Malwarebytes Breach Remediation
Advanced 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 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.

**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.