Malwarebytes

Malwarebytes Incident Response

The trusted standard in automated endpoint remediation

When a cyberattack occurs, speed is one of the most critical factors in the remediation process. Cyber-prepared security teams should aim to eradicate threats from the environment in under an hour to effectively combat sophisticated cyber threats and avoid the damage a successful breach can inflict on an organization's reputation and bottom line.

Yet, enterprises face increasing complexity and security operations center (SOC) resource drain from manually managing remediation across distributed locations and a dispersed workforce. This creates long response times that expose the enterprise to significant risk.

Investing in a solution that automates endpoint remediation significantly accelerates response times and advances your SOC security practices.

Product overview

Malwarebytes Incident Response (IR) is the trusted standard in automated endpoint remediation that bolsters enterprise cyber resilience by compressing your response times with fast and complete remediation. With our automated approach, Malwarebytes IR drives greater operational efficiency that saves analyst resource time, preserves user productivity, and improves your enterprise security posture.

Our flexible implementation options of either a persistent or non-persistent agent let you deploy according to your endpoint strategy, and the solution's API provides integration opportunities across your security stack to drive further automation and orchestration of your security processes.

With Malwarebytes IR, your enterprise gains effective and thorough endpoint remediation as attacks occur, and our proprietary remediation technology removes dynamic and related artifacts to ensure disinfection.

KEY BENEFITS

Compress response time
Get the trusted standard in automated endpoint remediation that lets you eradicate adversaries with compressed response time and complete remediation.

Drive greater operational efficiency
Advance your SOC practices with a solution that accelerates security operations, saves security analyst resource time, and preserves user productivity.

Deploy the way you want
With the choice of a persistent or non-persistent agent, our flexible options let you deploy according to your endpoint strategy.

Automate orchestration
Our API provides integration opportunities across your security investments to drive further automation and orchestration of your security processes.

Capabilities

Automated endpoint response that compresses response times
Our automated approach enables your security analysts to eliminate manual efforts to remediate attacks, freeing up valuable resource time so your analysts can focus on revenue-generating initiatives. Automated tasks take place in less time with greater accuracy and compress your response time.

Thorough remediation that eradicates the adversary
Most solutions only remediate active malware components—this doesn't provide complete remediation. Malwarebytes Linking Engine applies a propriety approach that also detects and removes dynamic and related artifacts. Our engine applies associated sequencing to ensure disinfection of malware persistence mechanisms.

Persistent or non-persistent agent—deploy the way you want
Malwarebytes provides flexible options to deploy in a way that suits you—choose either a persistent or non-persistent agent on the endpoint. Either approach easily integrates with your deployment tool for a fast roll out that is transparent to the end user.

Cloud-managed simplifies response across dispersed locations
Driven from the cloud, Malwarebytes IR makes it easy to manage response actions across your distributed locations and a dispersed workforce. The solution's centralized dashboards provide a single pane of glass that lets your security analysts quickly understand your attack response footprint and remediation status.

Deep threat intelligence that delivers effective endpoint response
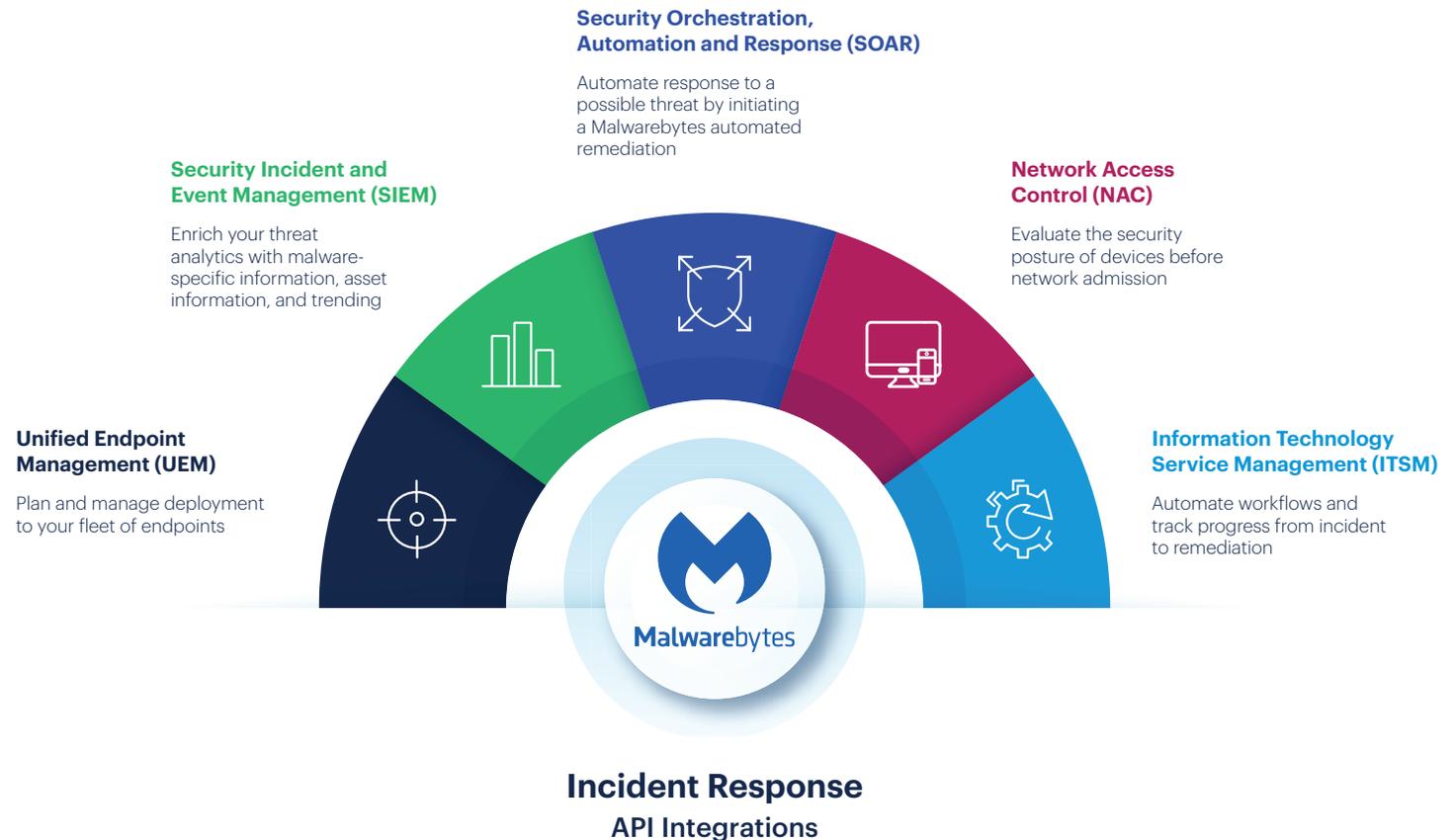Our cyber intelligence expertise in remediation means we have a deep understanding of the attacks that successfully execute on enterprise devices. This provides your enterprise with a solution that is powered by threat detection and remediation intelligence from millions of Malwarebytes protected endpoints, both business and consumer.

Scales to the largest enterprise need
With our cloud solution, you don't need to purchase or manage any equipment, and Malwarebytes IR scales to readily handle your enterprise incident response needs.

Orchestrate automation across your security investments

The Malwarebytes API provides integration opportunities across your security stack, such as your SIEM, SOAR, and ITSM to drive further automation and orchestration of your security processes. This delivers enterprise cyber resilience that is nimble with faster actions that protect and respond to attacks as they occur.

Security Orchestration, Automation and Response (SOAR)

Automate response to a possible threat by initiating a Malwarebytes automated remediation

Security Incident and Event Management (SIEM)

Enrich your threat analytics with malware-specific information, asset information, and trending

Network Access Control (NAC)

Evaluate the security posture of devices before network admission

Unified Endpoint Management (UEM)

Plan and manage deployment to your fleet of endpoints

Information Technology Service Management (ITSM)

Automate workflows and track progress from incident to remediation

Malwarebytes

Incident Response
API Integrations

REQUEST A TRIAL

To request a free trial, visit: www.malwarebytes.com/business/request_trial

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

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.