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
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).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.

**Vulnerability Management Remains A Critical Challenge**

<table>
<thead>
<tr>
<th>Top External Intrusion Methods</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

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

You have reached the end of this report extract. To continue reading and/or download the entire document, please complete the form in this LookBook or click here.