Malwarebytes

INTEGRATION SOLUTION BRIEF

Malwarebytes Integration with ForeScout

Improving real-time visibility and control of network-connected devices while automating threat response

ADVANTAGES

Visibility Into Emerging Threats

- Discover threats and exploit attempts across the enterprise with real-time visibility
- Profile and classify discovered threats based on severity, device, and remediation action
- Continuously sweep the enterprise for threats leveraging expert-curated, zero-hour threat intelligence

Rapid Threat Detection and Remediation

- Allow, deny, or limit network access based on detected threats and remediation response stage
- Assess high-risk endpoints and remediate threats instantly
- Remove unwanted applications and program modifications that lead to latent infection

Automated Threat Response

- Share contextual insights into discovered threats across the enterprise network
- Automate incident response workflows beyond just quarantine actions
- Accelerate system-wide response to quickly mitigate risks and data breaches

Malwarebytes integrates with ForeScout® to help businesses accelerate incident response, stop zero-day exploits, and reduce exposure to emerging threats. The solution provides bi-directional communication between ForeScout CounterACT® and the Malwarebytes agentless, head-less Breach Remediation and next-generation Endpoint Security solutions. Once deployed, the solutions natively deliver enterprise-wide threat sweeping, threat assessment, infection analysis, and automated on-demand incident response functionality using the ForeScout CounterACT console.

IT and business challenges

Limited Endpoint Visibility

Although most organizations have established strong enterprise perimeters and network anomaly detection solutions between their business-critical hosts and the Internet, many of them still lack the visibility to truly know what's happening on each endpoint across the enterprise. Also, these endpoints may have disabled or broken security agents installed that prevent threats from being detected by periodic scans. Relying on these traditional defenses to reduce threat exposure simply isn't enough. Continuously monitoring and proactively sweeping each endpoint on the enterprise network is an effective approach to prevention and early detection of a malicious attack.

Incomplete Threat Detection

Today's cyberthreats are more sophisticated than ever before and can easily evade traditional, legacy security defenses. Multi-vectored, stealthy, and targeted attacks are focused on acquiring sensitive personal information, intellectual property, or insider information. Compromised endpoints and data breaches can often remain undetected for weeks or months despite an attacker needing mere seconds to steal critical data. To detect and remediate advanced threats, zero-day attacks and infected endpoints, businesses need next-generation security technologies which can access each endpoint and actively assess the threat landscape.

Manual Incident Response Workflows

Many businesses have invested in security, event monitoring, and threat correlation tools to manage alerts on potential incidents across the enterprise. Unfortunately, most of these are disparate technologies which are ill-equipped—often unable—to remediate threats on compromised endpoints. Without an automated system to continuously monitor and mitigate endpoint security gaps, valuable time is lost performing these tasks manually. Businesses that lack the ability to quickly and automatically respond to attacks and security breaches are leaving the window open for cyberthreats to propagate within their network and exfiltrate data.

Malwarebytes Breach Remediation and Endpoint Security Integration to ForeScout CounterACT

Malwarebytes integration with ForeScout CounterACT provides businesses with comprehensive and up-to-date information regarding threats on their network. In addition, it offers the ability to automate responses to indicators of compromise (IOCs) while providing a dynamic threat detection approach to security that reduces the network's attack surface.

Using ForeScout CounterACT, administrators can easily and rapidly deploy either Malwarebytes Endpoint Security or Malwarebytes Breach Remediation onto all of their Windows and Mac endpoints. Advanced threats, including known and unknown (zero-day) exploits and ransomware, are automatically detected and removed from those devices. Security teams gain improved threat visibility across their entire enterprise due to shared reporting of discovered and remediated threats from Malwarebytes.

How it Works

1. CounterACT discovers, classifies and assesses endpoint systems the instant they connect to the network.
2. CounterACT silently installs Malwarebytes Endpoint Security or Malwarebytes Breach Remediation onto a host—either on-demand, or through an enacted policy.
3. CounterACT receives real-time health status and detection events from active endpoints across the enterprise with Malwarebytes Endpoint Security installed for use in automated hygiene and incident response policies.
4. If an endpoint has a missing or broken agent, CounterACT can attempt to silently install, repair, or alternatively direct the endpoint's browser to a captive portal where the user receives instructions to perform remediation.
5. Based upon defined security policies, the integrated solution can:
    a. Improve endpoint hygiene
    b. Proactively sweep managed and unmanaged endpoints for threats
    c. Automatically respond to discovered threats by performing thorough endpoint remediation—eliminating the need to wipe and re-image the endpoint.

Malwarebytes Breach Remediation Use Case

1. ForeScout CounterACT silently installs Malwarebytes Breach Remediation onto endpoints

2. Breach Remediation scans, detects, and thoroughly removes threats from compromised endpoint(s)

3. CounterACT receives detection event details and status from Breach Remediation. Breach Remediation is uninstalled automatically (non-persistent agent)

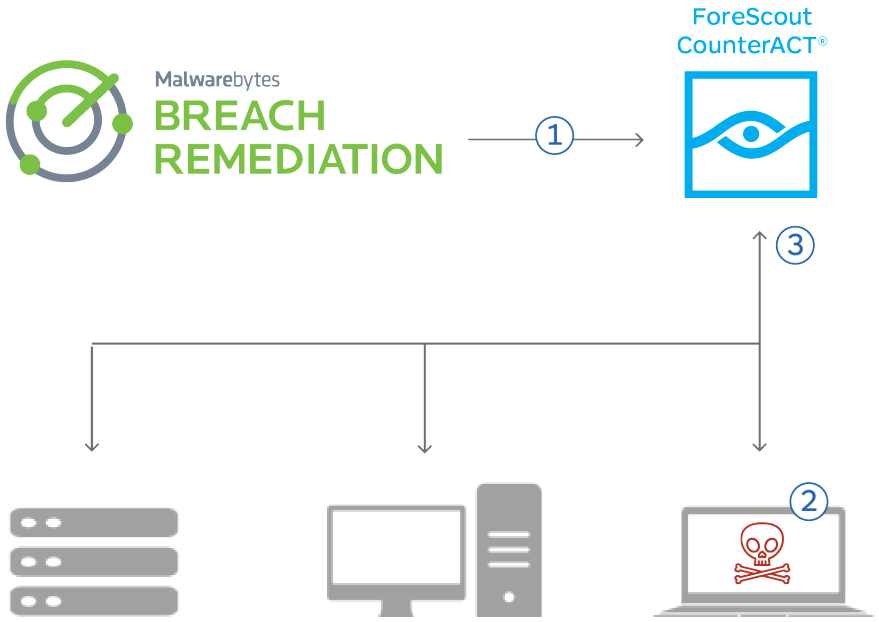


Figure 1. On-demand Malwarebytes scanning and remediation using CounterACT console

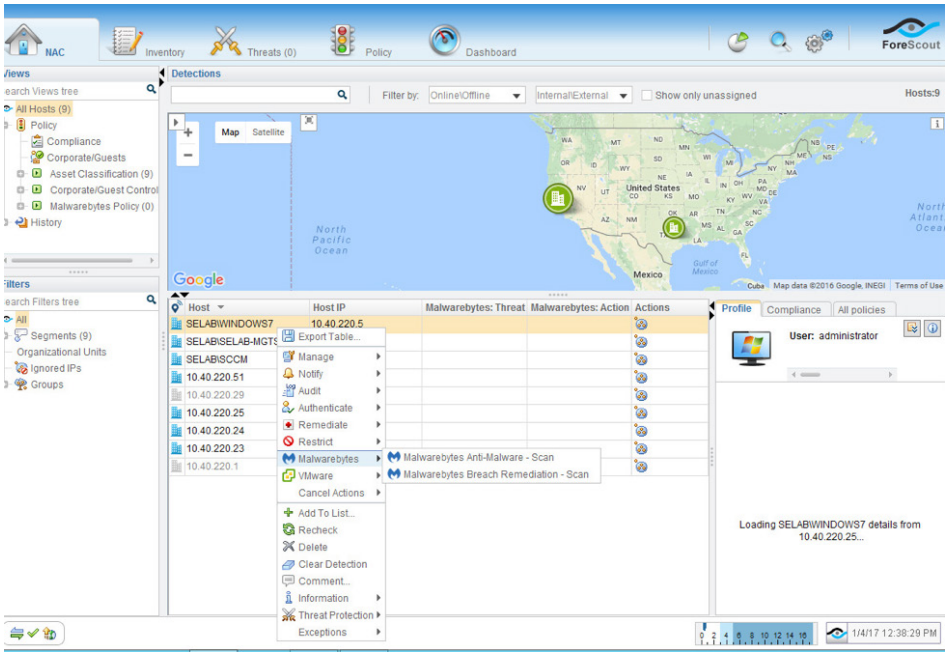


Figure 2. Status of Malwarebytes scan and protection actions within CounterACT console

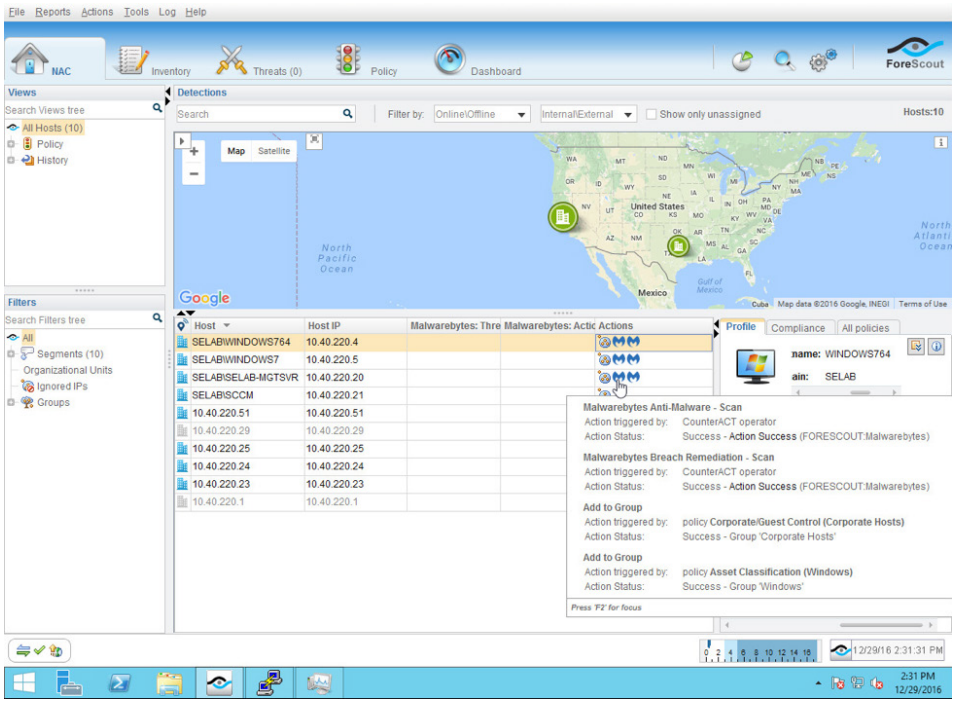
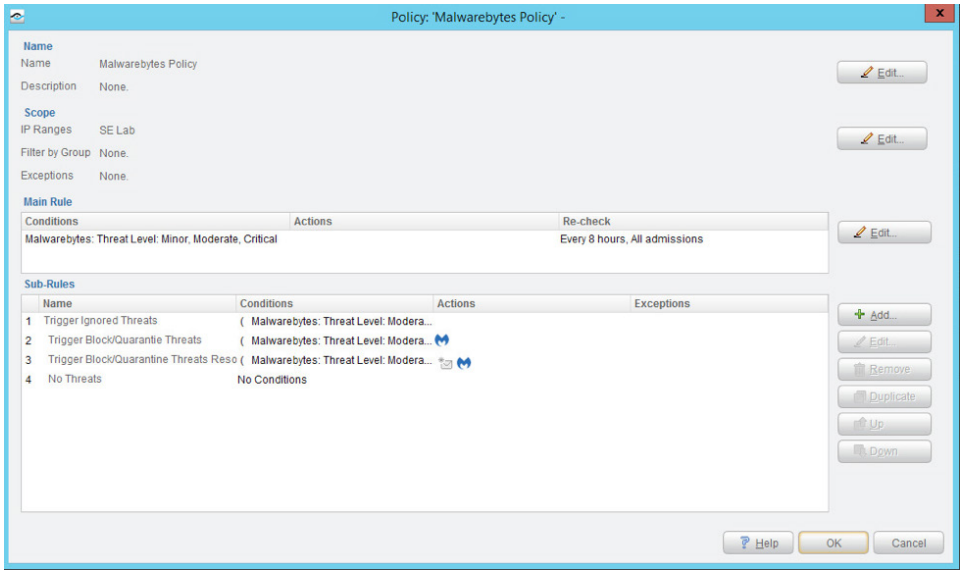


Figure 3. Automated Malwarebytes threat scanning via CounterACT console



malwarebytes.com/integrations 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. For more information, please visit us at http://www.malwarebytes.com/.