Vendor Landscape: Vulnerability Management, 2017

Software Vulnerabilities Are The Leading Means Of External Attacks — It's Time To Do Something About It

by Josh Zelonis
April 21, 2017

Why Read This Report

Breaches can undermine customer trust, endanger revenue growth and profits, and permanently tarnish reputations. According to our data, software vulnerabilities are the single largest factor in enterprise breaches. Identifying vulnerable systems on your network and applying patches is clearly not a rote process at enterprise scale. This report provides security and risk (S&R) pros an overview of the vulnerability management vendor landscape and information on trends that directly affect and enable business operations.

Key Takeaways

**Vulnerability Management Solutions Are Embracing A Risk-Based Approach**

Security teams have struggled with managing vulnerability reports and communicating critical patch mitigations that need to be applied. New vendors to the vulnerability management space are forgoing scanning technologies in favor of providing a central interface for managing the output of your tools, while enriching this data with threat intelligence and asset information to provide you a holistic view of risk.

**Containers Are Changing Everything**

Traditionally, security teams have used vulnerability management solutions in production environments and as a discussion tool between operations and security teams. Containers offer a tectonic shift to this dynamic, as developers now are responsible for specifying the runtime environments where their applications will live, at build definition, allowing security to integrate very early in the development life cycle.
Vendor Landscape: Vulnerability Management, 2017

Software Vulnerabilities Are The Leading Means Of External Attacks — It’s Time To Do Something About It

by Josh Zelonis
with Stephanie Balaouras, Bill Barringham, and Peggy Dostie
April 21, 2017

Table Of Contents

2  Vulnerability Management Remains A Critical Challenge
   A Brief History Of Vulnerability Management

5  Vulnerability Management Isn’t Just Scanners Anymore
   Veteran Vulnerability Management Players Average Over 15 Years’ Experience
   Risk-Management Vendors Are Centralizing Vulnerability Data And Decision Making

Recommendations

10  Vulnerability Management Tools Are Evolving; Evolve With Them

What It Means

10  Expect More Acquisitions In The Container Security Space

11  Supplemental Material

Related Research Documents

Secure Applications At The Speed Of DevOps
Ten Basic Steps To Secure Software Containers
Top Cybersecurity Threats In 2017
Vendor Landscape: Incident Response Service Providers
Vulnerability Management Remains A Critical Challenge

The vulnerability management market has been constantly evolving for the past 25 years and will continue to experience growth and innovation through necessity. According to Forrester Data Global Business Technographics® Security Survey, 2016, software vulnerabilities are the leading method of external intrusion in a breach (see Figure 1). To help S&R pros better prioritize threats and harden their infrastructure against known vulnerabilities, we surveyed 15 vendors to understand their key capabilities, differentiation, and future direction.

**FIGURE 1** Top External Intrusion Methods

<table>
<thead>
<tr>
<th>Top external intrusion method (Multiple responses accepted)</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software vulnerability (software exploit)</td>
<td>42%</td>
</tr>
<tr>
<td>User interaction (phishing, malicious link, or email attachment)</td>
<td>37%</td>
</tr>
<tr>
<td>Use of stolen credentials (logins, encryption keys)</td>
<td>36%</td>
</tr>
<tr>
<td>Web application (SQL injection, cross-site scripting, remote file inclusion)</td>
<td>34%</td>
</tr>
<tr>
<td>DDoS</td>
<td>25%</td>
</tr>
<tr>
<td>Strategic web compromise (watering hole attack)</td>
<td>24%</td>
</tr>
<tr>
<td>DNS</td>
<td>22%</td>
</tr>
<tr>
<td>Mobile malware</td>
<td>19%</td>
</tr>
<tr>
<td>Exploitation of lost/stolen asset</td>
<td>13%</td>
</tr>
</tbody>
</table>

Base: 346 global network security decision makers whose firms have had an external security breach in the past 12 months
A Brief History Of Vulnerability Management

Vulnerability management has changed dramatically over the past 20-plus years, and the 15 vendors we surveyed in this landscape represent the maturation of a market that has evolved with the needs and requirements of security teams. To understand how the vendors in this market have evolved and to properly evaluate the solutions we’ve profiled in this report, it helps to put a historical context to the features behind them (see Figure 2):

› Automated vulnerability assessment tools were initially feared. The Morris Worm is frequently credited as being the first vulnerability scanner, as it incorporated four methods of attack to gain access to a system, including software exploits and weak password checks; however, it was not designed as a security tool. Early pioneers in the vulnerability management space such as Dan Farmer, intrigued by the Morris Worm, began developing automated vulnerability assessment tools, combining remote checks for common security flaws and reporting the details to the end user. Unfortunately, the duality of a tool that would identify security vulnerabilities in computer systems and bear such names as Security Administrator Tool for Analyzing Networks (SATAN) led to condemnation by some, including the US Department of Justice.

› Productized offerings appeared in the market in the mid-1990s. In the mid-1990s and through the early 2000s, vulnerability management vendors and technology management professionals began to see vulnerability management as a commercially viable and even necessary process. Security was brand new, few organizations had dedicated security teams, and operations teams were desperately trying to get a handle on how malicious external hackers could penetrate their network. This also overlapped with the “cowboy era” of penetration testing where you could pay teenagers and 20-somethings to demonstrate they could find a way into your network — and hackers were as likely to be hired as prosecuted. This was a tumultuous time in security, and while many products didn’t make it (have you ever heard of CyberCop?), those that did are still around and appear in this landscape.

› The introduction of authenticated scanning dramatically improved accuracy of scans. Two significant advancements in vulnerability management came at the tail end of the 1990s when authenticated scanning became available. By allowing administrators to monitor all installed software on a system instead of just fingerprinting exposed network services, vendors were able to greatly increase the accuracy of security scans. Consequently, this provided much-needed endpoint visibility at a time when threat actors were leveraging ActiveX controls to automatically execute code out of your inbox. Twenty years later, the endpoint is still a battleground, but with culprits like Java and Flash instead of ActiveX.

› Application scanning emerged to identify critical app vulnerabilities. As enterprises began to mature and responsibly apply vendor patches, the threat landscape shifted toward application security. Early forays into the space focused on misconfiguration and CGI abuses, with full dynamic application security testing (DAST) coming later. These new capabilities allowed security teams to fuzz web applications to identify critical issues such as SQL injection, which allows remote command execution and direct database interaction.
The emergence of containers has necessitated features to support secure DevOps. The emergence of containers is reshaping the traditional paradigm of operations building systems to execute development code; now it’s developers who specify and build the entire runtime environment their applications should execute in. This shift will have a wide-ranging impact on vulnerability management in the enterprise, as security must truly become the third leg of the secure DevOps stool.

FIGURE 2 Key Innovations In Vulnerability Management

- 1995
  - Morris Worm scans for vulnerable systems over the network.
  - Dan Farmer develops Computer Oracle and Password System (COPS) vulnerability scanner for Unix systems.
  - Internet Security Systems (ISS) is founded, funding the development and marketing of the first commercial vulnerability scanner.
  - Authenticated scanning is incorporated into vulnerability management scanning tools.
  - Rain Forest Puppy writes Whisker to scan for web server vulnerabilities.
  - Open Web Application Security Project (OWASP) is founded.

- 2000
  - First commercial web application security scanners become available.
  - Vulnerability management tools start integrating web vulnerability scanning through modules such as Nikto and URL fuzzing.

- 2005
  - Application scanning

- 2015
  - Container security
  - Tenable acquires FlawCheck to add container registry scanning capabilities to its vulnerability management offering.
Vulnerability Management Isn’t Just Scanners Anymore

The vulnerability management market has traditionally been dominated by names such as Qualys, Rapid7, and Tenable, but new requirements within enterprise environments have given emerging vendors an opportunity to compete in this market. Today, vulnerability management is dividing into two distinct segments: 1) solutions focused on detecting vulnerabilities and 2) solutions focused on providing a holistic view of vulnerability and configuration management issues. However, both of these segments deliver a set of critical features for enterprise security teams (see Figure 3).

**FIGURE 3 Essential Features Of Today’s Vulnerability Management Solutions**

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application security</td>
<td>In addition to scanning for vulnerabilities in exposed services, this product includes dynamic application security testing (DAST) capabilities to identify common web vulnerabilities such as SQL injection and cross-site scripting.</td>
</tr>
<tr>
<td>Authenticated scanning</td>
<td>This product has the ability to authenticate to systems it is scanning to obtain more granular system and software vulnerability details beyond network-exposed services.</td>
</tr>
<tr>
<td>Endpoint agent</td>
<td>This product incorporates or has an integrated endpoint offering that offers the ability to obtain granular system and software details beyond exposed-network services.</td>
</tr>
<tr>
<td>Configuration auditing</td>
<td>This product performs configuration and compliance checks in addition to identifying vulnerable software.</td>
</tr>
<tr>
<td>Container registries</td>
<td>Registries are the distribution point for container images. These products allow you to perform vulnerability management at the source and predeployment.</td>
</tr>
<tr>
<td>Prioritization based on threat intelligence</td>
<td>This product integrates threat intelligence to help organizations prioritize patching based on exploit trends.</td>
</tr>
<tr>
<td>Prioritization based on business context</td>
<td>The Zero Trust model prioritizes data classification and understanding the data flows within your organization. These products allow you to identify systems as being business critical to prioritize remediation.</td>
</tr>
</tbody>
</table>

**Veteran Vulnerability Management Players Average Over 15 Years' Experience**

Vulnerability management is unique in the security space in that the majority of vendors have been around, figuratively, forever. Many of the names have changed as some of the players have been acquired, and, in some cases, the products themselves have as much name recognition as the brand itself. In this section, we provide key differentiation and critiques of each of the players (see Figure 4):
Software Vulnerabilities Are The Leading Means Of External Attacks — It’s Time To Do Something About It

- **Beyond Security.** Beyond Security has a full-featured scanning capability, and the vendor purports to have a false positive rate of less than 0.01%. It offers cash bounties for reporting false positive results, as well as integrations with third-party exploitation tools, both of which make this offering ideal for independent researchers and penetration testers.

- **BeyondTrust.** BeyondTrust has a dedicated focus on reporting and analytics, even ingesting threat data from next-generation firewalls to provide broader intelligence in prioritizing vulnerability remediation. Its ideal implementation in most environments would include external scanning, internal network scanners, endpoint integrations, and an IT risk-management platform, which, although carrying an operations management burden, offers flexibility into hardened environments.

- **Digital Defense.** Digital Defense heavily focuses on providing vulnerability management-as-a-service in addition to offering its own scanning technology. While it does not incorporate threat intelligence for assisting customers with patch prioritization, it does incorporate client feedback for prioritization of critical systems as well as the availability of exploit code in the wild. This approach makes a lot of sense for the firm, as approximately 40% of its business is related to ethical hacking, which would require access to exploit code.

- **Outpost24.** Outpost24, headquartered in Sweden, offers a comprehensive scanning solution focused on reduced false positive rates, data sovereignty, and risk management integration, which is very relevant given its geographic presence (UK/Ireland, the Nordic countries, and France/Benelux). Its solution can generate alerts based on system or vulnerability criticality when key performance indicators are not being met, enabling users to stay informed based on their needs without having to request this information through system interaction.

- **Qualys.** Qualys is the 800-pound gorilla in the vulnerability management space. Long dedicated to developing its own technologies instead of growing through acquisition, it has an extremely broad platform and came up more frequently than any other vendor in discussions about the competitive landscape. That said, one area it currently does not cover is the ability for customers to scan container registries, although this is currently in Qualys’ production road map.

- **Rapid7.** Rapid7 has two products that feature significantly in the vulnerability management space: Nexpose is a fully featured vulnerability scanner that even leverages the Dynamic Host Configuration Protocol (DHCP) to identify transient assets as they join the network, and Metasploit, a ubiquitous exploitation framework that many vendors in this space choose to partner with to achieve exploit capabilities. Rapid7 is also well known for its digital forensics consulting capabilities, although, surprisingly, it does not factor any of the reactive intelligence gathered from these investigations into helping customers prioritize patching based on threat actor trends.
Software Vulnerabilities Are The Leading Means Of External Attacks — It’s Time To Do Something About It

› SAINT. SAINT offers an excellent, full-featured vulnerability management solution for a fraction of the per-asset cost of many of the competitors in this space — making the company particularly appealing to small businesses as well as managed security service providers. SAINT is extremely engineering focused with a small sales staff, which likely explains why it doesn’t garner more attention, although it reports 25% growth year over year.

› Tenable. Tenable has as much brand equity as a company could have with Nessus, yet it strives to be one of the most forward-thinking companies in the vulnerability management space. With its acquisition of FlawCheck in October 2016, Tenable is the first, and so far the only, traditional vulnerability management vendor to add container registry scanning capabilities. Further evidence of innovation is a strategy of divorcing the concept of assets from IP addresses in its licensing, which has proven popular with customers, although it is too early to know if this will translate into actual cost savings.

› Tripwire. Tripwire IP360 uses a distributed architecture to enable speed and scalability while utilizing a dynamic host tracking function to fingerprint devices and correlate results over time. There is a tight integration with Tripwire Enterprise, but it is a little surprising not to see vulnerability management capabilities built into an agent which already includes file integrity monitoring and software configuration management on the endpoint.

› Trustwave. Trustwave is unique compared with other vendors in this space; it was offering application security scanning capabilities before it began offering a traditional vulnerability management scanning solution. That focus shows to this day, as there are obvious gaps such as the inability to perform credentialed scanning of hosts. Primarily a services company, Trustwave offers application and network penetration testing, forensic investigation, and managed security services.
Software Vulnerabilities Are The Leading Means Of External Attacks — It’s Time To Do Something About It

**FIGURE 4** Vulnerability Management Vendors Employing Scanning Technologies

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Application security</th>
<th>Authenticated scanning</th>
<th>Endpoint agent</th>
<th>Configuration auditing</th>
<th>Container registries</th>
<th>Prioritization based on threat intelligence</th>
<th>Prioritization based on business context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beyond Security</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Beyond Trust</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Digital Defense</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Outpost24</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Qualys</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Rapid7</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>SAINT</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Tenable</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Tripwire</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Trustwave</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

**Risk-Management Vendors Are Centralizing Vulnerability Data And Decision Making**

For many organizations, the vulnerability management maturity life cycle begins with Excel spreadsheets and matures to a homegrown solution that is cumbersome and never quite solves their biggest vulnerability management challenges. The following vendors have productized a commercial offering that replaces these struggling homegrown solutions (see Figure 5):

› **Bay Dynamics.** Bay Dynamics offers an integrated view of assets, attack trends, and vulnerability information to prioritize applications and systems based on the financial impact if those systems were compromised. Their product, Risk Fabric, offers a unique approach of putting responsibility for vulnerability remediation on the line of business or application owner instead of it being a negotiation between security and operations.

› **Core Security.** The Vulnerability Insight offering from Core Security is a shift into the vulnerability management market, leveraging its strong red team exploitation toolkit. By consolidating web and network scan data with topology and threat intelligence, it helps customers prioritize vulnerability remediation through threat modelling and attack simulation to validate attack paths.
Software Vulnerabilities Are The Leading Means Of External Attacks — It’s Time To Do Something About It

› **Kenna Security.** Kenna Security markets itself as a security and risk intelligence platform. By centralizing application and network vulnerability scan data with threat intelligence, it provides security and operations with a shared interface from which to prioritize vulnerability remediation and understand risk posture.

› **NetSPI.** As a company providing enterprise security testing services, NetSPI developed a collaboration tool in CorrelatedVM for centrally managing customer assessment data and the workflow through remediation. This platform has experienced a great deal of commercial success over the past two years as an offering to internal assessment teams while not just a penetration testing tool.

› **Skybox.** Skybox offers a security management platform that centralizes vulnerability and configuration management data. Skybox helps customers prioritize remediation and contextually understand risk through attack path visualization using a combination of network modeling and threat intelligence.

**FIGURE 5** Vulnerability Risk Management Vendors

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Application security</th>
<th>Authenticated scanning</th>
<th>Endpoint agent</th>
<th>Configuration auditing</th>
<th>Container registries</th>
<th>Prioritization based on threat intelligence</th>
<th>Prioritization based on business context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bay Dynamics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Core Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kenna Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetSPI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skybox</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Software Vulnerabilities Are The Leading Means Of External Attacks — It’s Time To Do Something About It

Recommendations

Vulnerability Management Tools Are Evolving; Evolve With Them

When software vulnerabilities are the leading attack vector for external breaches, it’s clear that security teams must stop struggling with spreadsheets and homegrown vulnerability management tools. There are commercial offerings to simplify your life by coalescing scanner data, tying in threat intelligence to help you quantify risk, and communicate prioritization to the relevant teams for remediation. As you evaluate solutions, we recommend that you also:

› Seek to integrate vulnerability management earlier in the development cycle. Application security scanning capabilities as well as the emerging container space are providing unprecedented insight into what is going to be deployed in production, sometimes weeks in advance. Harness the opportunity to get involved identifying security issues ahead of time, serving the business by reducing the cost of remediation, which increases dramatically as these issues hit production.

› Realize that exploitation capabilities are overrated. At no point should you send an exploit downstream to find out if your system is vulnerable. Do not sacrifice system stability for a proof of concept. If you’re trying to prove an attack path exists, test your firewall with a port scanner (or telnet for that matter). If you’re not sure if your system or service is vulnerable after scanning, review patch notes or contact the vendor.

What It Means

Expect More Acquisitions In The Container Security Space

Similar to trends we saw starting around 2007 with application security scanners, container registry scanning capabilities are shaping up to become mainstream in the vulnerability management market over the next two years. Tenable has led this charge with the acquisition of FlawCheck, and Qualys is about a year behind with this feature on the development road map for Q3 2017. Expect market pressure from these two huge players to lead to more acquisitions in the space. Two vendors that have added features through acquisition, Rapid7 and Tripwire, would pair nicely with a Twistlock or Aqua Security, who offer the ability to scan Docker container registries. Expect to see them acquire one of these companies in the next 12 to 24 months.
For Security & Risk Professionals

Vendor Landscape: Vulnerability Management, 2017

Software Vulnerabilities Are The Leading Means Of External Attacks — It’s Time To Do Something About It

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester’s research apps for iPhone® and iPad®

Stay ahead of your competition no matter where you are.

Supplemental Material

Survey Methodology

Forrester Data Global Business Technographics Security Survey, 2016, was fielded in March to May 2016. This online survey included 3,588 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

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. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.
Software Vulnerabilities Are The Leading Means Of External Attacks — It's Time To Do Something About It

Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Bay Dynamics
Beyond Security
BeyondTrust
Core Security
Digital Defense
Kenna Security
NetSPI
Outpost24
Qualys
Rapid7
SAINT
Skybox
Tenable
Tripwire
Trustwave

Endnotes

1 See the Forrester report “Top Cybersecurity Threats In 2017.”


7 See the Forrester report “The State Of Application Security: 2016 And Beyond.”

8 See the Forrester report “Brief: Why Docker Is All The Rage.”

9 See the Forrester report “Secure Applications At The Speed Of DevOps.”
We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES
› Core research and tools
› Data and analytics
› Peer collaboration
› Analyst engagement
› Consulting
› Events

Forrester’s research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE
Marketing & Strategy Professionals
CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals
CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
› Security & Risk
Sourcing & Vendor Management

Technology Industry Professionals
Analyst Relations

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.