FORRESTER®

For: Security &
Risk Professionals

Market Overview: Vulnerability Management

by Kelley Mak and Rick Holland, April 22, 2015

KEY TAKEAWAYS

Security And Risk Pros Can't Keep Up With The Tsunami Of Vulnerabilities

CVSS reported 7,945 official vulnerabilities in 2014 alone -- which means that S&R pros simply can't handle the volume of findings from vulnerability assessments. And the rise of the Internet of Things means that employees and customers have bugs not just in their pockets, but also in their thermostats, in their cars, and on their wrists.

Integration Makes Vulnerability Management More Powerful

Integrating adjacent spaces like attack-path modeling, GRC, operational automation, and penetration testing with vulnerability management allows S&R pros to gain insight into prioritization, get a better picture of risk, reduce unneeded work, and decrease operational friction.

Vendors Offer Solutions To Move Vulnerability Management Past Scanning

Vulnerability management is a necessary component to security, but it becomes more meaningful when coupled with complementary security solutions. To aid in this, vendors offer products that link vulnerability management with technologies such as privileged identity management, configuration management, and behavioral monitoring.

Market Overview: Vulnerability Management

Vulnerability Management Is Key For Defending Your Digital Business

by Kelley Mak and Rick Holland
with Laura Koetzle, Stephanie Balaouras, and Josh Blackborow

WHY READ THIS REPORT

Cybersecurity incident disclosures and vulnerability warnings continue to be released at an alarming and fatiguing rate, and there aren't any signs of breach activity slowing down. Vulnerability management is more important than ever, yet staying on top of vulnerabilities poses a major challenge for security and risk (S&R) professionals. This report analyzes the ways in which the vulnerability management technology space has evolved. It will help S&R pros repair their strained or broken processes and move past low-impact checkbox scanning to proactive, risk-based assessments.

Table Of Contents

Notes & Resources

Forrester interviewed 19 vendor companies in developing this report.

Related Research Documents

The Forrester Wave™: Application Security, Q4 2014

Forrester's Targeted-Attack Hierarchy Of Needs: Assess Your Core Capabilities

Introducing Forrester's Prioritized Patching Process (P3)

MANAGING VULNERABILITIES IS CRITICAL, BUT S&R STILL STRUGGLES WITH IT

Exploiting weaknesses in applications, browsers, and operating systems is often the first step in compromising a target. In Forrester's Business Technographics® Global Security Survey, 2014, software vulnerabilities were the leading method for carrying out external attacks, and web applications were the third most popular avenue (see Figure 1-1). Addressing existing threats and vulnerabilities was security technology decision-makers' top priority in 2014 and has been a top three priority for the past three years (see Figure 1-2).[1] Furthermore, 76% of IT security groups say that they are mostly or fully responsible for threat and vulnerability management (see Figure 1-3).

Despite the focus on vulnerabilities, security and risk (S&R) teams still struggle to address them. Vulnerabilities come in a variety of flavors, targeting web applications, network controls, databases, or endpoints. If it's connected to the network and contains software, it can contain vulnerabilities. Cross-site scripting (XSS) and SQL injection have been around for years, yet we struggle to remediate them — Verizon's "2015 Data Breach Investigations Report" found that 19% of web application attacks it studied began with successful SQL injections.[2] Flawed vulnerability management practices are making it trivial for attackers to breach you. Traditional vulnerability scanning falls short because:

- **The main driver is compliance.** A host of government and industry regulations, such as the Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act (HIPAA), mandate a regular and active vulnerability management program. Vulnerability management tools are mainly used to ensure minimal compliance with regulations, the dreaded "checkbox/tick-box compliance." Many organizations rarely operate outside of these standards. Home Depot and Target had met their PCI compliance requirements, but they still lost payment card data.[3] As one executive at vulnerability management vendor Core Security put it, "Compliance has become a ceiling, not a floor."

- **S&R pros are overwhelmed by vulnerability scanner findings.** 2014's avalanche of 7,945 vulnerabilities far outstripped 2013's 5,191 (see Figure 2). S&R pros have neither the time nor the resources to handle the sheer volume of findings from vulnerability assessments. 2014 terrorized S&R pros with pernicious and widespread vulnerabilities like Heartbleed, Shellshock, and POODLE.[4] For example, attackers exploited the unpatched Heartbleed bug at Community Health Systems and stole around 4.5 million patients' data.[5] The attack allegedly occurred after the vulnerability was disclosed, highlighting Community Health Systems' laggard response.

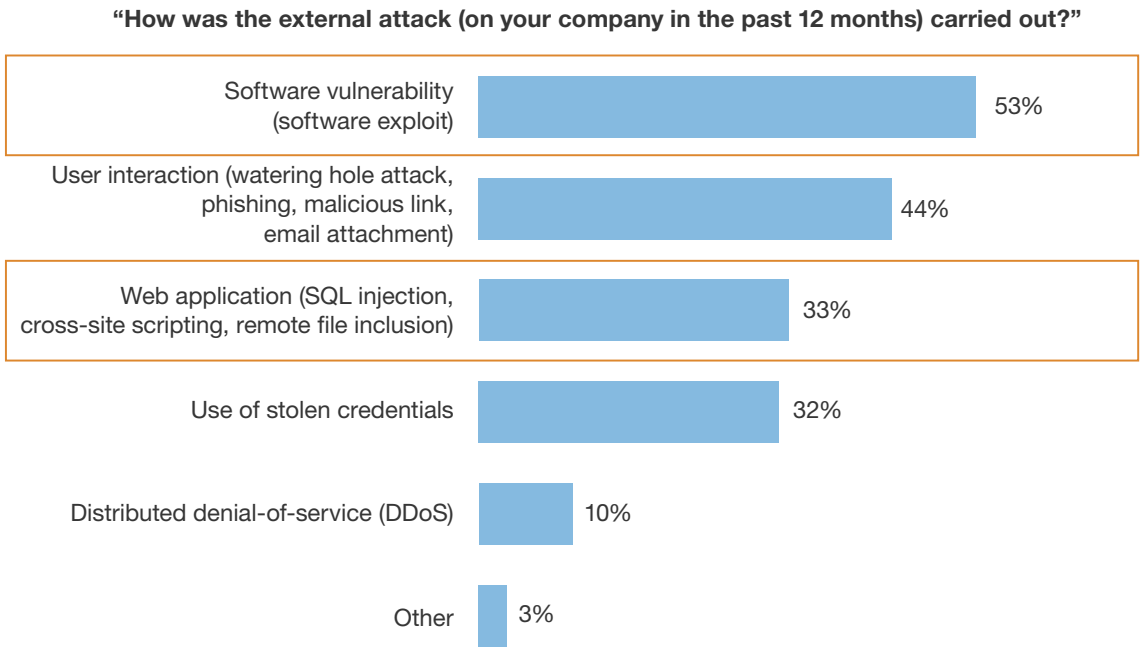
- **S&R pros lack proper prioritization.** Security and operations team have very limited resources, and remediating the most critical vulnerabilities is a constant challenge. Vulnerability scans produce reams of red flags, many of which are not immediately vital. This is because S&R pros often rely on default, vendor-supplied criticality measures or third-party metrics, such as Common Vulnerability Scoring System (CVSS). Researchers at the University of Trento in Italy found that CVSS scores focus on impact without enough emphasis on risk, such as the prevalence of exploits in the wild. In doing so, CVSS leads to inaccurate assessments of criticality and to S&R pros wasting resources remediating the wrong vulnerabilities.[6]

- **S&R teams have a multitude of different scanners.** S&R pros use a number of different vulnerability scanning solutions for their technology environment. For example, many firms use a traditional vulnerability scanner like Rapid7's Nexpose, a web application scanner like HP's WebInspect, a database scanner from Imperva, and an SAP scanning solution like Onapsis — all at the same time. Thus, getting a single view of the vulnerabilities across these scanners is a challenge. These solutions tend to silo results and prevent S&R pros from getting a clear macro understanding of the vulnerabilities of high-value assets.

- **The remediation process is painfully inefficient.** Vulnerability management and patch management go hand in hand because after the S&R group finds critical vulnerabilities, it must patch and validate them. However, remedial friction and inefficient handoff to the operations team can lengthen the time it takes to patch.[7] The longer the vulnerability window is open, the easier it is for an attacker to stroll in.

Figure 1 Vulnerabilities Plague Organizations

1-1 | Software vulnerabilities are the most commonly exploited avenues into organizations



Base: 117 North American and European security technology decision-makers who have experienced an external data breach in the past 12 months (1,000+ employees)

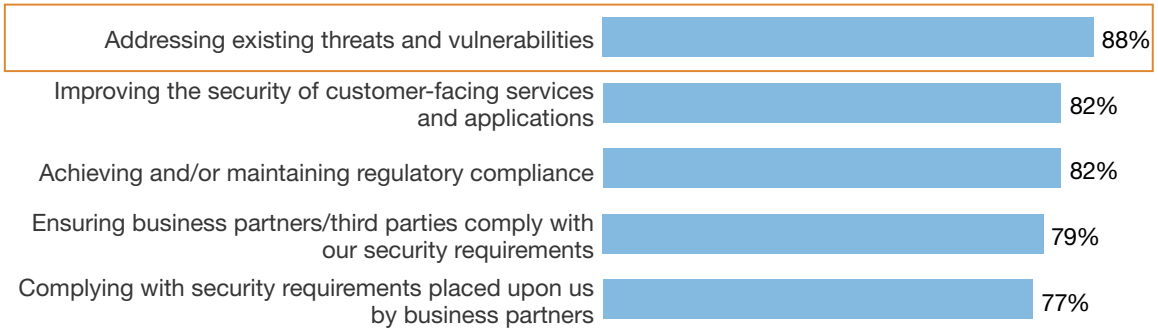
Source: Forrester's Business Technographics® Global Security Survey, 2014

119814 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Figure 1 Vulnerabilities Plague Organizations (Cont.)

1-2 Addressing threats and vulnerabilities is the top priority

"Which of the following initiatives are likely to be your firm's/organization's top IT security priorities over the next 12 months?"
(High/critical priorities — top five responses)

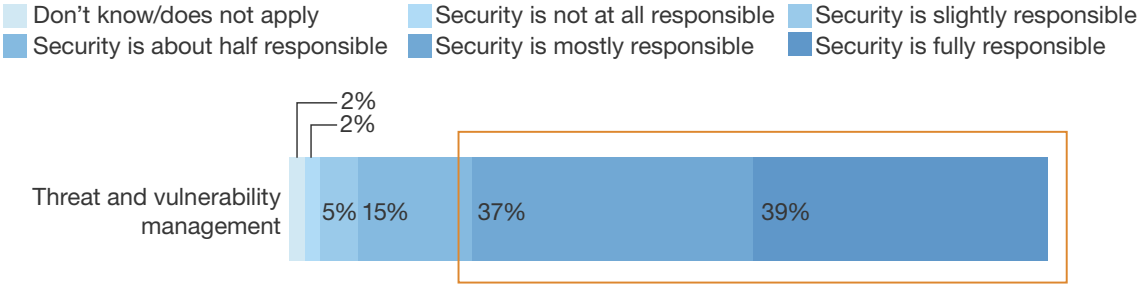


Base: 372 to 402 North American and European security technology decision-makers
(1,000+ employees)

Note: Base fluctuation is due to randomization of response options.

1-3 Majority of S&R pros are responsible for vulnerability management

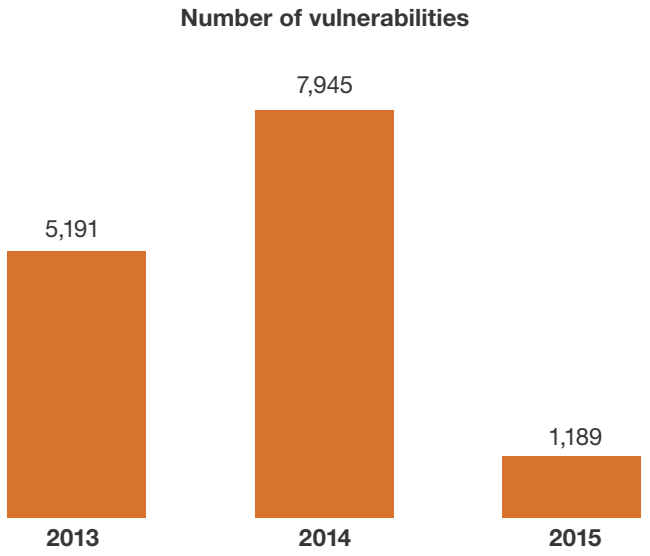
"To what extent is your firm's IT security group responsible for the following activities?"



Base: 701 North American and European security technology decision-makers
(1,000+ employees)

Source: Forrester's Business Technographics Global Security Survey, 2014

Figure 2 The Volume Of Vulnerabilities Is Overwhelming



Note: Data is up to date as of March 3, 2015.
Source: CVE Details (http://www.cvedetails.com)

VULNERABILITY MANAGEMENT IS MORE THAN JUST SCANNING

The vulnerability management process involves five important steps: 1) discover, 2) assess, 3) report, 4) remediate, and 5) validate (see Figure 3). However, S&R pros have trouble navigating the life cycle and instead find themselves falling back on low-value, tactical, checkbox vulnerability scanning. S&R pros run scans as needed, but they will often miss reporting, remediation, and validation. Here are the questions S&R pros wrestle with:

- **What should I scan?** While it would be ideal to know every single weakness, scanning your entire technology environment isn't feasible. Vulnerability scans involve sending and receiving large amounts of packets — hence, engaging all endpoints would be extremely taxing and disruptive for your network. Also, probing the whole of your systems for information will produce an overwhelming amount of results.

- **When should I scan?** Forrester's top customer vulnerability management inquiry is "How often should I scan X?" S&R pros commonly initiate scans on daily, weekly, monthly, quarterly, or annual basis, often as required by compliance mandates. Prioritization of assets — *not* compliance mandates — should determine scan frequency. Additionally, vulnerabilities are only detected at the time of scan, leaving a window of time between scans when systems remain or become vulnerable. You should do vulnerability assessments on a regular basis, if not continuously. You can't remediate what you don't know; vulnerability assessment frequency is directly related to your security risk visibility.

- **How do I make sense of this information?** After vulnerability scans, S&R pros get a giant list of the existing vulnerabilities in their environment. You need to triage the enormous volume of results — of which an alarming number will be marked "critical" — with a mix of process and technology. You can't fix everything, but you can implement measures to reduce the risk exposure of your organization. Thus, focus on your data. Base remediation prioritization on high-level measures of risk: host compromise difficulty, application data toxicity, and vulnerability intrinsic risk.[8] Vulnerability management technology platforms include tools to assist with the visualization and prioritization of vulnerability remediation efforts.

- **How should I remediate?** Solutions will depend on the nature of the problem and the availability of a fix. Remediation can constitute deploying software patches, correcting misconfigured settings of affected systems, or implementing additional security controls if a fix isn't available. At the same time, you might accept vulnerability risks depending on your organization's risk appetite. After you triage vulnerabilities, have IT operations carry out corrective actions and ensure the asset owners aware of the process.

- **How do I work with the operations team?** This is a painful roadblock for many organizations, and remediation timeliness suffers. The transfer of duties from security to operations is the digital equivalent of handing off a stack of paper. This isn't productive; operations must know the highest priorities they need to respond to with their limited resources. S&R pros and ops should be partners, not enemies. The important part here is communication. Reduce operational friction through clear roles and responsibilities and cooperation. Leverage vulnerability management tools for automation and workflow orchestration.

- **What next?** Vulnerability management doesn't stop after remediation. Rescan to verify all patch implementations and configuration corrections. Additionally, use penetration testing products and services to further validate that you've closed all the holes that have existing exploits in the wild. If remediation of your most critical assets fails, the entire vulnerability management process falls apart.

Figure 3 The Vulnerability Management Life Cycle

119814 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Disruptive Technologies Introduce More Vulnerabilities And Challenges

Today, practically every company is a technology company, with mobile applications, social communication channels, cloud services, and other innovations changing the way businesses engage at each stage of the customer life cycle.[9] Thus, the traditional technology border is extending, assets are proliferating, and data volumes are exploding. Your number of vulnerabilities increases as your attack surface expands, which puts your critical customer data and intellectual property at greater risk.

What does this mean for vulnerability management? Periodic scanning isn't enough, because snapshot assessments of risk aren't effective in today's dynamic environments. You need continuous monitoring.[10] Continuous monitoring is required by compliance mandates such as the Federal Information Security Management Act (FISMA), but it shouldn't stop there. Continuous monitoring provides situational awareness and real-time visibility into your environment. Yet monitoring alone isn't enough; continuous monitoring must extend into containment and response.

There's A Bug In Your Pocket

Mobility continues to extend your company's reach and utility in unique and powerful ways.[11] The mobile mind shift is an expectation that an individual (consumer or employee) can get what they want in their immediate context and moments of need.[12] What this means for S&R pros is that static security policies and controls must become dynamic security policies and controls determined at the time of engagement.[13] S&R pros need to be business enablers, or they'll risk business owners launching rogue mobile initiatives or bypassing security altogether.[14] But S&R pros still struggle with mobility, because:

- **Traditional vulnerability management is inadequate for securing the mobile moment.** According to Forrester's Global Business Technographics Telecommunications And Mobility Workforce Survey, 2015, 61% of employees work from home, 31% work in public places such as coffee shops, and 43% work while commuting at least a few times a month.[15] Content and services need to be available immediately for employees and easy to use. More people are opting for software-as-a-service (SaaS) applications to perform their job, rendering virtual private networks (VPNs) less effective in connecting devices to the corporate network. This poses a significant challenge: How can you scan devices when they aren't on the corporate network? The effectiveness of traditional vulnerability management on mobility is limited. S&R pros need to find a way to balance the seamlessness, simplicity, and availability of user experience with granular and proactive security.

- **More operating systems mean more problems.** A majority of employees use some form of a mobile device to get their jobs done, and these devices have an array of operating systems.[16] However, the most commonly used operating systems face their own challenges. An analysis by GFI Software of the National Vulnerability Database found that iOS had the second highest number of vulnerabilities in 2014, right behind Mac OS X.[17] Mobile phone carriers are notorious for not providing updates to the latest version of Android. This delay results in Android vulnerabilities that go unpatched, leaving mobile devices at risk. Google disclosed it will no longer be developing security patches for vulnerabilities found in Android versions below KitKat (4.4).[18] Yet as of March 2, 2015, more than half of the 1.4 billion Android users are using platform versions older than Android KitKat (4.4).[19]

Virtualization And Cloud Add To Vulnerability Complexity

Firms adopt cloud-based services and virtual systems for their cost, flexibility, and speed.[20] But transitioning to the cloud doesn't come without challenges. The dynamic nature of virtualization can create blind spots in vulnerability management. Virtual machines (VMs) are vulnerable to compromises like hyperjacking and hypervisor escape.[21] In 2014 alone, VMware provided advisories for 14 vulnerabilities.[22] Several startups, such as Evident.io and Threat Stack, offer solutions to help S&R pros manage the vulnerabilities in cloud environments. Evident.io provides Amazon Web Services (AWS) assessments for security vulnerabilities, usage of infrastructure, and risk posture. Threat Stack monitors and protects Linux workloads operating in AWS environments. Particular vulnerability management concerns for virtualization are:

- **Configuration management.** Provisioning and deleting virtual machines are easy tasks, but keeping track of VMs as they are spun up, cloned, moved, or suspended can be quite demanding. VM sprawl is a nightmare for many organizations. Unchecked virtualization is problematic for change and configuration management because of the inability to be certain you have scanned all systems, leaving your assets vulnerable.

- **Governance.** Hosting of workloads and data in a cloud infrastructure is a shared responsibility. For example, in Amazon's web security environment, Amazon is responsible for the underlying infrastructure but the customer is responsible for everything on top of that, such as the infrastructure-as-a-service (IaaS) and SaaS workloads. Protection of workloads regardless of location is still the liability of S&R pros, so protection must travel with the data.

The Connected World Raises The Bar

S&R pros need to stay ahead of the wave of technological change — or at least keep pace. Vulnerabilities can pop up all over, and S&R pros need to be both aware of and ready to remediate them. Looking ahead, vulnerability management programs must consider:

- **The Internet of Things (IoT).** People are finding novel ways of improving products by connecting them to other devices, systems, or services. Products such as smart refrigerators, connected home monitors, and intelligent printers will soon make their debut in the corporate environment. But don't let the allure of shiny new toys distract you. Researchers at HP Fortify studied 10 of the most popular IoT devices, which include home thermostats and alarms. They found that six out of the 10 evaluated devices that provide user interfaces were vulnerable to problems such as cross-site scripting and weak credentials.[23] Heartbleed and Shellshock affect IoT devices.

- **Third-party security.** Enterprises engage with multiple partners and third parties for daily business. But your partners' technology environments are a part of your digital ecosystem. If access controls are not properly implemented, a misstep in an affiliate's security is all an adversary needs to gain a foothold into your environment. The Target breach is a good example of the risks of connectivity to third parties. Adversaries compromised credentials from Target's HVAC contractor, Fazio Mechanical Services, and used them to move laterally into the retailer's network system. Once inside, attackers were able to exfiltrate 110 million consumers' credit card and personal data.[24]

VULNERABILITY MANAGEMENT IS REINVENTING ITSELF

Chief information security officers (CISOs) have tended to see vulnerability management as blocking and tackling — important, but not exciting or new. However, 2014's serious open source vulnerabilities put vulnerability management back in the spotlight. Forrester has found that traditional vulnerability scanners are commoditized with little difference between each in terms of capabilities. Vendors also understand the maturity of these tools and are adding more value to their product through a more comprehensive offering. We are seeing heightened activity in this space from:

- **Technology complements.** Vulnerability management is a necessary component to security, but it becomes more powerful when coupled with complementary security solutions like privileged identity management and configuration management. In the past several years, we have seen some interesting merger and acquisition movement that indicates the move to enhanced vulnerability management. In 2009, Rapid7 bought the Metasploit Project, an open source tool for penetration testing, to add to its vulnerability management solution.[25] BeyondTrust, specialists in privileged identity management, acquired vulnerability management vendor eEye Digital Security in 2012.[26] Security and compliance solution player Tripwire strengthened its portfolio with its acquisition of nCircle in 2013.[27]

- **Market offerings beyond traditional vulnerability scanning.** Vulnerability management vendors have developed new capabilities to extend beyond pure vulnerability scanning. Qualys' SaaS security suite includes web application scanning, web application firewall, and compliance monitoring. Core Security moved into the vulnerability management space with Core Insight, a solution focused on providing a single view into vulnerabilities across the organization. Rapid7's UserInsight provides behavioral monitoring and incident detection. Furthermore, Tenable Network Security developed its passive scanning technology to aid continuous monitoring.

- **New entrants like NopSec, Risk I/O, and Synack.** NopSec offers a SaaS vulnerability management product that helps S&R pros prioritize, remediate, and collaborate among technology management groups. Risk I/O's SaaS vulnerability management platform leverages external threat intelligence and exploit data. Synack pioneers a crowdsourced penetration testing solution for enterprises through a bug bounty program.

Integration Enhances Vulnerability Management

Vulnerability management is a means to an end: the reduction of attack surface to the CISO's most critical assets. According to Forrester's targeted attack hierarchy of needs, integration should be a key component of S&R pros' vulnerability management strategy.[28] Use integration to gain insight into prioritization, get a better picture of risk, reduce unneeded work, and decrease operational friction. Keep an eye on:

- **Attack path modeling.** These tools help S&R pros map network topology to understand vulnerable systems based on attack paths within the environment.[29] Integrating vulnerability management with attack path modeling aids risk, prioritization, and remediation efforts to secure assets that are within arm's reach for an attacker. Vendors that provide this capability include Core Security, RedSeal, and Skybox Security.

- **Governance, risk, and compliance (GRC).** The data and information collected from vulnerability management is useful when integrated with a GRC platform for enriched business context, workflow, and risk analysis. Tying the risks from vulnerability management into GRC

aids in unifying the risks across the organization, mapping risks to business objectives, and reviewing risks regularly. Example GRC vendors that work with vulnerability management tools are EMC-RSA, LogicManager, Modulo, and Rsam.

- **Remediation automation.** Rectifying vulnerabilities involves coordination between security and risk professionals and their infrastructure and operations (I&O) colleagues. After vulnerabilities are found, teams on both sides are required to make sure fixes are implemented and then validated for completion. ITSM vendors such as BMC and ServiceNow offer integrations that automate ticket and workflow creation upon finding vulnerabilities and ensure actions are assigned to the appropriate team. Qualys and BMC have made an integrated solution by combining Qualys' Vulnerability Management and BMC's BladeLogic.[30]

- **Penetration testing.** Vulnerability scans uncover potential vulnerabilities in your environment, but penetration testing reduces false positives by determining which weaknesses are valid and exploitable. Scanning alone simply isn't enough. CISOs need to know which vulnerabilities are actually exploitable so they can properly prioritize remediation efforts. Incorporate the results of penetration tests into your vulnerability scanning solutions. Penetration testing depth can vary with a firm's maturity, and solutions exist for different levels of expertise. Notable penetration testing vendors that provide services are Core Security, Digital Defense, Immunity, NopSec, Rapid7, and Synack. Core Security, Immunity, and Rapid7 also sell penetration testing products and frameworks for S&R pros to deploy themselves.

Vendor Landscape

The vulnerability management landscape has various solutions and specialized products. Each technology has its own strength in the vulnerability management life cycle. Many vendors provide vulnerability management products and services. When selecting a vendor, prioritize those that help you better operationalize your efforts. Below, Forrester analyzes each of the major vulnerability management players:

- **BeyondTrust.** BeyondTrust, whose roots are in the privileged identity market, burst onto the vulnerability management scene in 2012 with its acquisition of eEye Digital Security. Its Retina Network Security Scanner, in operation since 1999, can scan networks, web applications, virtual and cloud infrastructure, mobile devices, and databases, and it can be purchased as a standalone scanner, a vulnerability management suite, or as a platform that unifies BeyondTrust's vulnerability management and privileged access and identity management solutions. The focus on correlating vulnerability information with privileged access and identity management is a big differentiator.

- **Core Security.** Core Security is best known for its flagship commercial penetration testing solution, Core Impact. Core built on that expertise (the firm also provides penetration testing services) with Core Insight. Core Insight consolidates and prioritizes vulnerabilities from scans

and correlates them with known exploits and network topology that allows users to track attack paths to critical business assets. This enables users to identify and focus remediation efforts on vulnerabilities that pose the most significant risk to the organization.

- **Digital Defense (DDI).** Digital Defense, based in San Antonio, developed its patented scanning and proprietary network endpoint correlation technology for use in its managed service and on-demand SaaS scanning. DDI's main market is managed services, supporting small and medium-size organizations as well as large enterprises. Its vulnerability management platform, Frontline Vulnerability Manager, focuses on ease of use and good end user experience for S&R pros. Additionally, DDI offers penetration testing services and security training.

- **Immunity.** Headquartered in Miami, Immunity is a boutique security company that specializes in offensive security and penetration testing — it offers both products and commercial consulting. Immunity has a range of tools for penetration testers, including wireless penetration testing and exploit writing and analysis tools, plus the Canvas penetration testing framework. Immunity also sells Innuendo, an advanced penetration testing tool that models the capabilities of advanced adversaries.

- **NopSec.** Recent startup entrant NopSec offers cloud-based vulnerability management with a specific focus on remediation planning. Its scanner-agnostic SaaS product, Unified VRM, correlates vulnerability data with malware, exploit, social, and other feeds as well as an organization's IT environment, and allows S&R pros to prioritize vulnerabilities with insight based on business risk and context. Unified VRM offers automated workflow capabilities, including social collaboration and knowledge-sharing features, to ease remediation across organizational barriers. NopSec also offers penetration testing services.

- **Positive Technologies.** Positive Technologies started out in 2002 with its vulnerability scanner. It currently offers vulnerability and compliance management, as well as application security and critical infrastructure protection. Positive Technologies' main market is currently Europe and Asia, but it has started to expand in North America. Positive Technologies also offers application security capabilities through its Application Firewall and Application Inspector. Its MaxPatrol vulnerability management solution features protection for SAP and critical infrastructure including industrial control systems (ICS).

- **Qualys.** Qualys is a pioneer in SaaS-based vulnerability management and delivers additional security controls via the cloud. Qualys offers continuous perimeter scanning, policy compliance scanning, and web application security. Its web application security capabilities feature web app scanning, web application firewall, and malware detection. Qualys's cloud platform allows customers to engage in on-demand or continuous scans without the need for infrastructure investment. For S&R pros who need to keep data on-premises, Qualys offers a private cloud instance with remote management.

- **Rapid7.** Rapid7 is focused on security data and analytics solutions and services; its primary product portfolio includes Nexpose for vulnerability management and Metasploit for penetration testing. The Threat Exposure Management solution integrates Nexpose with Metasploit to provide the capability to simulate attacks and prioritize risk based on exploitability within the organization's environment. Rapid7 has also released UserInsight to provide incident detection and response leveraging its intruder analytics. Rapid7 offers professional services for security program development, maturity assessments, incident response, and penetration testing. The company received an additional $30 million in funding from Bain Capital and Technology Crossover Ventures in December 2014 to fund accelerated growth. [31]

- **RedSeal.** RedSeal offers an analytics platform that uses configuration data from network devices and vulnerability scan results to identify and prioritize risks stemming from access paths to vulnerable critical systems. The company creates a visual model of an organization's network and uses this to provide context around how an intruder would be able to move around your environment. RedSeal helps S&R pros understand network exposure and asset value to direct remediation efforts to the most meaningful vulnerabilities.

- **Secunia.** Headquartered in Copenhagen, Secunia has been in business since 2002 and focuses on operationalizing remediation and supporting the entire software vulnerability management life cycle. Its solution portfolio includes its Corporate Software Inspector (CSI) for patch and vulnerability management and its lightweight Vulnerability Intelligence Manager (VIM). Secunia also offers free tools for consumer vulnerability management for PCs and Android. Its patch management product integrates with both Microsoft WSUS/System Center 2012 and Altiris for third-party patch deployment.

- **Synack.** Synack, whose cofounders supported intelligence operations at the National Security Agency (NSA), uncovers security vulnerabilities for its clients through a crowdsourced bug bounty program using its own vetted team of white-hat hackers. Delivering its services through its cloud infrastructure, Synack can engage in continual testing of customer environments. The firm recently received $25 million in its latest Series B funding.

- **Tenable Network Security.** Tenable's Nessus vulnerability scanner has been in operation since 2002. Tenable's product portfolio includes solutions for continuous monitoring, vulnerability management, and vulnerability scanning. The Nessus vulnerability scanner is widely deployed either standalone or as part of its vulnerability management solution — on-premises or in the cloud. Tenable also offers a passive scanner as part of its continuous monitoring solution, ideal for real-time visibility into vulnerabilities. Tenable brings its breadth of capabilities together in its SecurityCenter CV product for continuous monitoring, pulling in additional information such as malware detection, configuration audit, network behavior analysis, and log data for analytics and reporting.

- **Tripwire.** Tripwire entered the vulnerability management market with its purchase of nCircle in 2013. Leveraging its position as a provider of file integrity monitoring, security configuration management, and log management, Tripwire's security portfolio focuses on detecting and responding to indicators of compromise and vulnerabilities. Its vulnerability management solution, Tripwire IP360, features network discovery and profiling and web application scanning. Tripwire continues to build integrated capabilities between its vulnerability management and configuration management products. In January 2015, end-to-end single transmission solution provider Belden acquired Tripwire.[32]

RECOMMENDATIONS

CONCENTRATE ON REMEDIATION

S&R pros need to be proactive, cut through the noise, and extract meaningful information that will protect their companies. Remember: Ruthless prioritization coupled with strong, simple, and standardized tools and processes gives you the key to timely remediation.

- **Look at managed services.** Managed services can lift the burden off of security operations, so S&R pros can dedicate efforts to identifying high-risk vulnerabilities and how to fix them. The more security functions a CISO stacks with a managed security service provider (MSSP), the better the economies of scale.[33] If your firm already uses managed services for IT operations, ask your MSSP to take on vulnerability management also.

- **Adopt continuous monitoring that includes detection and response.** You need real-time visibility into vulnerabilities of your most critical assets. Continuous monitoring of high-impact systems and assets should be the norm. Remember that monitoring isn't enough; you must be able to detect and respond to attacks against these assets.

- **Know your data.** Not all data are created equal. Protecting toxic data (personal cardholder information, personal health information, personally identifiable information, and intellectual property) are paramount.[34] Better inform prioritization of remediation by implementing data classification and discovery. This will help you understand where the most important data resides and how it is used.

- **Know your adversary.** Threat intelligence can also help you identify the areas where you need the most attention. With adversary intelligence, such as the details of the motivations, intent, and capabilities of internal and external threat actors, cybersecurity strategies become targeted and aware.[35]

SUPPLEMENTAL MATERIAL

Survey Methodology

Forrester conducted a mixed methodology phone and online survey, fielded in April and May 2014, of 3,305 business and technology decision-makers located in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Each calendar year, Forrester's Business Technographics fields business-to-business technology studies in 10 countries spanning North America, Latin America, Europe, and Asia Pacific. For quality control, we carefully screen respondents according to job title and function. Forrester's Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Additionally, we set quotas for company size (number of employees) and industry as a means of controlling the data distribution and establishing alignment with IT spend calculated by Forrester analysts. Business Technographics uses only superior data sources and advanced data-cleaning techniques to ensure the highest data quality.

Forrester conducted an online survey fielded in January 2015 of 7,238 information workers located in Australia, New Zealand, Brazil, Canada, China, France, Germany, India, the UK, and US from companies with two or more employees.

Each calendar year, Forrester's Business Technographics fields business-to-business technology studies in 10 countries spanning North America, Latin America, Europe, and Asia Pacific. For quality control, we carefully screen respondents according to job title and function. Forrester's Business Technographics ensures that the final survey population contains only those employed adults who use a computing device at least 1 hour per day as part of their job. Additionally, we set quotas for age, gender, and job function as a means of controlling the data distribution. Business Technographics uses only superior data sources and advanced data-cleaning techniques to ensure the highest data quality.

Companies Interviewed For This Report

Archer

BeyondTrust

BMC

Core Security

Digital Defense (DDI)

Immunity

LogicManager

Modulo

NopSec

Positive Technologies

Qualys

Rapid7

RedSeal

Rsam

Secunia

ServiceNow

Synack

Tenable Network Security

Tripwire

ENDNOTES

[1] Source: Forrester's Business Technographics Global Security Survey, 2014.

[2] Source: "2015 Data Breach Investigations Report," Verizon, 2015 (http://www.verizonenterprise.com/DBIR/2015/).

[3] Source: Paula Rosenblum, "Lessons From Home Depot: Expect Hackers To Crack More Retailers This Holiday Season," Forbes, November 6, 2014 (http://www.forbes.com/sites/paularosenblum/2014/11/06/lessons-from-home-depot-expect-hackers-to-crack-more-retailers-this-holiday-season/).

[4] Heartbleed is a bug found in the OpenSSL cryptographic software library that allows attackers to compromise communication and read the memory of systems under vulnerable versions of OpenSSL protection. Source: The Heartbleed Bug (http://heartbleed.com/).

Shellshock affects the Unix Bash shell that allows attackers to remotely execute commands without authentication. Security reports identified attackers exploiting compromised machines as botnets for distributed denial-of-service (DDoS) attacks and vulnerability scanning. Source: Andy Greenberg, "Hackers Are Already Using the Shellshock Bug to Launch Botnet Attacks," Wired, September 25, 2014 (http://www.wired.com/2014/09/hackers-already-using-shellshock-bug-create-botnets-ddos-attacks/).

The POODLE bug, which stands for Padding Oracle On Downgraded Legacy Encryption, exploits the fallback on SSL 3.0 from TLS implementations, which enables attackers to break the encryption of traffic. Source: United States Computer Emergency Readiness Team (US-CERT) (https://www.us-cert.gov/ncas/alerts/TA14-290A).

[5] Source: Jim Finkle and Supriya Kurane, "U.S. hospital breach biggest yet to exploit Heartbleed bug: expert," Reuters, August 20, 2014 (http://www.reuters.com/article/2014/08/20/us-community-health-cybersecurity-idUSKBN0GK0H420140820).

[6] Source: Luca Allodi and Fabio Massacci, "How CVSS is DOSsing your patching policy (and wasting your money)," Department of Information Engineering and Computer Science (http://disi.unitn.it/~allodi/allodi-massacci-BHUSA13-handout.pdf).

[7] For more information on patch management, see the "Introducing Forrester's Prioritized Patching Process (P3)" Forrester report.

[8] For more information, see the "Introducing Forrester's Prioritized Patching Process (P3)" Forrester report.

[9] Digital businesses cannot succeed in today's competitive environment if they don't protect their customers from cybercriminals and fraudsters, safeguard their firm's intellectual property from espionage, and ensure the continuity of business operations in the face of market shifts and other risks. To do this, S&R leaders must refocus their priorities and technology investments in support of their firm's business technology (BT). See the "Top Security And Risk Priorities For The Business Technology Agenda" Forrester report.

[10] NIST Special Publication 800-137 defines continuous monitoring as "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions." Source: "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," National Institute of Standards and Technology (NIST), September 2011 (http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf).

[11] For more information, see the "Equipped To Thrive: Help Employees Turn Mobile Moments Into Customer Value" Forrester report.

[12] For more information, see the "Re-Engineer Your Business For Mobile Moments" Forrester report.

[13] For more information, see the "Secure And Protect Mobile Moments" Forrester report.

[14] For more information, see the "The Future Of Mobile Security: Securing The Mobile Moment" Forrester report.

[15] Source: Forrester's Global Business Technographics Telecommunications And Mobility Workforce Survey, 2015.

[16] For more information, see the "Habitat For Engagement: Unleash Workforce Potential With Agile Enablement" Forrester report.

[17] Source: Christian Florian, "Most vulnerable operating systems and applications in 2014," GFI Blog, February 18, 2015 (http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/).

[18] Source: Tod Beardsley, "Google No Longer Provides Patches for WebView Jelly Bean and Prior," Security Street Rapid7, January 12, 2015 (https://community.rapid7.com/community/metasploit/blog/2015/01/11/google-no-longer-provides-patches-for-webview-jelly-bean-and-prior).

[19] Source: Forrester Research World Mobile And Smartphone Adoption Forecast, 2014 To 2019 (Global).

Source: Emil Protalinski, "Android Lollipop hits 3.3% adoption, KitKat passes 40%, and Jelly Bean continues to slide," VentureBeat, March 2, 2015 (http://venturebeat.com/2015/03/02/android-lollipop-hits-3-3-adoption-kitkat-passes-40-and-jelly-bean-continues-to-slide/).

[20] For more information, see the "Justify Your Hybrid Cloud Future With A Solid Business Case" Forrester report.

[21] In hyperjacking, an attacker installs a rogue hypervisor that is able to take control of a server. Source: Dimitri McKay, "A Deep Dive Into Hyperjacking," SecurityWeek, February 3, 2011 (http://www.securityweek.com/deep-dive-hyperjacking).

Hypervisor escape involves a guest obtaining access to the host hypervisor. Source: C. Meier and M. Novellino, "Virtualization vulnerabilities related to hypervisors," MIT Geospatial Data Center, October 26, 2013 (http://cybersecurity.mit.edu/2013/10/virtualization-vulnerabilities-related-to-hypervisors/).

[22] Source: "VMware Security Advisories," VMware (http://www.vmware.com/security/advisories).

[23] Source: "Internet of Things Research Study," HP, 2014 (http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en).

[24] Source: Brian Krebs, "Target Hackers Broke in Via HVAC Company," Krebs on Security, February 5, 2014 (http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/).

[25] Source: "Rapid7 Acquires Metasploit," Business Wire press release, October 21, 2009 (http://www.businesswire.com/news/home/20091021005675/en/Rapid7-Acquires-Metasploit#.VPTDAfmjOSo).

[26] Source: "BeyondTrust Acquires Vulnerability Management Pioneer eEye Digital Security," BeyondTrust press release, May 9, 2012 (http://www.beyondtrust.com/NewsEvents/PressReleasesDetails/201/).

[27] Source: "Tripwire, Inc. Acquires nCircle," Tripwire press release, March 11, 2013 (http://www.tripwire.com/company/news/press-release/tripwire-inc-acquires-ncircle/).

[28] An integrated portfolio that enables orchestration is the fourth need in Forrester's targeted attack hierarchy of needs. See the "Forrester's Targeted-Attack Hierarchy Of Needs: Assess Your Core Capabilities" Forrester report.

[29] For more information on predictive threat modeling, see the "TechRadar™: Zero Trust Network Threat Mitigation Technology, Q1 2015" Forrester report.

[30] Source: "BMC and Qualys Join Forces to Improve Enterprise Security," Qualys press release, February 25, 2015 (https://www.qualys.com/company/newsroom/news-releases/usa/2015-02-25-bmc-qualys-join-forces-improve-enterprise-security/).

[31] Source: "Rapid7 Receives $30 Million Investment to Accelerate Growth and Strong Traction of New Security Data Analytics and Strategic Services Offerings," Rapid7 press release, December 17, 2014 (http://www.rapid7.com/company/news/press-releases/2014/rapid7-receives-30million-investment.jsp).

[32] Source: "Belden to Acquire Tripwire, a Leader in Cybersecurity, for $710 Million," Tripwire press release, December 9, 2014 (http://www.tripwire.com/company/news/press-release/belden-to-acquire-tripwire-a-leader-in-cybersecurity-for-710-million/).

[33] For more information, see the "The Forrester Wave™: Managed Security Services: North America, Q4 2014" Forrester report.

[34] For more information, see the "Rethinking Data Discovery And Data Classification" Forrester report.

[35] For more information, see the "Use Actionable Threat Intelligence To Protect Your Digital Business" Forrester report.

FORRESTER®

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.