Malwarebytes

AVR IT Security & Mobility Solutions

DATA SHEET

www.avr.co.uk
01189 344 300

# Malwarebytes Breach Remediation

## Advanced threat removal

### TECHNICAL FEATURES

- Advanced malware remediation with anti-rootkit scanning
- Intelligent heuristic- and definitions-based scanning engine
- Automated remote malware discovery and remediation
- Timeline view of forensic events
- 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
- Dedicated Mac malware and adware scanning engine
- Extensible platform supports flexible deployment options

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 for 205 to 229 days on average*. Once malware is discovered on a laptop or server, it can take an IT administrator six hours of their time to re-image each compromised machine.

Malwarebytes Breach Remediation is a next-generation advanced threat detection and remediation 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 re-image 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 re-imaging hardware across your enterprise.

**Gartner Security & Risk Management Summit Presentation, Defending Endpoints From Persistent Attack, Peter Firstbrook, 8-11 June 2015. Ponemon Institute, 2016 Cost of Data Breach Study, June 2016*

### 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.

### Extracts forensic events

Tracks forensic events using proprietary Forensic Timeliner feature so your team can address security gaps or unsafe user behavior. Gathers system events prior to and during an infection and presents data in a convenient timeline for comprehensive analysis of vector and attack chain. Events covered include file and registry modifications, file execution, and websites visited.

### 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.

### Closes Apple security gap

Removes malware and adware quickly from Mac endpoints. Cleans up OS X systems in less than a minute from start to finish. Separate GUI and command line programs enable flexible deployment using popular Mac management solutions (e.g., Apple Remote Desktop, Casper Suite, Munki). Allows remote, automated operation using shell or AppleScript commands. System administrators and incident responders can collect system information using convenient snapshot command.

## SYSTEM REQUIREMENTS

Please refer to malwarebytes.com/business/breachremediation for complete technical specifications and system requirements.

**Included Components:**

Windows CLI program
Windows Forensic Timeliner program
Mac GUI program
Mac CLI program

**Endpoints**

**Supported Operating Systems:**

Windows 10, 8.1, 8, 7, Vista, XP
Windows Server 2012, 2008, 2003
Mac OS X (10.8 and newer)



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

Malwarebytes protects consumers and businesses against dangerous threats such as malware, ransomware, and exploits 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 10,000 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.