Malwarebytes™ for Business

DATA SHEET

MALWAREBYTES VULNERABILITY AND PATCH MANAGEMENT

Easily Identify and Patch Software Vulnerabilities

Patching—the Struggle is Real

While software vulnerabilities don't induce the pearl-clutching fear that ransomware does, make no mistake: the topic is equally important. If ransomware is the comic villain, then software vulnerabilities are the open doors through which the black hat coolly waltzes in, only to hold your assets hostage (and perform a host of other nefarious activities). One in three (34%) IT professionals from Europe admit their organization was breached as a result of a vulnerability they could have patched.[1] That's got to hurt. But Europe's not alone: at 27%, the global average is only slightly better.[1] That organizations were breached by way of unpatched vulnerabilities is alarming, but the volume of breaches that applied patches could have averted is more alarming still. According to the Ponemon Institute, *60% of breaches* could have been prevented if available patches had been applied.[2] What is going on? The answer is plain: IT and security teams struggle to stay apace of patch releases.

Software vendors constantly release new patches to fix problems, but when patching must be done manually, the time involved leads to gaps in the process. And gaps in the patching process invite software vulnerabilities to hang around like unwelcome guests—who summon villainous friends. In fact, the 2022 Vulnerability Statistics Report found at least one Common Vulnerability or Exposure (CVE) in 51% of scanned systems.[3] Of the discovered CVEs, 57% were two years old and one had been partying since 1999.[3]

CHALLENGE & SOLUTION

VULNERABLE SYSTEMS

- **51%—systems** with at least one software vulnerability[3]
- **57%—vulnerabilities** that are two years old[3]
- **60%—breaches** that could have been prevented with available patches[2]

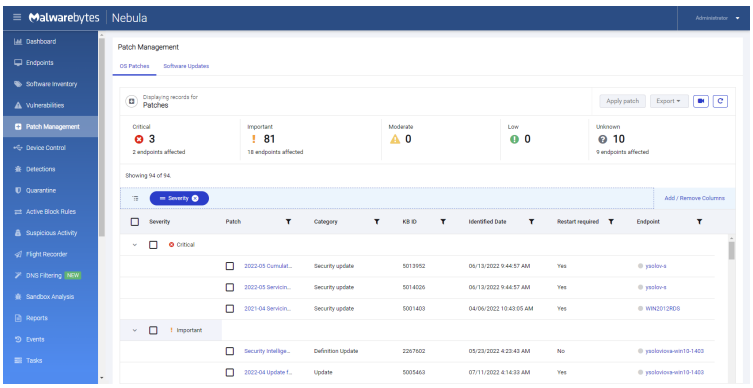
MALWAREBYTES HELPS YOU

- **Understand and quickly neutralize** vulnerability-born risk
- **Insulate applications, devices, and servers** from attacks via software vulnerabilities
- **Identify and resolve long-standing exposures** in 3rd-party legacy and modern apps

Malwarebytes Eases & Accelerates the Patching Process

Malwarebytes can help you address the problems associated with patching software vulnerabilities with two easy-to-add modules for our Nebula cloud platform.

MALWAREBYTES VULNERABILITY ASSESSMENT: Helps you identify, classify and prioritize vulnerabilities in drivers, applications, macOS, and Windows server and desktop operating systems (OSes) by matching the results from its automatic scans against an up-to-date inventory of the software in your IT environment. With this module for Nebula, you can schedule scans that uncover missing updates on, or outdated versions of, your software. You can then use scan results to generate custom reports.



MALWAREBYTES PATCH MANAGEMENT: Designed to automate and accelerate the deployment and verification of software code revisions across OSes and a wide range of third-party legacy and modern applications, including Adobe, Chrome, and cloud storage apps (such as Box). With this add-on module for Nebula, you can schedule patch deployment and create summary reports that may help you comply with governance, data regulation, and cyber insurance requirements.

[1] (June 2019). "2019 Vulnerability Management Survey." Tripwire.
[2] Ponemon Institute. (2019). "Costs and Consequences of Gaps in Vulnerability Response." Sponsored by ServiceNow.
[3] (2022). "2022 Vulnerability Statistics Report." EdgeScan.

Features at a Glance

Our Vulnerability Assessment and Patch Management modules work together seamlessly to extend the capabilities of our Endpoint Detection and Response (EDR), Endpoint Protection (EP), and Incident Response (IR) solutions that run on our Nebula platform. Users manage Vulnerability and Patch Management from the same intuitive cloud-based console they use to manage our business security solutions.

IMPROVED VISIBILITY DECREASES RISK: Our Vulnerability and Patch Management offers improved visibility of software vulnerabilities in your environment.

- Knowing what threats and exposures exist in your environment is an essential first step toward prevention and resilience.
- Better visibility helps ensure that legacy 3rd-party apps—which are too often forgotten—get the same risk assessment as modern apps, so you can address long-standing exposures.

AUTOMATED PRIORITIZATION ACCELERATES ACTION:
Our Vulnerability and Patch Management uses the Common Vulnerability Scoring System (CVSS) to automatically assess the degree of risk associated with detected vulnerabilities. Prioritizing vulnerabilities to address those of highest risk helps protect against breaches, lost time, and unnecessary expense.

- From within the dashboard in our Nebula cloud-based console, users can see at a glance which endpoints are at risk and the projected degree of risk for each: High, Medium, or Low.
- By improving visibility and prioritizing risks, our Vulnerability and Patch Management can help facilitate and accelerate the action users take to prevent cybercriminals from exploiting detected vulnerabilities.

BUSINESS OUTCOMES

- **Reduction in (or elimination of) critical vulnerabilities** in your IT environment
- **Cutback in time between vulnerability detection and exploitation prevention** (whether via patches, updates or configuration changes)
- **Fewer helpdesk tickets** related to vulnerability-induced alerts and infections
- **Elimination of "swivel chair" security management** (with Nebula—one tool to do it all)
- **Means to satisfy boards, comply with regulations, and potentially save on insurance**

BUILT-IN SCHEDULING FREES TIME: By increasing the efficiency of vulnerability assessment and including scheduling capabilities for patch deployment, Malwarebytes Vulnerability and Patch Management helps teams conduct patch-related tasks with increased efficiency, leaving them more bandwidth for other important projects.

REQUEST A TRIAL

To learn more, please contact your account team or your authorized channel partner. You may also contact us to communicate with a local sales expert: **malwarebytes.com/business/contact-us**

www.malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes believes that when people and organizations are free from threats, they are free to thrive. Much more than malware remediations, the company provides cyberprotection, privacy, and prevention to tens of thousands of consumers and organizations every day. for more information, visit https://www.malwarebytes.com.