Malwarebytes™

MALWAREBYTES VULNERABILITY AND PATCH MANAGEMENT

Understand risks quickly and strengthen defenses across your digital ecosystem

OVERVIEW

Even though vulnerability assessment and patch management play an important role in an organization's overall security posture, almost 75 percent of companies large and small say limited resources prevent them from patching fast enough. Despite the risks of malware and ransomware infections, the average time to patch is 102 days.*

Organizations need a streamlined approach with effective and intuitive vulnerability visibility coupled with inclusive patch management.

Customers of our Malwarebytes Business Solutions recognize the value of being able to detect threats and thoroughly remediate infections. The Malwarebytes Vulnerability and Patch Management modules extend these capabilities, enabling your organization to see more deeply into your digital ecosystem to uncover vulnerabilities and swiftly respond to these threats—all from the same platform you use to remediate infections.

CHALLENGES

It takes an average **287 days** to identify and contain a breach.

$4.33M is the average cost of a breach originating from a third-party app vulnerability.

Almost **60 percent** of breaches could've been prevented by installing correct patches.

Intuitive
Intuitive, proactive cyberprotection to easily assess vulnerabilities and prioritize patching.

Effective
Effectively identify and understand risks and efficiently patch across your ecosystem.

Inclusive
Reduce costs and effort with a simplified vulnerability assessment and patch management program.

* IBM: Cost of a Data Breach Report 2021

EFFECTIVE

Malwarebytes Vulnerability and Patch Management modules effectively monitor, prioritize, and remediate vulnerabilities before they can lead to cyberattacks that impact your company's reputation and revenue. Our simplified approach alleviates difficult processes and expedites remediation so you can stay ahead of security risks. You'll gain insights into the severity of vulnerabilities and threats, enabling you to quickly and efficiently prioritize the patches to deploy. This streamlines your efforts to provide the highest level of security protection for your organization.

• Improve critical vulnerability visibility

• Expedite efficient patch management

• Rapidly eliminate vulnerability risks

INTUITIVE

Malwarebytes Vulnerability and Patch Management modules are fast and easy to deploy via a lightweight agent that provides continuous vulnerability discovery, assessment, reporting, and remediation, enabling same-day attention to critical cyber risks.

Our cloud-native Nebula management console is easy-to-use and provides broad visibility across your attack surface, so you can rapidly identify security gaps and eliminate attack vectors.

• Lightweight agent deploys within minutes

• Single, intuitive cloud management console

• Broad visibility across attack surfaces

INCLUSIVE

You gain instant visibility into potential vulnerabilities in your applications and operating systems—all from the same platform you use for your endpoint protection. And when you preview our Patch Management module, you'll see how it can accelerate and scale patch deployment while limiting scarce resource requirements. And it provides a transparent framework to assess risks and simplify patch deployment across dispersed machines. Companies of all sizes will experience improved scalability, a high return on investment (ROI), and lower total cost of ownership (TCO).

• Relieve constrained resources

• Experience a high ROI, low TCO

• Gain a scalable, modular approach

NEBULA SECURITY PLATFORM

When it comes to managing endpoint protection, organizations need a simple solution that relieves constrained IT and security resources by offering visibility into prioritized vulnerabilities and emerging threats. Malwarebytes Vulnerability and Patch Management modules are built on our Malwarebytes Nebula Security Platform, making it easy to manage all your Malwarebytes solutions from a single platform: Malwarebytes Incident Response (IR), Endpoint Protection (EP), and Endpoint Detection and Response (EDR). The Nebula Security Platform provides an intuitive guided user interface; next-generation threat intelligence; multi-layered security, including industry-leading remediation; and easy integration with SIEM, SOAR, and ITSM solutions to simplify detection and response and resolve IT tickets with ease.*

*SIEM: Security Information and Event Management SOAR: Security Orchestration, Automation and Response ITSM: IT Service Management

VULNERABILITY ASSESSMENT MODULE

- Supports most applications, Windows servers and operating systems; Mac OS coming soon

- Scan, identify, assess, and prioritize vulnerabilities by exploitability, severity, age, affected system count, and patch availability

- Visibility into critical vulnerabilities and sorting by severity, vulnerability score, and more

- Vulnerability reports can be generated for task assignment and compliance requirements

- Centralized cloud-native Nebula Security Platform provides an intuitive single pane of glass for all Malwarebytes products

- Single, lightweight agent conserves network resources and avoids performance issues

PATCH MANAGEMENT MODULE (AVAILABLE FOR PREVIEW)

- Accelerates response actions, including patching, software updates, configuration changes, and more

- Customize, orchestrate, and simplify your entire patching process

- Prioritize and deploy patches to Windows, MacOS (coming soon), and third-party applications

- Provides a consistently updated list of available patches

- Enables immediate software updates and simultaneous patch deployments

- Intuitive and guided management console reduces time and effort

- Single, lightweight agent conserves network resources and avoids performance issues

Supported Operating Systems

Windows 8.1 and higher; Windows Server 2012 and higher
MacOS support is coming soon

INDUSTRY-LEADING TECHNOLOGY

Malwarebytes provides innovative capabilities for ransomware detection and remediation, including behavior-based detection and ransomware rollback. We leverage years of security expertise in remediation to provide you with solutions powered by threat intelligence from millions of Malwarebytes-protected endpoints, both business and consumer. The Malwarebytes API makes it easy to integrate our security products with SIEM, SOAR, and ITSM solutions to further drive automation and compatibility. Malwarebytes ensures a high ROI and low TCO, and we're also known for our superior service and support.

YOUR SAFEST CHOICE

Extend your Malwarebytes Endpoint Detection & Response with Vulnerability and Patch Management modules to effectively identify and close security gaps for your organization—all managed from a single, cloud-native platform that does not sacrifice performance or customization.

With Vulnerability and Patch Management, you're able to see deeper into the software ecosystem, exposing more vulnerabilities and threats introduced by third-party applications and out-of-date device drivers or server operating systems. And as gaps are identified, you can take action swiftly to proactively address risks before an attack occurs.

Malwarebytes is your safest and smartest choice. We've won high customer loyalty and praise for enterprise-class security products that are effective, intuitive, and inclusive.

REQUEST A TRIAL

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

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