Malwarebytes

SOLUTION BRIEF

Malwarebytes Incident Response

World's most trusted and thorough remediation

KEY BENEFITS

- Delivers automated, accurate, and thorough remediation
- Bridges operational silos
- Reduces malware dwell time
- Closes gap in personnel and skills shortage
- Reduces cost and complexity of managing incident response

AWARDS

Forbes — America's Most Promising Company

CRN — Product of the Year

V3 — Security Innovation of the Year

The number and types of security events your cyber incident response team (CIRT) faces is steadily increasing, as is the cost and complexity of managing remediation.

In fact, more than 60 percent of attacks take organizations more than nine hours to remediate.[1] Now, more than ever, organizations need to shift from reactive to automated incident response processes in the face of limited resources and constant barrage of advanced threats.

Malwarebytes Incident Response is your trusted solution for accurate and thorough remediation that optimizes your incident response efficiency and effectiveness. Our automated approach helps fortify your security model and bridge operational silos.

Key features

Automated remediation

Our automated remediation enables your CIRT staff to eliminate manual, ad hoc efforts to clean and restore user devices after a malware infection—and it frees up valuable time and resources. Automated tasks take place in less time with greater accuracy and reduce malware dwell time.

Thorough remediation

Most solutions only remediate active malware components—and don't provide complete remediation. Malwarebytes Linking Engine applies a propriety approach that also detects and removes dynamic and related artifacts. And our engine applies associated sequencing to ensure malware persistence mechanisms are removed in such a way that disinfection is permanent. Our advanced remediation methodology provides organizations with expedient malware identification and thorough removal.

Best-informed telemetry

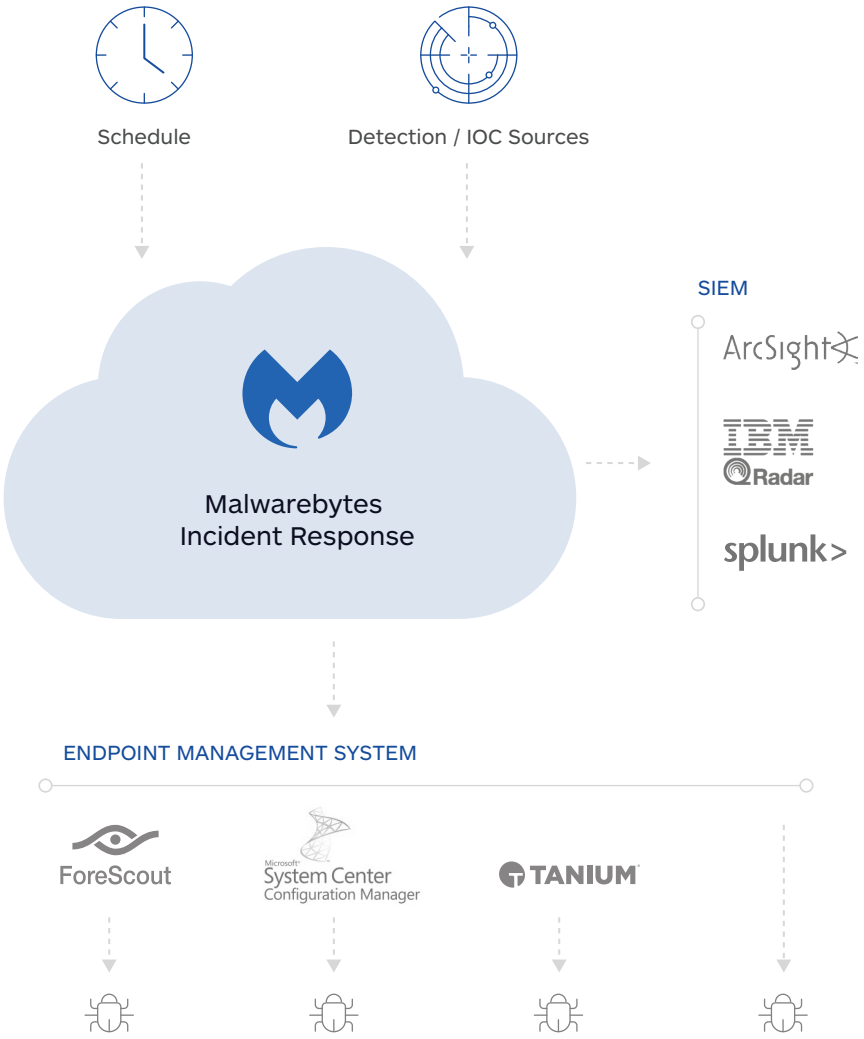
Our threat intelligence expertise in remediation means we understand the "bad stuff"—the attacks that successfully execute on corporate devices. Powered by our big data analytics systems and expert research analysis, we process more than 3 million endpoint remediations each day. This valuable telemetry on zero-day malware makes our technology more responsive to emerging threats, and helps us anticipate tomorrow's malware.

Proactive hunting

It's likely threats already exist in your environment. When an endpoint is successfully infected, attackers often initiate lateral movement to infect other endpoints. Malwarebytes empowers your incident responders to run scheduled scans that proactively hunt for recently reported indicators of compromise (IOCs). Our solution makes it easy to adopt an assume-the-compromise process that greatly improves your security posture.

Flexible deployment & integration-ready

Malwarebytes provides flexible options to deploy the way you want: choose from our persistent cloud-managed endpoint agent or our non-persistent endpoint agent (Breach Remediation). And the non-persistent agent makes it simple to integrate with your existing SIEM and endpoint management system. Our solution can take real-time action on IOCs your SIEM discovers on the network. For example, Malwarebytes can conduct an incident response based on alert from your Splunk or ForeScout solutions.



Website resources

For more information on Malwarebytes Incident Response, go to: malwarebytes.com/business/incidentresponse/
Latest news: blog.malwarebytes.com/
Request a trial: malwarebytes.com/business/licensing

References

[1] *Understanding the Depth of the Global Ransomware Problem*, Osterman Research

Santa Clara, CA | malwarebytes.com | corporate-sales@malwarebytes.com | 1.800.520.2796

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts.