth would add complexity to our organization and require effective coordination across our organization. Failure to manage any future growth effectively could result in increased costs, harm our results of operations and lead to investors losing confidence in our internal systems and processes.

Forecasts of market growth may prove to be inaccurate, and even if the markets in which we compete achieve the forecasted growth, there can be no assurance that our business will grow at similar rates, or at all.
Growth forecasts relating to the expected growth in the market for IT security and compliance and other markets are subject to significant uncertainty and are based on assumptions and estimates which may prove to be inaccurate. Even if these markets experience the forecasted growth, we may not grow our business at similar rates, or at all. Our growth is subject to many factors, including our success in implementing our business strategy, which is subject to many risks and uncertainties. Accordingly, the forecasts of market growth included in this Annual Report on Form 10-K should not be taken as indicative of our future growth.

If we are unable to continue the expansion of our sales force, sales of our solutions and the growth of our business would be harmed.

We believe that our growth will depend, to a significant extent, on our success in recruiting and retaining a sufficient number of qualified sales personnel and their ability to obtain new customers, manage our existing customer base and expand the sales of our newer solutions. We plan to continue to expand our sales force and make significant investment in our sales and marketing activities. Our recent hires and planned hires may not become as productive as quickly as we would like, and we may be unable to hire or retain sufficient numbers of qualified individuals in the future in the markets where we do business. If we are unable to recruit and retain a sufficient number of productive sales personnel, sales of our solutions and the growth of our business may be harmed. Additionally, if our efforts do not result in increased revenues, our operating results could be negatively impacted due to the upfront operating expenses associated with expanding our sales force.

Our sales cycle can be long and unpredictable, and our sales efforts require considerable time and expense. As a result, revenues may vary from period to period, which may cause our operating results to fluctuate and could harm our business.

The timing of sales of subscriptions for our solutions is difficult to forecast because of the length and unpredictability of our sales cycle, particularly with large enterprises. We sell subscriptions to our security and compliance solutions primarily to IT departments that are managing a growing set of user and compliance demands, which has increased the complexity of customer requirements to be met and confirmed during the sales cycle and prolonged our sales cycle.

Further, the length of time that potential customers devote to their testing and evaluation, contract negotiation and budgeting processes varies significantly, which has also made our sales cycle long and unpredictable. The length of the sales cycle for our solutions typically ranges from six to twelve months but can be more than eighteen months. In addition, we might devote substantial time and effort to a particular unsuccessful sales effort, and as a result we could lose other sales opportunities or incur expenses that are not offset by an increase in revenues, which could harm our business.

Table of Contents

We rely on third-party channel partners to generate a substantial amount of our revenues, and if we fail to expand and manage our distribution channels, our revenues could decline and our growth prospects could suffer.

Our success is significantly dependent upon establishing and maintaining relationships with a variety of channel partners and we anticipate that we will continue to depend on these partners in order to grow our business. For 2012, 2011 and 2010, we derived approximately 40%, 38% and 33%, respectively, of our revenues from sales of subscriptions for our solutions through channel partners, and the percentage of revenues derived from channel partners may increase in future periods. Additionally, one of our channel partners, Dell, Inc. accounted for 5%, 4% and 3% of our revenues for the years ended December 31, 2012, 2011 and 2010, respectively. Our agreements with our channel partners are generally non-exclusive and do not prohibit them from working with our competitors or offering competing solutions, and many of our channel partners have more established relationships with our competitors. If our channel partners choose to place greater emphasis on products of their own or those offered by our competitors, do not effectively market and sell our solutions, or fail to meet the needs of our customers, then our ability to grow our business and sell our solutions may be adversely affected. In addition, the loss of one or more of our larger channel partners, who may cease marketing our solutions with limited or no notice, and our possible inability to replace them, could adversely affect our sales. Moreover, our ability to expand our distribution channels depends in part on our ability to educate our channel partners about our solutions, which can be complex. Our failure to recruit additional channel partners, or any reduction or delay in their sales of our solutions or conflicts between channel sales and our direct sales and marketing activities may harm our results of operations. Even if we are successful, these relationships may not result in greater customer usage of our solutions or increased revenues.

We rely on software-as-a-service vendors to operate certain functions of our business and any failure of such vendors to provide services to us could adversely impact our business and operations.

We rely on software-as-a-service vendors to operate certain critical functions of our business, including financial management and human resource management. If these services become unavailable due to extended outages or interruptions or because they are no longer available on commercially reasonable terms or prices, our expenses could increase, our ability to manage our finances could be interrupted and our processes for managing sales of our solutions and supporting our customers could be impaired until equivalent services, if available, are identified, obtained and integrated, all of which could harm our business.

We use third-party software and data that may be difficult to replace or cause errors or failures of our solutions that could lead to lost customers or harm to our reputation and our operating results.

We license third-party software as well as security and compliance data from various third parties to deliver our solutions. In the future, this software or data may not be available to us on commercially reasonable terms, or at all. Any loss of the right to use any of this software or data could result in delays in the provisioning of our solutions until equivalent technology or data is either developed by us, or, if available, is identified, obtained and integrated, which could harm our business. In addition, any errors or defects in or failures of this third-party software could result in errors or defects in our solutions or cause our solutions to fail, which could harm our business and be costly to correct. Many of these providers attempt to impose limitations on their liability for such errors, defects or failures, and if enforceable, we may have additional liability to our customers or third-party providers that could harm our reputation and increase our operating costs.

We will need to maintain our relationships with third-party software and data providers, and to obtain software and data from such providers that does not contain any errors or defects. Any failure to do so could adversely impact our ability to deliver effective solutions to our customers and could harm our operating results.

21

Table of Contents

Our solutions contain third-party open source software components, and our failure to comply with the terms of the underlying open source software licenses could restrict our ability to sell our solutions.

Our solutions contain software licensed to us by third-parties under so-called “open source” licenses, including the GNU General Public License, or GPL, the GNU Lesser General Public License, or LGPL, the BSD License, the Apache License and others. From time to time, there have been claims against companies that distribute or use open source software in their products and services, asserting that such open source software infringes the claimants’ intellectual property rights. We could be subject to suits by parties claiming that what we believe to be licensed open source software infringes their intellectual property rights. Use and distribution of open source software may entail greater risks than use of third-party commercial software, as open source licensors generally do not provide warranties or other contractual protections regarding infringement claims or the quality of the code. In addition, certain open source licenses require that source code for software programs that are subject to the license be made available to the public and that any modifications or derivative works to such open source software continue to be licensed under the same terms. If we combine our proprietary software with open source software in certain ways, we could, in some circumstances, be required to release the source code of our proprietary software to the public. Disclosing the source code of our proprietary software could make it easier for cyber attackers and other third parties to discover vulnerabilities in or to defeat the protections of our solutions, which could result in our solutions failing to provide our customers with the security they expect from our services. This could harm our business and reputation. Disclosing our proprietary source code also could allow our competitors to create similar products with lower development effort and time and ultimately could result in a loss of sales for us. Any of these events could have a material adverse effect on our business, operating results and financial condition.

Although we monitor our use of open source software in an effort both to comply with the terms of the applicable open source licenses and to avoid subjecting our solutions to conditions we do not intend, the terms of many open source licenses have not been interpreted by U.S. courts, and there is a risk that these licenses could be construed in a way that could impose unanticipated conditions or restrictions on our ability to commercialize our solutions. In this event, we could be required to seek licenses from third parties to continue offering our solutions, to make our proprietary code generally available in source code form, to re-engineer our solutions or to discontinue the sale of our solutions if re-engineering could not be accomplished on a timely basis, any of which could adversely affect our business, operating results and financial condition.

Delays or interruptions in the manufacturing and delivery of our physical scanner appliances by our sole source manufacturer may harm our business.

Upon customer request, we provide physical or virtual scanner appliances on a subscription basis as an additional capability to the customer’s subscription for use during their subscription term. Our physical scanner appliances are built by a single manufacturer. Our reliance on a sole manufacturer involves several risks, including a potential inability to obtain an adequate supply of physical scanner appliances and limited control over pricing, quality and timely deployment of such scanner appliances. In addition, replacing this manufacturer may be difficult and could result in an inability or delay in deploying our solutions to customers that request physical scanner appliances as part of their subscriptions.

Furthermore, our manufacturer’s ability to timely manufacture and ship our physical scanner appliances depends on a variety of factors, such as the availability of hardware components, supply shortages or contractual restrictions. In the event of an interruption from this manufacturer, we may not be able to develop alternate or secondary sources in a timely manner. If we are unable to purchase physical scanner appliances in quantities sufficient to meet our requirements on a timely basis, we may not be able to effectively deploy our solutions to new customers that request physical scanner appliances, which could harm our business.

22

Table of Contents

A significant portion of our customers and channel partners are located outside of the United States, which subjects us to a number of risks associated with conducting international operations and if we are unable to successfully manage these risks, our business and operating results could be harmed.

We market and sell subscriptions to our solutions throughout the world and have personnel in many parts of the world. In addition, we have sales offices and research and development facilities outside the United States and we conduct, and expect to continue to conduct, a significant amount of our business with organizations that are located outside the United States, particularly in Europe and Asia. Therefore, we are subject to risks associated with having international sales and worldwide operations, including:

- foreign currency exchange fluctuations;
- trade and foreign exchange restrictions;
- economic or political instability in foreign markets;
- greater difficulty in enforcing contracts, accounts receivable collection and longer collection periods;
- changes in regulatory requirements;
- difficulties and costs of staffing and managing foreign operations;
- the uncertainty and limitation of protection for intellectual property rights in some countries;
- costs of compliance with foreign laws and regulations and the risks and costs of non-compliance with such laws and regulations;
- costs of complying with U.S. laws and regulations for foreign operations, including the Foreign Corrupt Practices Act, import and export control laws, tariffs, trade barriers, economic sanctions and other regulatory or contractual limitations on our ability to sell our solutions in certain foreign markets, and the risks and costs of non-compliance;
- heightened risks of unfair or corrupt business practices in certain geographies and of improper or fraudulent sales arrangements that may impact financial results and result in restatements of, and irregularities in, financial statements;
- the potential for political unrest, acts of terrorism, hostilities or war;
- management communication and integration problems resulting from cultural differences and geographic dispersion; and
- multiple and possibly overlapping tax structures.

Our business, including the sales of subscriptions of our solutions, may be subject to foreign governmental regulations, which vary substantially from country to country and change from time to time. Failure to comply with these regulations could adversely affect our business. Further, in many foreign countries it is common for others to engage in business practices that are prohibited by our internal policies and procedures or U.S. regulations applicable to us. Although we have implemented policies and procedures designed to ensure compliance with these laws and policies, there can be no assurance that all of our employees, contractors, channel partners and agents have complied or will comply with these laws and policies. Violations of laws or key control policies by our employees, contractors, channel partners or agents could result in delays in revenue recognition, financial reporting misstatements, fines, penalties or the prohibition of the importation or exportation of our solutions and could have a material adverse effect on our business and results of operations. If we are unable to successfully manage the challenges of international operations, our business and operating results could be adversely affected.

Table of Contents

We are exposed to fluctuations in currency exchange rates, which could negatively affect our financial condition and results of operations.

Our reporting currency is the U.S. dollar and we generate a majority of our revenues in U.S. dollars. However, in 2012, we incurred approximately 21% of our expenses outside of the United States in foreign currencies, primarily Euros, principally with respect to salaries and related personnel expenses associated with our European operations. Additionally, in 2012, approximately 21% of our revenues were generated in foreign currencies. Accordingly, changes in exchange rates may have a material adverse effect on our business, operating results and financial condition. The exchange rate between the U.S. dollar and foreign currencies has 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 Euros. The results of our operations may be adversely affected by foreign exchange fluctuations.

We use forward foreign exchange contracts to mitigate the effect of changes in foreign exchange rates on cash and accounts receivable balances denominated in certain foreign currencies. However, we may not be able to purchase derivative instruments that are adequate to insulate ourselves from foreign currency exchange risks. Additionally, our hedging activities may contribute to increased losses as a result of volatility in foreign currency markets.

Failure to protect our proprietary technology and intellectual property rights could substantially harm our business and operating results.

The success of our business depends in part on our ability to protect and enforce our trade secrets, trademarks, copyrights, patents and other intellectual property rights. We attempt to protect our intellectual property under copyright, trade secret, patent and trademark laws, and through a combination of confidentiality procedures, contractual provisions and other methods, all of which offer only limited protection.

We primarily rely on our unpatented proprietary technology and trade secrets. Despite our efforts to protect our proprietary technology and trade secrets, unauthorized parties may attempt to misappropriate, reverse engineer or otherwise obtain and use them. The contractual provisions that we enter into with employees, consultants, partners, vendors and customers may not prevent unauthorized use or disclosure of our proprietary technology or intellectual property rights and may not provide an adequate remedy in the event of unauthorized use or disclosure of our proprietary technology or intellectual property rights. Moreover, policing unauthorized use of our technologies, solutions and intellectual property is difficult, expensive and time-consuming, particularly in foreign countries where the laws may not be as protective of intellectual property rights as those in the United States and where mechanisms for enforcement of intellectual property rights may be weak. We may be unable to determine the extent of any unauthorized use or infringement of our solutions, technologies or intellectual property rights.

We have one issued patent and several pending U.S. patent applications, and may file additional patent applications in the future. Additionally, as of December 31, 2012, we had an exclusive license to four third-party patents. The process of obtaining patent protection is expensive and time-consuming, and we may not be able to prosecute all necessary or desirable patent applications at a reasonable cost or in a timely manner, if at all. We may choose not to seek patent protection for certain innovations and may choose not to pursue patent protection in certain jurisdictions. Furthermore, it is possible that our patent applications may not result in granted patents, that the scope of our issued patents will be limited or not provide the coverage originally sought, that our issued patents will not provide us with any competitive advantages, or that our patents and other intellectual property rights may be challenged by others or invalidated through administrative processes or litigation. In addition, issuance of a patent does not guarantee that we have an absolute right to practice the patented invention. As a result, we may not be able to obtain adequate patent protection or to enforce our issued patents effectively.

From time to time, legal action by us may be necessary to enforce our patents and other intellectual property rights, to protect our trade secrets, to determine the validity and scope of the intellectual property rights of others or to defend against claims of infringement or invalidity. Such litigation could result in substantial costs and diversion of resources and could negatively affect our business, operating results and financial condition. If we are unable to protect our intellectual property rights, we may find ourselves at a competitive disadvantage to others who need not incur the additional expense, time and effort required to create the innovative solutions that have enabled us to be successful to date.

Table of Contents

Assertions by third parties of infringement or other violations by us of their intellectual property rights could result in significant costs and harm our business and operating results.

Patent and other intellectual property disputes are common in our industry. Some companies, including some of our competitors, own large numbers of patents, copyrights and trademarks, which they may use to assert claims against us. Third parties may in the future assert claims of infringement, misappropriation or other violations of intellectual property rights against us. They may also assert such claims against our customers or channel partners whom we typically indemnify against claims that our solutions infringe, misappropriate or otherwise violate the intellectual property rights of third parties. As the numbers of products and competitors in our market increase and overlaps occur, claims of infringement, misappropriation and other violations of intellectual property rights may increase. Any claim of infringement, misappropriation or other violation of intellectual property rights by a third party, even those without merit, could cause us to incur substantial costs defending against the claim and could distract our management from our business.

The patent portfolios of our most significant competitors are larger than ours. This disparity may increase the risk that they may sue us for patent infringement and may limit our ability to counterclaim for patent infringement or settle through patent cross-licenses. In addition, future assertions of patent rights by third parties, and any resulting litigation, may involve patent holding companies or other adverse patent owners who have no relevant product revenues and against whom our own patents may therefore provide little or no deterrence or protection. There can be no assurance that we will not be found to infringe or otherwise violate any third-party intellectual property rights or to have done so in the past.

An adverse outcome of a dispute may require us to:

- pay substantial damages, including treble damages, if we are found to have willfully infringed a third party's patents or copyrights;
- cease making, licensing or using solutions that are alleged to infringe or misappropriate the intellectual property of others;
- expend additional development resources to attempt to redesign our solutions or otherwise develop non-infringing technology, which may not be successful;
- enter into potentially unfavorable royalty or license agreements in order to obtain the right to use necessary technologies or intellectual property rights; and
- indemnify our partners and other third parties.

In addition, royalty or licensing agreements, if required or desirable, may be unavailable on terms acceptable to us, or at all, and may require significant royalty payments and other expenditures. Some licenses may also be non-exclusive, and therefore our competitors may have access to the same technology licensed to us. Any of the foregoing events could seriously harm our business, financial condition and results of operations.

If we are required to collect sales and use or other taxes on the solutions we sell, we may be subject to liability for past sales and our future sales may decrease.

Taxing jurisdictions, including state and local entities, have differing rules and regulations governing sales and use or other taxes, and these rules and regulations are subject to varying interpretations that may change over time. In particular, the applicability of sales taxes to our subscription services in various jurisdictions is unclear. We have recorded sales tax liabilities of $0.4 million on our consolidated balance sheet as of December 31, 2012 with respect to sales and use tax liabilities in various jurisdictions where we have not yet billed sales tax to our customers and where we believe we may have exposure. It is possible that we could face sales tax audits and that our liability for these taxes could exceed our estimates as tax authorities could still assert that we are obligated to collect additional amounts as

taxes from our customers and remit those taxes to those authorities. We could also be subject to audits with respect to state and international jurisdictions for which we have not accrued tax liabilities. A successful assertion that we should be collecting additional sales or other taxes on our services in jurisdictions where we have not historically done so and do not accrue for sales taxes could result in substantial tax liabilities for past sales, discourage customers from purchasing our solutions or otherwise harm our business and operating results.

Table of Contents

We are dependent on the continued services and performance of our senior management and other key employees, the loss of any of whom could adversely affect our business, operating results and financial condition.

Our future performance depends on the continued services and continuing contributions of our senior management, particularly Philippe F. Courtot, our Chairman, President and Chief Executive Officer, and other key employees to execute on our business plan and to identify and pursue new opportunities and product innovations. We do not maintain key-man insurance for Mr. Courtot or for any other member of our senior management team. From time to time, there may be changes in our senior management team resulting from the termination or departure of executives. Our senior management and key employees are generally employed on an at-will basis, which means that they could terminate their employment with us at any time. The loss of the services of our senior management, particularly Mr. Courtot, or other key employees for any reason could significantly delay or prevent the achievement of our development and strategic objectives and harm our business, financial condition and results of operations.

If we are unable to hire, retain and motivate qualified personnel, our business may suffer.

Our future success depends, in part, on our ability to continue to attract and retain highly skilled personnel. The loss of the services of any of our key personnel, the inability to attract or retain qualified personnel or delays in hiring required personnel, particularly in engineering and sales, may seriously harm our business, financial condition and results of operations. Any of our employees may terminate their employment at any time. Competition for highly skilled personnel is frequently intense, especially in the San Francisco Bay Area, one of the locations in which we have a substantial presence and need for highly-skilled personnel and we may not be able to compete for these employees.

For example, we are required under accounting principles generally accepted in the United States (“U.S. GAAP”) to recognize compensation expense in our operating results for employee stock-based compensation under our equity grant programs, which may negatively impact our operating results and may increase the pressure to limit stock-based compensation that we might otherwise offer to current or potential employees. In addition, to the extent we hire personnel from competitors, we may be subject to allegations that they have been improperly solicited or divulged proprietary or other confidential information.

Changes in laws or regulations related to the Internet may diminish the demand for our solutions and could have a negative impact on our business.

We deliver our solutions through the Internet. Federal, state or foreign government bodies or agencies have in the past adopted, and may in the future adopt, laws or regulations affecting data privacy and the use of the Internet. In addition, government agencies or private organizations may begin to impose taxes, fees or other charges for accessing the Internet or on commerce conducted via the Internet. These laws or charges could limit the viability of Internet-based solutions such as ours and reduce the demand for our solutions.

Table of Contents

A portion of our revenues are generated by sales to government entities, which are subject to a number of challenges and risks.

Government entities have historically been particularly concerned about adopting cloud-based solutions for their operations, including security solutions, and increasing sales of subscriptions for our solutions to government entities may be more challenging than selling to commercial organizations. Selling to government entities can be highly competitive, expensive and time consuming, often requiring significant upfront time and expense without any assurance that we will win a sale. We have invested in the creation of a cloud offering certified under the Federal Information Security Management Act, or FISMA, for government usage but we cannot be sure that we will continue to sustain or renew this certification, that the government will continue to mandate such certification or that other government agencies or entities will use this cloud offering. Government demand and payment for our solutions may be impacted by public sector budgetary cycles and funding authorizations, with funding reductions or delays adversely affecting public sector demand for our solutions. Government entities may have contractual or other legal rights to terminate contracts with our channel partners for convenience or due to a default, and any such termination may adversely impact our future results of operations. Governments routinely investigate and audit government contractors' administrative processes, and any unfavorable audit could result in the government refusing to continue buying our solutions, a reduction of revenues or fines or civil or criminal liability if the audit uncovers improper or illegal activities. Any such penalties could adversely impact our results of operations in a material way.

Governmental export or import controls could subject us to liability if we violate them or limit our ability to compete in foreign markets.

Our solutions are subject to U.S. export controls, and we incorporate encryption technology into certain of our solutions. These encryption solutions and the underlying technology may be exported only with the required export authorizations, including by license, a license exception or other appropriate government authorizations. U.S. export controls may require submission of an encryption registration, product classification and/or annual or semi-annual reports. Governmental regulation of encryption technology and regulation of imports or exports of encryption products, or our failure to obtain required import or export authorization for our solutions, when applicable, could harm our international sales and adversely affect our revenues. Compliance with applicable regulatory requirements regarding the export of our solutions, including with respect to new releases of our solutions, may create delays in the introduction of our solutions in international markets, prevent our customers with international operations from deploying our solutions throughout their globally-distributed systems or, in some cases, prevent the export of our solutions to some countries altogether. In addition, various countries regulate the import of our appliance-based solutions and have enacted laws that could limit our ability to distribute solutions or could limit our customers' ability to implement our solutions in those countries. Any new export or import restrictions, new legislation or shifting approaches in the enforcement or scope of existing regulations, or in the countries, persons or technologies targeted by such regulations, could result in decreased use of our solutions by existing customers with international operations, declining adoption of our solutions by new customers with international operations and decreased revenues. If we fail to comply with export and import regulations, we may be fined or other penalties could be imposed, including a denial of certain export privileges.

Our success in acquiring and integrating other businesses, products or technologies could impact our financial position.

In order to remain competitive, we have in the past and may in the future seek to acquire additional businesses, products or technologies. The environment for acquisitions in our industry is very competitive and acquisition candidate purchase prices will likely exceed what we would prefer to pay. Moreover, achieving the anticipated benefits of future acquisitions will depend in part upon whether we can integrate acquired operations, products and technology in a timely and cost-effective manner. The acquisition and integration process is complex, expensive and

time consuming, and may cause an interruption of, or loss of momentum in, product development and sales activities and operations of both companies. We may not find suitable acquisition candidates, and acquisitions we complete may be unsuccessful. If we consummate a transaction, we may be unable to integrate and manage acquired products and businesses effectively or retain key personnel. If we are unable to effectively execute acquisitions, our business, financial condition and operating results could be adversely affected.

Table of Contents

Our financial results are based in part on our estimates or judgments relating to our critical accounting policies. These estimates or judgments may prove to be incorrect, which could harm our operating results and result in a decline in our stock price.

The preparation of financial statements in conformity with U.S. GAAP requires management to make estimates and assumptions that affect the amounts reported in the consolidated financial statements and accompanying notes. We base our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances, as provided in the section titled "Part II, Item 7 - Management's Discussion and Analysis of Financial Condition and Results of Operations," the results of which form the basis for making judgments about the carrying values of assets, liabilities, equity, revenues and expenses that are not readily apparent from other sources. Our operating results may be adversely affected if our assumptions change or if actual circumstances differ from those in our assumptions, which could cause our operating results to fall below the expectations of securities analysts and investors, resulting in a decline in our stock price. Significant assumptions and estimates used in preparing our consolidated financial statements include those related to revenue recognition, goodwill and intangibles, reserves, accounting for income taxes and stock-based compensation.

Changes in financial accounting standards may cause adverse and unexpected revenue fluctuations and impact our reported results of operations.

A change in accounting standards or practices could harm our operating results and may even affect our reporting of transactions completed before the change is effective. New accounting pronouncements and varying interpretations of accounting pronouncements have occurred and may occur in the future. Changes to existing rules or the questioning of current practices may harm our operating results or the way we conduct our business.

Because we expense commissions associated with sales of our solutions immediately upon receipt of a subscription order from a customer and generally recognize the revenues associated with such sale over the term of the agreement, our operating income in any period may not be indicative of our financial health and future performance.

We expense commissions paid to our sales personnel in the quarter in which the related order is received. In contrast, we generally recognize the revenues associated with a sale of our solutions ratably over the term of the subscription, which is typically one year. Although we believe increased sales is a positive indicator of the long-term health of our business, increased sales would increase our operating expenses and decrease net income in any particular period. Thus, we may report poor operating results due to higher sales commissions in a period in which we experience strong sales of our solutions. Alternatively, we may report better operating results due to the reduction of sales commissions in a period in which we experience a slowdown in sales. Therefore, you should not rely on our operating results during any one quarter as an indication of our financial health and future performance.

We recognize revenues from subscriptions over the term of the relevant service period, and therefore any decreases or increases in bookings are not immediately reflected in our operating results.

We recognize revenues from subscriptions over the term of the relevant service period, which is typically one year. As a result, most of our reported revenues in each quarter are derived from the recognition of deferred revenues relating to subscriptions entered into during previous quarters. Consequently, a shortfall in demand for our solutions in any period may not significantly reduce our revenues for that period, but could negatively affect revenues in future periods. Accordingly, the effect of significant downturns in bookings may not be fully reflected in our results of operations until future periods. We may be unable to adjust our costs and expenses to compensate for such a potential shortfall in revenues. Our subscription model also makes it difficult for us to rapidly increase our revenues through additional bookings in any period, as revenues are recognized ratably over the subscription period.

28

Table of Contents

Changes in our provision for income taxes or adverse outcomes resulting from examination of our income tax returns could adversely affect our operating results.

We are subject to income taxes in the United States and various foreign jurisdictions, and our domestic and international tax liabilities are subject to the allocation of expenses in differing jurisdictions. Our tax rate is affected by changes in the mix of earnings and losses in countries with differing statutory tax rates, certain non-deductible expenses arising from the requirement to expense stock options and the valuation of deferred tax assets and liabilities, including our ability to utilize our federal net operating losses, which were $52.9 million as of December 31, 2012. Increases in our effective tax rate could harm our operating results.

Our business is subject to the risks of earthquakes, fire, power outages, floods and other catastrophic events, and to interruption by manmade problems such as terrorism.

A significant natural disaster, such as an earthquake, fire or a flood, or a significant power outage could have a material adverse impact on our business, operating results and financial condition. Our corporate headquarters and a significant portion of our operations are located in the San Francisco Bay Area, a region known for seismic activity. In addition, natural disasters could affect our business partners' ability to perform services for us on a timely basis. In the event we or our business partners are hindered by any of the events discussed above, our ability to provide our solutions to customers could be delayed, resulting in our missing financial targets, such as revenues and net income, for a particular quarter. Further, if a natural disaster occurs in a region from which we derive a significant portion of our revenues, customers in that region may delay or forego subscriptions of our solutions, which may materially and adversely impact our results of operations for a particular period. In addition, acts of terrorism could cause disruptions in our business or the business of our business partners, customers or the economy as a whole. All of the aforementioned risks may be exacerbated if the disaster recovery plans for us and our suppliers prove to be inadequate. To the extent that any of the above results in delays of customer subscriptions or commercialization of our solutions, our business, financial condition and results of operations could be adversely affected.

If we fail to maintain an effective system of internal control over financial reporting, our ability to produce timely and accurate financial statements or comply with applicable regulations could be impaired.

As a public company, we are subject to the reporting requirements of the Securities Exchange Act of 1934, or the Exchange Act, the Sarbanes-Oxley Act, and the rules and regulations of the NASDAQ Stock Market. To comply with the requirements of being a public company, we may need to undertake various actions, such as implementing new internal controls and procedures and hiring accounting or internal audit staff.

During the quarter ended June 30, 2012, we identified a deficiency in our internal control over financial reporting and we determined that we should restate our consolidated financial statements as of December 31, 2010 and 2011 and for the year ended December 31, 2010 to correct an error in our 2010 provision for income taxes. The restatement related to the tax benefit resulting from a reduction of our liability for uncertain tax positions upon the lapse of the statute of limitations for the 2007 tax year of our French subsidiary. We did not release the liability at December 31, 2010 due to an error in the determination of when the statute of limitations would expire. Our review of the tax provision prepared by a third-party tax advisor was not effective in identifying the error in an appropriate timeframe. We concluded that this control deficiency was not a material weakness, but rather constituted a significant deficiency in our internal control over financial reporting. However, other control deficiencies which may rise to the level of a material weakness may be discovered in the future. In addition, our current controls and any new controls that we develop may become inadequate because of changes in conditions in our business. Any failure to develop or maintain effective controls, or any difficulties encountered in their implementation or improvement, could harm our operating results or cause us to fail to meet our reporting obligations and may result in additional restatements of our financial statements for prior periods. Any failure to implement and maintain effective internal control over financial reporting also could

adversely affect the results of periodic management evaluations and annual independent registered public accounting firm attestation reports regarding the effectiveness of our internal control over financial reporting that we will be required to include in our periodic reports we will file with the SEC under Section 404 of the Sarbanes-Oxley Act. In the event that we are not able to demonstrate compliance with Section 404 of the Sarbanes-Oxley Act, that our internal control over financial reporting is perceived as inadequate or that we are unable to produce timely or accurate financial statements, investors may lose confidence in our operating results and our stock price could decline. In addition, if we are unable to continue to meet these requirements, we may not be able to remain listed on the NASDAQ Stock Market.

Table of Contents

As a public company, we are required to comply with certain of these rules, which require management to certify financial and other information in this Annual Report on Form 10-K and other quarterly and annual reports and provide an annual management report on the effectiveness of our internal control over financial reporting commencing with our Annual Report on Form 10-K for the year ending December 31, 2013. Our independent registered public accounting firm is not required to formally attest to the effectiveness of our internal control over financial reporting until the later of our Annual Report on Form 10-K for the year ending December 31, 2013 or the first annual report required to be filed with the SEC following the date we are no longer an “emerging growth company” as defined in the JOBS Act. At such time, our independent registered public accounting firm may issue a report that is adverse in the event it is not satisfied with the level at which our controls are documented, designed or operating. Our remediation efforts may not enable us to avoid a material weakness in the future. We would remain an “emerging growth company” for up to five years, although, we will cease to be an “emerging growth company” upon the earliest of (i) the first fiscal year following the fifth anniversary of September 28, 2012, the date of our initial public offering, (ii) the first fiscal year after our annual gross revenues are $1 billion or more, (iii) the date on which we have, during the previous three-year period, issued more than $1 billion in non-convertible debt securities, or (iv) the date on which we are deemed to be a “large accelerated filer” as defined in the Exchange Act.

We have incurred and expect to continue to incur significant costs and have devoted and will continue to devote substantial management time as a result of operating as a public company, and these commitments will increase after we are no longer an “emerging growth company,” which could adversely affect our business and operating results.

As a public company, we have incurred and expect to continue to incur significant legal, accounting and other expenses. For example, we are required to comply with certain of the requirements of the Sarbanes-Oxley Act and the Dodd Frank Wall Street Reform and Consumer Protection Act, as well as rules and regulations implemented by the SEC and the NASDAQ Stock Market, including the establishment and maintenance of effective disclosure controls and procedures, internal control over financial reporting, and changes in corporate governance practices. Despite recent reform made possible by the JOBS Act, which allows us to take advantage of certain exemptions from various reporting requirements applicable to other public companies that are not “emerging growth companies,” compliance with these requirements increases our legal and financial compliance costs and makes some activities more time-consuming and costly compared to when we were a privately-held company. In addition, our management and other personnel must divert attention from operational and other business matters to devote substantial time to these public company requirements.

After we are no longer an “emerging growth company,” we expect to incur significant expenses and devote substantial management effort toward ensuring compliance with the requirements of Section 404(b) of the Sarbanes-Oxley Act, when applicable to us.

We cannot predict or estimate the amount of additional costs we may incur in the future as a result of being a public company or the timing of such costs. Being a public company also makes it more difficult and more expensive for us to obtain director and officer liability insurance, and we may be required to accept reduced policy limits and coverage or incur substantially higher costs to obtain the same or similar coverage for our officers and directors in the future. As a result, it may be more difficult for us to attract and retain qualified people to serve on our board of directors and our board committees or as executive officers.

We are an “emerging growth company” and we cannot be certain if the reduced disclosure requirements applicable to emerging growth companies makes our common stock less attractive to investors.

We are an “emerging growth company,” as defined in the JOBS Act, and, for so long as we remain an "emerging growth company," we may choose to take advantage of certain exemptions from various reporting requirements that are applicable to other public companies that are not “emerging growth companies” including, but not limited to, the auditor

attestation requirements of Section 404 of the Sarbanes-Oxley Act, reduced disclosure obligations regarding executive compensation in our periodic reports and proxy statements, and exemptions from the requirements of holding a nonbinding advisory vote on executive compensation and shareholder approval of any golden parachute payments not previously approved. We cannot assess if investors find our common stock less attractive for so long as we choose to rely on these exemptions. If some investors find our common stock less attractive as a result of our choice to reduce disclosure, there may be a less active trading market for our common stock and our trading price may be more volatile.

Table of Contents

Market volatility may affect our stock price and the value of an investment in our common stock and could subject us to litigation.

The trading price of our common stock has been, and may continue to be, subject to significant fluctuations in response to a number of factors, most of which we cannot predict or control, including:

- announcements of new solutions, services or technologies, commercial relationships, acquisitions or other events by us or our competitors;
- fluctuations in stock market prices and trading volumes of securities of similar companies;
- general market conditions and overall fluctuations in U.S. equity markets;
- variations in our operating results, or the operating results of our competitors;
- changes in our financial guidance or securities analysts' estimates of our financial performance;
- changes in accounting principles;
- sales of large blocks of our common stock, including sales by our executive officers, directors and significant stockholders;
- additions or departures of any of our key personnel;
- announcements related to litigation;
- changing legal or regulatory developments in the United States and other countries; and
- discussion of us or our stock price by the financial press and in online investor communities.

In addition, the stock market in general, and the stocks of technology companies such as ours in particular, have experienced substantial price and volume volatility that is often seemingly unrelated to the operating performance of particular companies. These broad market fluctuations may cause the trading price of our common stock to decline. In the past, securities class action litigation has often been brought against a company after a period of volatility in the trading price of its common stock. We may become involved in this type of litigation in the future. Any securities litigation claims brought against us could result in substantial expenses and the diversion of our management's attention from our business.

An active trading market for our common stock may not be sustained.

Our common stock is listed on the NASDAQ Stock Market under the symbol "QLYS." However, there can be no assurance that an active trading market for our common stock will be sustained. Accordingly, we cannot provide any assurance regarding the liquidity of any trading market or the ability of an investor to sell shares of our common stock when desired or the prices that may be obtained for such shares.

Concentration of ownership among our existing executive officers, directors and holders of 5% or more of our outstanding common stock may prevent new investors from influencing significant corporate decisions.

As of December 31, 2012, our executive officers, directors and holders of 5% or more of our outstanding common stock beneficially own, in the aggregate, a majority of our outstanding common stock. As a result, such persons, acting together, have the ability to control our management and affairs and substantially all matters submitted to our stockholders for approval, including the election and removal of directors and approval of any significant transaction. These persons also have the ability to control our management and business affairs. This concentration of ownership may have the effect of delaying, deferring or preventing a change in control, impeding a merger, consolidation, takeover or other business combination involving us, or discouraging a potential acquirer from making a tender offer or otherwise attempting to obtain control of our business, even if such a transaction would benefit other stockholders.

Table of Contents

Future sales of shares by existing stockholders could cause our stock price to decline.

We commenced trading of our common stock on September 28, 2012 and on October 3, 2012, we closed our initial public offering, or the IPO, of 8,711,250 shares of common stock. The offering included 7,836,250 shares sold and issued by us and 875,000 shares sold by selling stockholders. As of December 31, 2012, we had 31,420,028 shares of common stock outstanding. The 8,711,250 shares sold in the IPO are freely tradable. The remaining outstanding common shares of 22,708,778 are subject to lock up agreements and may be sold upon expiration of the lock-up agreements in March 2013, subject to compliance with applicable law. In addition, as of December 31, 2012, we had outstanding options to purchase 6,513,508 shares of common stock that, if exercised, will result in these additional shares becoming available for sale upon expiration of the lock-up agreements. A large portion of these shares and options are held by a small number of persons and investment funds. Sales by these stockholders or optionholders of a substantial number of shares could significantly reduce the trading price of our common stock. Moreover, certain holders of shares of common stock have rights, subject to some conditions, to require us to file registration statements covering the shares they currently hold, or to include these shares in registration statements that we may file for ourselves or other stockholders.

An aggregate of 2,902,125 shares of our common stock is reserved for future issuance under our 2012 Equity Incentive Plan, which can be freely sold in the public market upon issuance, subject to lock-up agreements. If a large number of these shares are sold in the public market, the sales could reduce the trading price of our common stock.

If securities or industry analysts do not publish research or publish inaccurate or unfavorable research about our business, our stock price and trading volume could decline.

The trading market for our common stock depends in part on the research and reports that securities and industry analysts publish about us and our business. If we do not maintain adequate research coverage or if one or more of the analysts who covers us downgrades our stock or publishes inaccurate or unfavorable research about our business, our stock price would likely decline. If one or more of these analysts ceases coverage of our company or fails to publish reports on us regularly, demand for our stock could decrease, which could cause our stock price and trading volume to decline.

We do not intend to pay dividends on our common stock and therefore any returns will be limited to the value of our stock.

We have never declared or paid any cash dividend on our common stock. We currently anticipate that we will retain future earnings for the development, operation and expansion of our business and do not anticipate declaring or paying any cash dividends for the foreseeable future. Any return to stockholders will therefore be limited to the value of their stock.

Anti-takeover provisions in our charter documents and under Delaware law could make an acquisition of us, which may be beneficial to our stockholders, more difficult and may prevent attempts by our stockholders to replace or remove our current management.

Our amended and restated certificate of incorporation and amended and restated bylaws contain provisions that may delay or prevent an acquisition of us or a change in our management. These provisions include:

- authorizing “blank check” preferred stock, which could be issued by the board without stockholder approval and may contain voting, liquidation, dividend and other rights superior to our common stock, which would increase the number of outstanding shares and could thwart a takeover attempt;
- a classified board of directors whose members can only be dismissed for cause;
- the prohibition on actions by written consent of our stockholders;

- the limitation on who may call a special meeting of stockholders;
- the establishment of advance notice requirements for nominations for election to our board of directors or for proposing matters that can be acted upon at stockholder meetings; and
- the requirement of at least two-thirds of the outstanding capital stock to amend any of the foregoing second through fifth provisions.

Table of Contents

In addition, because we are incorporated in Delaware, we are governed by the provisions of Section 203 of the Delaware General Corporation Law, which limits the ability of stockholders owning in excess of 15% of our outstanding voting stock to merge or combine with us. Although we believe these provisions collectively provide for an opportunity to obtain greater value for stockholders by requiring potential acquirers to negotiate with our board of directors, they would apply even if an offer rejected by our board were considered beneficial by some stockholders. In addition, these provisions may frustrate or prevent any attempts by our stockholders to replace or remove our current management by making it more difficult for stockholders to replace members of our board of directors, which is responsible for appointing the members of our management.

Item 1B. Unresolved Staff Comments

None.

Item 2. Properties

Our principal executive offices are located in Redwood City, California, where we occupy a 50,000 square-foot facility under a lease expiring on November 30, 2017. We have additional U.S. offices in Bellevue, Washington; Denver, Colorado; Durham, North Carolina; and Madison, Wisconsin. We also lease offices in Beijing, China; Courbevoie, France; Manila, Philippines; Munich, Germany; Pune, India; Ras al-Khaimah, United Arab Emirates; Slough, United Kingdom; and Tokyo, Japan. We believe our facilities are adequate for our current needs and for the foreseeable future.

We operate two principal data centers at third-party facilities in Santa Clara, California and Geneva, Switzerland.

Item 3. Legal Proceedings

From time to time we may become involved in legal proceedings or be subject to claims arising in the ordinary course of our business. We are not presently a party to any legal proceedings that, if determined adversely to us, would individually or taken together have a material adverse effect on our business, operating results, financial condition or cash flows. Regardless of the outcome, litigation can have an adverse impact on us because of defense and settlement costs, diversion of management resources and other factors.

Item 4. Mine Safety Disclosures.

Not Applicable.

Table of Contents

PART II

Item 5. Market for Registrant's Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities

Market Information

Our common stock has been listed on the NASDAQ Stock Market under the trading symbol “QLYS” since September 28, 2012. Prior to that date, there was no public trading market for our common stock. Our IPO was priced at $12.00 per share on September 27, 2012. The following table sets forth the high and low per share sales prices for our common stock as reported on the NASDAQ Stock Market for the periods indicated:

	Low	High
Fiscal 2012:		
Fourth quarter	$11.07	$15.25
Third quarter (from September 28, 2012)	$12.00	$14.85

Holders of Common Equity

As of February 28, 2013, there were approximately 501 holders of record of our common stock. Because many of our shares of common stock are held by brokers and other institutions on behalf of stockholders, we are unable to estimate the total number of stockholders represented by these record holders.

Dividend Policy

We have never declared or paid any cash dividends on our capital stock. We currently intend to retain any future earnings to fund business development and growth, and do not expect to pay any dividends in the foreseeable future. Any future determination to declare cash dividends will be made at the discretion of our board of directors, subject to applicable laws, and will depend on a number of factors, including our financial condition, results of operations, capital requirements, contractual restrictions, general business conditions and other factors that our board of directors may deem relevant.

Securities Authorized for Issuance under Equity Compensation Plans

The following table summarizes information about our equity compensation plans as of December 31, 2012. All outstanding awards relate to our common stock.

Plan Category	(a) Number of Securities to be Issued Upon Exercise of Outstanding Options, Warrants and Rights	(b) Weighted-Average Exercise Price of Outstanding Options, Warrants and Rights	(c) Number of Securities Remaining Available for Future Issuance Under Equity Compensation Plans (Excluding Securities Reflected in Column (a))
Equity compensation plans approved by security holders[1]	6,513,508	$4.39	2,902,125

[1] Equity compensation plans approved by stockholders include the 2000 Equity Incentive Plan, as amended and the 2012 Equity Incentive Plan. Prior to our IPO, we issued securities under our 2000 Equity Incentive Plan, as amended. Following our IPO, we issued securities under our 2012 Equity Incentive Plan.

Table of Contents

Stock Price Performance Graph

The following graph shows a comparison from September 28, 2012 (the date our common stock commenced trading on the NASDAQ Stock Market) through December 31, 2012 of the cumulative total return for an investment of $100 (and the reinvestment of dividends) in our common stock, the NASDAQ Global Select Market and the NASDAQ Computer. Such returns are based on historical results and are not intended to suggest future performance.

* $100 invested on 9/28/12 in stock or index, including reinvestment of dividends. Fiscal year ending December 31.

	September 28, 2012	October 31, 2012	November 30, 2012	December 31, 2012
Qualys Inc.	$100.00	$91.67	$94.49	$104.45
NASDAQ Global Select Market	$100.00	$95.55	$96.67	$96.97
NASDAQ Computer	$100.00	$93.12	$93.04	$92.56

The information on the above Stock Price Performance Graph shall not be deemed to be “filed” for purposes of Section 18 of the Securities Exchange Act of 1934, as amended, or otherwise subject to the liabilities of that section or Sections 11 and 12(a)(2) of the Securities Act of 1933, as amended, and shall not be incorporated by reference into any registration statement or other document filed by us with the Securities and Exchange Commission, whether made before or after the date of this Annual Report on Form 10-K, regardless of any general incorporation language in such filing, except as shall be expressly set forth by specific reference in such filing.

Table of Contents

Recent Sales of Unregistered Securities and Use of Proceeds

Use of Proceeds from Public Offering of Common Stock

The Form S-1 Registration Statement (Registration No. 333-182027) relating to our IPO was declared effective by the SEC on September 27, 2012 and the offering commenced on September 28, 2012. On October 3, 2012, we closed our IPO and received net proceeds of approximately $87.5 million after deducting underwriting discounts and commissions, and before deducting total expenses in connection with our IPO of approximately $2.9 million.

We believe our existing cash and cash from operations will be sufficient to fund our operations for at least the next twelve months. We intend to use the net proceeds from the offering for capital expenditures, working capital and other general corporate purposes, which may include hiring additional personnel and investing in sales and marketing and research and development. In addition, we expect to spend approximately $12.0 million through December 31, 2013 for capital expenditures, primarily related to infrastructure to support the anticipated growth in our business. We may also use a portion of the net proceeds to acquire or invest in complementary businesses, technologies, or other assets. We have not entered into any agreements or commitments with respect to any acquisitions or investments at this time.

Pending these uses, we invested the net proceeds in highly liquid money market funds, fixed-income U.S. government agency securities and commercial paper.

Purchases of Equity Securities by the Issuer and Affiliated Purchasers

No shares of our common stock were repurchased during the fourth quarter of 2012.

Table of Contents

Item 6. Selected Consolidated Financial and Other Data

The following selected consolidated financial and other data should be read in conjunction with "Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations" and our consolidated financial statements, related notes and other financial information included elsewhere in this Annual Report on Form 10-K. Our historical results are not necessarily indicative of the results that may be expected in the future, and the results for the year ended December 31, 2012 are not necessarily indicative of operating results to be expected for any other period.

	Year Ended December 31,				
	2012	2011	2010	2009	2008
	(in thousands, except per share data)				
Consolidated Statements of Operations Data:					
Revenues	$91,420	$76,212	$65,432	$57,425	$50,258
Cost of revenues[1]	18,404	13,247	11,204	10,692	9,540
Gross profit	73,016	62,965	54,228	46,733	40,718
Operating expenses:					
Research and development[1]	20,195	19,633	15,780	13,377	11,705
Sales and marketing[1]	37,738	31,526	29,056	24,782	22,830
General and administrative[1]	12,079	8,900	8,183	7,455	6,670
Total operating expenses	70,012	60,059	53,019	45,614	41,205
Income (loss) from operations	3,004	2,906	1,209	1,119	(487)
Other income (expense), net:					
Interest expense	(192)	(204)	(186)	(180)	(263)
Interest income	14	14	3	10	85
Other income (expense), net	(188)	(346)	(383)	130	(176)
Total other income (expense), net	(366)	(536)	(566)	(40)	(354)
Income (loss) before provision for (benefit from) income taxes	2,638	2,370	643	1,079	(841)
Provision for (benefit from) income taxes	358	416	(204)	220	23
Net income (loss)	$2,280	$1,954	$847	$859	$(864)
Net income (loss) attributable to common stockholders	$1,076	$436	$179	$171	$(864)
Net income (loss) per share attributable to common stockholders: [2]					
Basic	$0.09	$0.09	$0.04	$0.04	$(0.21)
Diluted	$0.08	$0.08	$0.04	$0.04	$(0.21)
Weighted-average shares used in computing net income (loss) per share attributable to common stockholders: [2]					
Basic	11,891	5,053	4,706	4,400	4,144
Diluted	28,352	24,194	23,562	22,804	4,144

Table of Contents

	As of December 31,				
	2012	2011	2010	2009	2008
	(in thousands)				
Consolidated Balance Sheet Data:					
Cash, cash equivalents and short-term investments	$118,432	$24,548	$15,010	$9,949	$7,655
Total assets	170,318	68,789	44,360	34,244	27,932
Deferred revenues, current	56,497	46,717	37,811	33,266	29,019
Deferred revenues, noncurrent	8,616	4,713	1,734	1,864	1,090
Convertible preferred stock	—	63,873	63,745	63,745	63,745
Total stockholders' equity (deficit)	91,555	(64,424)	(69,401)	(72,740)	(74,310)

(1) Includes stock-based compensation as follows:

	Year Ended December 31,				
	2012	2011	2010	2009	2008
	(in thousands)				
Cost of revenues	$276	$143	$80	$47	$49
Research and development	672	499	359	315	227
Sales and marketing	1,074	578	467	284	218
General and administrative	1,430	927	964	474	309
Total stock-based compensation	$3,452	$2,147	$1,870	$1,120	$803

(2) See Notes 1 and 12 to our consolidated financial statements included elsewhere in this Annual Report on Form 10-K for an explanation of the calculations of our basic and diluted income (loss) per share attributable to common stockholders.

Other Financial Data (unaudited):

In addition to measures of financial performance presented in our consolidated financial statements, we monitor the key metrics set forth below to help us evaluate growth trends, establish budgets, measure the effectiveness of our sales and marketing efforts and assess operational efficiencies.

	Four Quarters Ended December 31,				
	2012	2011	2010	2009	2008
	(in thousands)				
Four-Quarter Bookings	$101,200	$85,118	$69,977	$61,672	$53,765
	Year Ended December 31,				
	2012	2011	2010	2009	2008
	(in thousands)				
Adjusted EBITDA	$13,797	$10,426	$7,648	$6,162	$3,677

Table of Contents

Non-GAAP Financial Measures

Four-Quarter Bookings

We monitor Four-Quarter Bookings, a non-GAAP financial measure, which is calculated as revenues for the preceding four quarters plus the change in current deferred revenues for the same period. We believe this metric provides an additional tool for investors to use in assessing our business performance in a way that more fully reflects current business trends than reported revenues and reduces the variations in any particular quarter caused by customer subscription renewals. We believe Four-Quarter Bookings reflects the material sales trends for our business because it includes sales of subscriptions to new customers, as well as subscription renewals and upsells of additional subscriptions to existing customers. Since over 80% of our subscriptions are one year in length, we use current deferred revenues in this metric in order to focus on revenues to be generated over the next four quarters and to exclude the impact of multi-year subscriptions. Under our revenue recognition policy, we record subscription fees as deferred revenues and recognize revenues ratably over the subscription periods. For this reason, substantially all of our revenues for a period are typically generated from subscriptions commencing in prior periods. In addition, subscription renewals may vary during the year based on the date of our customers' original subscriptions, customer requests to modify subscription periods, or other factors.

The following unaudited table presents the reconciliation of revenues to Four-Quarter Bookings for the four quarters ended December 31, 2012, 2011, 2010, 2009 and 2008.

	Four Quarters Ended December 31,				
	2012	2011	2010	2009	2008
	(in thousands)				
Revenues	$91,420	$76,212	$65,432	$57,425	$50,258
Deferred revenues, current					
Beginning of the Four-Quarter Period	46,717	37,811	33,266	29,019	25,512
Ending	56,497	46,717	37,811	33,266	29,019
Net change	9,780	8,906	4,545	4,247	3,507
Four-Quarter Bookings	$101,200	$85,118	$69,977	$61,672	$53,765

Adjusted EBITDA

We monitor Adjusted EBITDA, a non-GAAP financial measure, to analyze our financial results and believe that it is useful to investors, as a supplement to U.S. GAAP measures, in evaluating our ongoing operational performance and enhancing an overall understanding of our past financial performance. We believe that Adjusted EBITDA helps illustrate underlying trends in our business that could otherwise be masked by the effect of the income or expenses that we exclude in Adjusted EBITDA. Furthermore, we use this measure to establish budgets and operational goals for managing our business and evaluating our performance. We also believe that Adjusted EBITDA provides an additional tool for investors to use in comparing our recurring core business operating results over multiple periods with other companies in our industry.

Adjusted EBITDA should not be considered in isolation from, or as a substitute for, financial information prepared in accordance with U.S. GAAP. We calculate Adjusted EBITDA as net income (loss) before (1) other (income) expense, net, which includes interest income, interest expense and other income and expense, (2) provision for (benefit from) income taxes, (3) depreciation and amortization of property and equipment, (4) amortization of intangible assets and (5) stock-based compensation.

Table of Contents

The following unaudited table presents the reconciliation of net income (loss) to Adjusted EBITDA for the years ended December 31, 2012, 2011, 2010, 2009 and 2008.

	Year Ended December 31,				
	2012	2011	2010	2009	2008
	(in thousands)				
Net income (loss)	$2,280	$1,954	$847	$859	$(864)
Other (income) expense, net	366	536	566	40	354
Provision for (benefit from) income taxes	358	416	(204)	220	23
Depreciation and amortization of property and equipment	6,895	4,939	4,400	3,868	3,317
Amortization of intangible assets	446	434	169	55	44
Stock-based compensation	3,452	2,147	1,870	1,120	803
Adjusted EBITDA	$13,797	$10,426	$7,648	$6,162	$3,677

Limitations of Four-Quarter Bookings and Adjusted EBITDA

Four-Quarter Bookings and Adjusted EBITDA, non-GAAP financial measures, have limitations as analytical tools, and should not be considered in isolation from or as a substitute for the measures presented in accordance with U.S. GAAP. Some of these limitations are:

- Four-Quarter Bookings reflects the amount of revenues over a four-quarter period, plus the net change in the current portion of deferred revenues, while revenues are recognized ratably over the subscription periods;
- Adjusted EBITDA does not reflect certain cash and non-cash charges that are recurring;
- Adjusted EBITDA does not reflect income tax payments that reduce cash available to us;
- Adjusted EBITDA excludes depreciation and amortization of property and equipment and, although these are non-cash charges, the assets being depreciated and amortized may have to be replaced in the future; and
- Other companies, including companies in our industry, may calculate Four-Quarter Bookings or Adjusted EBITDA differently or not at all, which reduces their usefulness as a comparative measure.

Because of these limitations, Four-Quarter Bookings and Adjusted EBITDA should be considered alongside other financial performance measures, including revenues, net income (loss) and our financial results presented in accordance with U.S. GAAP.

Table of Contents

Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations

You should read the following discussion in conjunction with the section titled "Selected Consolidated Financial and Other Data" and our consolidated financial statements and the related notes included elsewhere in this Annual Report on Form 10-K. In addition to historical information, this discussion contains forward-looking statements that involve risks and uncertainties that could cause our actual results to differ materially from our expectations, as discussed in "Forward-Looking Statements" in Part I of this Annual Report on Form 10-K. Factors that could cause such differences include, but are not limited to, those described in the section titled "Risk Factors" and elsewhere in this Annual Report on Form 10-K.

Overview

We are a pioneer and leading provider of cloud security and compliance solutions that enable organizations to identify security risks to their IT infrastructures, help protect their IT systems and applications from ever-evolving cyber attacks and achieve compliance with internal policies and external regulations. Our cloud solutions address the growing security and compliance complexities and risks that are amplified by the dissolving boundaries between internal and external IT infrastructures and web environments, the rapid adoption of cloud computing and the proliferation of geographically dispersed IT assets. Our integrated suite of security and compliance solutions delivered on our QualysGuard Cloud Platform enable our customers to identify their IT assets, collect and analyze large amounts of IT security data, discover and prioritize vulnerabilities, recommend remediation actions and verify the implementation of such actions. Organizations use our integrated suite of solutions delivered on our QualysGuard Cloud Platform to cost-effectively obtain a unified view of their security and compliance posture across globally-distributed IT infrastructures.

We were founded and incorporated in December 1999 with a vision of transforming the way organizations secure and protect their IT infrastructure and applications and initially launched our first cloud solution, QualysGuard Vulnerability Management, in 2000. This solution has provided the substantial majority of our revenues to date, representing 87%, 90% and 92% of total revenues in 2012, 2011 and 2010, respectively. As this solution gained acceptance, we introduced new solutions to help customers manage increasing IT security and compliance requirements. In 2006, we added our PCI Compliance solution, and in 2008, we added our Policy Compliance solution. In 2009, we broadened the scope of our cloud services by adding Web Application Scanning. We continued our expansion in 2010, launching Malware Detection Service and Qualys SECURE Seal for automated protection of websites.

We provide our solutions through a software-as-a-service model, primarily with renewable annual subscriptions. These subscriptions require customers to pay a fee in order to access our cloud solutions. We invoice our customers for the entire subscription amount at the start of the subscription term, and the invoiced amounts are treated as deferred revenues and are recognized ratably over the term of each subscription. Historically, we have experienced significant revenue growth from existing customers as they renew and purchase additional subscriptions. Revenues from customers existing at or prior to December 31, 2011 grew $7.8 million to $84.0 million during 2012. We expect this trend to continue.

We market and sell our solutions to enterprises, government entities and to small and medium size businesses across a broad range of industries, including education, financial services, government, healthcare, insurance, manufacturing, media, retail, technology and utilities. As of December 31, 2012, we had over 6,150 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. In 2012, 2011 and 2010, approximately 68%, 67% and 67%, respectively, of our revenues were derived from customers in the United States. We sell our solutions to enterprises and government entities primarily through our field sales force and to small and medium-sized businesses through our inside sales force. We generate a significant portion of sales through our

channel partners, including managed service providers, value-added resellers and consulting firms in the United States and internationally.

We have had strong revenue growth over the past three years. Our revenues increased from $65.4 million in 2010 to $76.2 million in 2011, and reached $91.4 million in 2012, representing period-over-period increases of $10.8 million, and $15.2 million, or 16% and 20%, respectively. We generated net income of $0.8 million in 2010, $2.0 million in 2011, and $2.3 million in 2012.

Table of Contents

On September 28, 2012, our common stock commenced trading on the NASDAQ Stock Market under the trading symbol “QLYS,” and on October 3, 2012 we closed our initial public offering. In our initial public offering, we sold and issued 7,836,250 shares and certain selling stockholders sold an additional 875,000 shares. The net proceeds to us from the offering were approximately $87.5 million, after deducting underwriting discounts and commissions, and before deducting total expenses in connection with this offering of $2.9 million.

Key Metrics

In addition to measures of financial performance presented in our consolidated financial statements, we monitor the key metrics set forth below to help us evaluate growth trends, establish budgets, measure the effectiveness of our sales and marketing efforts, and assess operational efficiencies.

Four-Quarter Bookings

We monitor Four-Quarter Bookings, a non-GAAP financial measure, which is calculated as revenues for the preceding four quarters plus the change in current deferred revenues for the same period. We believe this metric provides an additional tool for investors to use in assessing our business performance in a way that more fully reflects current business trends than reported revenues and reduces the variations in any particular quarter caused by customer subscription renewals. We believe Four-Quarter Bookings reflects the material sales trends for our business because it includes sales of subscriptions to new customers, as well as subscription renewals and upsells of additional subscriptions to existing customers. Since over 80% of our subscriptions are one year in length, we use current deferred revenues in this metric in order to focus on revenues to be generated over the next four quarters and to exclude the impact of multi-year subscriptions. Under our revenue recognition policy, we record subscription fees as deferred revenues and recognize revenues ratably over the subscription periods. For this reason, substantially all of our revenues for a period are typically generated from subscriptions commencing in prior periods. In addition, subscription renewals may vary during the year based on the date of our customers’ original subscriptions, customer requests to modify subscription periods or other factors. See the section titled “Selected Consolidated Financial and Other Data-Non-GAAP Financial Measures” for a reconciliation of revenues to Four-Quarter Bookings.

	Four Quarters Ended December 31,	
	2012	2011