ThreatDown
Powered by Malwarebytes

Data Sheet

ThreatDown Patch Management

Strengthen your security by addressing vulnerabilities with software and operating system updates.

Overview

While software vulnerabilities do not induce the gut-wrenching fear that ransomware does; make no mistake, they are just as important to address. Software vulnerabilities are the open doors through which attackers easily walk through to conduct reconnaissance, hold assets hostage, and perpetuate attack activities throughout the network and endpoints.

In response, software vendors constantly release new patches to fix problems, but when patching must be done manually, the time involved leads to security gaps in the process. And these gaps allow software vulnerabilities to hang around like unwelcome guests—who bring along unwelcome friends.

ThreatDown Patch Management automates and accelerates the deployment and verification of software code revisions across operating systems and a wide range of third-party applications including: Adobe, Chrome, and cloud storage apps (such as Box). With this capability, IT teams can schedule patch deployment and create summary reports that may help with compliance, governance, data regulation, and cyberinsurance requirements.

Explore the Advantages

Improve Security

- **Reduced risk exposure** via swift implementation of timely software updates to address security gaps identified by ThreatDown Vulnerability Assessment to enhance security posture.
- **Updated patches** consistently available so that IT teams can test quickly and deploy to endpoints
- **Better visibility** helps ensure that legacy 3rd-party apps get the same risk assessment as modern apps, so you can address long-standing exposures.

[1] Cyber Security Report 2021, Check Point.
[2] Ivanti 2021.
[3] 2021 Tuxcare State of Enterprise Vulnerability Detection and Patch Management.

Challenges

- Greater risks – 80% of organizations have suffered an exploit attempt on a known vulnerability[1]
- Too much complexity – 71% say patching is overly complex and time-consuming[2]
- Need for automation – 76% of companies deploy automated patching[3]

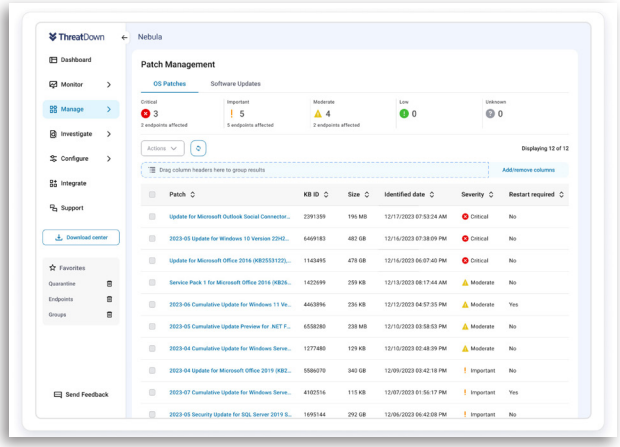
Benefits

Protect endpoints by patching vulnerabilities before they are exploited, all without adding complexity

- Improve Security – Patch identified software vulnerabilities to reduce the risk of a successful cyber attack
- Reduce Complexity – Eliminate time and effort spent on finding and deploying patches to vulnerabilities through automation
- Optimize Performance – Eliminate bugs and enhance the overall stability and performance of your applications

Reduce Complexity

- **Automated patching process**, in combination with ThreatDown Vulnerability Assessment; simplifies workload, prioritizes critical updates and provides visibility with detailed reporting, all from your ThreatDown user console.
- **Patch prioritization** deploys patches, based on degree of risk, to Windows, macOS, and third-party applications.
- **Single cloud console** enables a single pane of glass for the entire ThreatDown portfolio.
- **Single, lightweight agent** powers the entire endpoint security stack and avoids performance issues.



Optimize Performance

- **More reliable endpoint productivity** by deploying software patches to address security vulnerabilities and fix bugs.
- **Faster response times** for patching, software updates, configuration changes and more

Patch Management Service

- Accelerates response actions including patching, software updates, configuration changes and more
- Prioritizes deployment of patches to Windows, macOS, and third-party applications
- Available patches are consistently updated, making it possible to test and safely deploy patches to your endpoints
- Saves your team time and effort spent patching by delegating to our team
- Single, lightweight agent conserves network performance and avoids performance issues

Request for more information

For more information, visit: www.threatdown.com/products/patch-management/

ThreatDown™ Powered by Malwarebytes | www.threatdown.com | corporate-sales@malwarebytes.com | 1.800.520.2796