ESG SHOWCASE

Closing the Gap Between Vulnerability Discovery and Remediation

Date: April 2021 **Author:** Dave Gruber, Senior ESG Analyst

ABSTRACT: While efficient patch management is considered one of the basic tenets of vulnerability management, it is not necessarily a clearly defined practice. While security teams are typically responsible for identifying and prioritizing vulnerabilities, IT teams are often tasked with mitigating the issues. When security and IT priorities are not in sync, too much time is wasted on vulnerabilities that pose little or no risk to the business, resulting in security breaches and wasted resources. Here are some suggestions for how you can bridge the gap, reduce critical vulnerabilities based on business context, and properly focus IT resources to save time and money at the same time.

Overview

Vulnerability detection and patching every asset across your entire attack surface is foundational to modern security programs. Automated vulnerability detection and patch management tools are both widely deployed and understood. But while most organizations invest in and utilize these tools regularly, nearly one-third of all detected vulnerabilities remain open after a year, and over one-quarter are never remediated (see Figure 1).[1] As many as 60% of organizations said that at least one recent data breach occurred because a patch was available for a known vulnerability but was not applied.[2]

So where is the gap?

Figure 1. Despite Use of Vulnerability Assessment and Patching Tools, Vulnerabilities Persist

Source: Tenable

[1] Source: Tenable Research, *Persistent Vulnerabilities, Their Causes and the Path Forward*, June 2020.
[2] Source: Ponemon Institute LLC, *Costs and Consequences of Gaps in Vulnerability Response*, October 2019.

This ESG Showcase was commissioned by HCL and is distributed under license from ESG.
© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The issue begins with common operational silos of detection vs remediation, which result in misaligned goals and limited communication between security and IT Operations teams. While security teams are focused on blocking, identifying, and mitigating threats, IT Operations teams, who typically own responsibility for patching[3], are busy focusing on business agility, continuity, and operations. In support of their respective objectives, many teams employ separate, specialized tools for vulnerability management, as well as patch and security configuration management, causing teams to operate independently and out of sync.

Vulnerability management platforms are remarkably effective at identifying vulnerable software and recommending specific patches to mitigate vulnerabilities. However, few IT teams follow the recommended patches as stated. First, there is often an overwhelming number of recommended patches across the entire attack surface, making it nearly impossible to fix every risk that is posed. This drives the need to prioritize and remediate critical issues that matter the most. In an effort to minimize downtime and performance impact, IT teams often further aggregate patches, together with the deployment of net-new software, existing software feature updates, and configuration updates, into broader updates that can be more easily deployed and tracked. However, this process requires an arduous, manual analysis process for most organizations.

Wasted Resources, Delayed Patching, and Unnecessary Organizational Risk

The misalignment in patch recommendation forces IT and security teams to spend significant amounts of manual effort, wasting resources and delaying vulnerability mitigation.

Here lies the gap. This manual analysis and aggregation process is tedious, error-prone, and time consuming, which leads to delays in remediation. This gap results in wasted time spent by precious security and IT resources as they attempt to reconcile reports from vulnerability detection and remediation tools, ultimately leaving organizations with unnecessary risk associated with delayed remediation of highly vulnerable systems. A new approach is needed.

A Closer Look at the Reconciliation Challenge

Traditional vulnerability management tools both identify issues and recommend patches to mitigate them. However, modern patching programs often roll up multiple fixes, which are prioritized based on actual risk to the organization, into a single patch activity to resolve issues more efficiently. IT teams want both an efficient and an effective process, therefore often preferring to apply consolidated patches instead of the many specific patches recommended by vulnerability detection solutions.

Most IT organizations are also concerned about the potential for patching to disrupt business operations. Depending on the size and complexity of the patch, a patching operation can impact system performance or create service outages. For these reasons, patches are often highly scrutinized to minimize operational impact. Further, because vulnerability detection tools are typically run more frequently, new vulnerabilities and their associated patches are often discovered and released before patches can be applied, further exacerbating the issue.

Reconciling specific vulnerabilities to consolidated patches is arduous and time consuming, making it challenging to ensure vulnerabilities are mitigated in a timely and accurate manner. IT and security teams spend significant amounts of manual effort in this reconciliation process, wasting resources and more importantly, delaying vulnerability mitigation. As a result, it becomes even more critical that security teams prioritize the right patches based on cyber-risk.

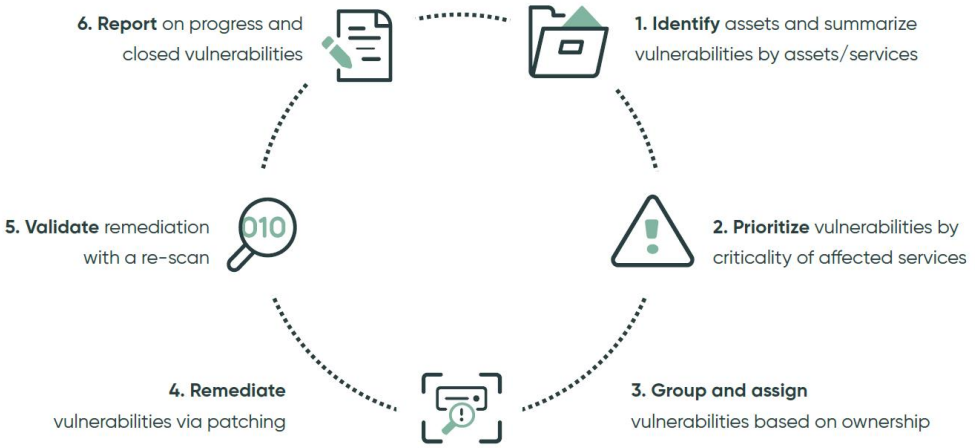
[3] Source: ESG Master Survey Results, *Modern Endpoint Management*, December 2018.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Overcoming the Challenges – What's Needed

Helping IT and security teams close this gap requires systems and product integration between vulnerability management (like Tenable and other leading vulnerability management companies) and patch management solutions[4] (see Figure 2).

Figure 2. 6 Key Components of a Vulnerability Response Platform



Source: Tenable

Organizations should expect software vendors to deliver these integrations, focusing on the following capabilities:

Automated Ingest of Vulnerability Data – Automating the ingest of vulnerability data from popular vulnerability detection and management tools into endpoint management tools is core to the rest of the process. Automation both accelerates and adds consistency to the process, helping to ensure that the vulnerability and remediation data is prioritized based on overall cyber-risk to the organization.

Automated Reconciliation Reports – Mapping detected vulnerabilities with risk and content to their recommended remediations enables teams to identify opportunities for patch cycle compression. Highlighting overlapping or conflicting patches helps teams focus on opportunities to refine remediation strategies.

Updated Workflows – Integrating vulnerability data and workflow inside endpoint management tools brings visibility that will help organizations save time, effort, and resources. When security and IT analysts can monitor and alter recommendations as needed, the process can move to an exception-driven model, speeding patch operations and providing the highest risk-reduction impact.

ESG believes these integration and functional additions to unified endpoint management platforms will help organizations accelerate patching, while reducing wasted reconciliation efforts by both IT and security teams.

[4] ibid.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

HCL BigFix Integrates with Tenable and Other Leading Companies and Automates, Closing the Gap

HCL BigFix lays out an effective approach for CISOs and CIOs trying to synchronize priorities so that patching can be timely and effective. Automation and intelligent patch correlation leverages vulnerability and prioritization data from leading tools like Tenable to improve business context, leading to more efficient, effective patching. Using a more advanced automated system approach, IT and security teams can take multiple patches and apply them concurrently, ensuring they are done in the right order to gain maximum efficiency and effectiveness. Coordinating tasks can result in mitigating the problem faster than a human can respond and ensuring appropriate actions are taken in the correct order, especially when multiple patches are required and must be completed in the proper order for compliance requirements. This integrated solution, like Tenable and BigFix, helps security and IT Operations teams compress the time to patch, reduce errors associated with manual processes, reduce windows of vulnerability, and provide confidence in knowing that proper resources are aligned and being used appropriately.

HCL BigFix has long been recognized as a leading solution in unified endpoint management. As integrations with various vulnerability assessment solutions are added, IT and security teams should further recognize improvements in both operational efficiency and patch delays.

The Bigger Truth

The risk of unpatched systems is well understood. However, even with a long history of investments in vulnerability identification and patch management, most organizations still fail to close vulnerability gaps in a timely way. IT and security teams struggle to work effectively together, utilizing multiple siloed tools that all too often are misaligned. To overcome these challenges, many depend on excessive investment in manual reconciliation processes that are costly and add delays to security vulnerability patching.

Integrating vulnerability assessment solutions with endpoint management tools set the stage for eliminating these challenges, with the potential to offer dramatic improvements in vulnerability mitigation and resource savings.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.