Malwarebytes

BREACH REMEDIATION

Automated threat removal

Today's incident response personnel are hindered by traditional breach detection systems that produce thousands of alerts a day, but can't fully remove the malware to prevent it from recurring or spreading laterally. This reactive approach requires manual investigative efforts to find the relevant breach, allowing malicious attacks to roam undetected an average of 205 days*. Once malware is discovered on a laptop or server, it can take an IT administrator six hours of their time to reimage each compromised machine.

Malwarebytes Breach Remediation is a next-generation automated Endpoint Detection and Remediation (EDR) platform for small to large enterprise businesses. With Malwarebytes Breach Remediation, organizations can proactively hunt for malware to resolve incidents remotely, rather than physically going to each infected computer to remediate or reimage the machine. It is a self-contained platform that easily integrates with existing enterprise security and management tools. Malwarebytes Breach Remediation provides the unique ability to simultaneously detect and remediate malware—greatly reducing the risk of persistent threats.

Key Benefits

Remediates malware thoroughly

Removes all traces of infections and related artifacts, not just the primary payload or infector. Eliminates risk of new attacks or lateral movements that capitalize on leftover malware traces. Malwarebytes is the industry leader in malware remediation—trusted by millions and proven by AV-Test.org.

Reduces downtime drastically

Enables you to direct efforts toward revenue-positive projects, versus spending countless hours manually resolving malware-related incidents and reimaging hardware across your enterprise.

Works proactively, not reactively

Deploys automated remediation that proactively detects and simultaneously resolves incidents. It's like installing a sprinkler system to stop small fires before they get out of hand. Makes you the hero by enabling you to solve the problem rather than reacting to thousands of security alerts a day.

Hunts for malware

Discovers new and undetected malware and malicious activities and rapidly remediates them. Uses Malwarebytes behavioral rules and heuristics, in addition to indicators of compromise (IOCs) from third-party breach detection tools and repositories.

Enhances existing investments

Integrates easily with existing security information and event management tools (e.g., Splunk, ArcSight, QRadar), Breach Detection Systems (e.g., Lastline, Mandiant, Fidelis), and endpoint management platforms (e.g., Tanium, ForeScout, Microsoft SCCM). You can trigger deployment and remediation through your endpoint management platform based on alerts received from your SIEM and automatically feed resolution details back into your SIEM.

*Gartner Security & Risk Management Summit Presentation, Defending Endpoints From Persistent Attack, Peter Firstbrook, 8-11 June 2015

Malwarebytes

BREACH REMEDIATION

Automated threat removal

Technical Features

- Advanced malware remediation with anti-rootkit scanning
- Intelligent heuristic- and definitions-based scanning engine
- Automated remote malware discovery and remediation
- Custom OpenIOC threat indicators (XML format)
- Four system scan types (Full, Threat, Hyper, Path)
- Optional scan-and-remediate or scan-only modes
- Quarantine management of detected threats
- Event logging to central location (CEF format)
- No lasting footprint on endpoint
- Extensible platform supports flexible deployment options

Tech Specs

Version: 2.6 Windows client

Hardware Requirements:
CPU: 800 MHz or faster
RAM: 256 MB (512 MB or more recommended)
Free disk space: 20 MB
Screen resolution: 800x600 or higher
Active Internet connection, for license validation and threat updates

Languages Available: English

Software Requirements:
Windows 10® (32-bit, 64-bit)
Windows 8.1® (32-bit, 64-bit)
Windows 8® (32-bit, 64-bit)
Windows 7® (32-bit, 64-bit)
Windows Vista® (32-bit, 64-bit)
Windows XP® (Service Pack 2 or later, 32-bit only)
Windows Server 2012®/2012 R2® (32-bit, 64-bit)
Windows Server 2008®/2008 R2® (32-bit, 64-bit)
Windows Server 2003® (32-bit only)
(Excludes Server Core installation option)

About Malwarebytes
Malwarebytes protects consumers and businesses against malicious threats that escape detection by traditional antivirus solutions. Malwarebytes Anti-Malware, the company's flagship product, has a highly advanced heuristic detection engine that removed more than five billion malicious threats from computers worldwide. More than 70,000 SMBs and enterprise businesses worldwide trust Malwarebytes to protect their data. Founded in 2008, the company is headquartered in California with offices in Europe, and a global team of researchers and experts. For more information, please visit us at www.malwarebytes.com.