Malwarebytes

DATA SHEET

Breach remediation for Forescout

Improve real-time visibility, control, and automated threat response of network-connected devices.

Overview

Enhance endpoint protection within your security and IT ecosystems for faster response, reduced re-imaging, and continuous productivity.

Responding to incidents with speed and efficiency is of upmost importance in today's security environment—despite limited resources and a seemingly endless stream of updates. Malwarebytes Breach Remediation's integration with Forescout revs up incident response, stops zero-day exploits, and reduces exposure to new threats. Security teams can identify, prioritize, and remediate infected endpoints faster, without impacting user productivity.

KEY BENEFITS

Increased visibility
Discover threats across the network in real-time

Enhanced remediation
Assess high-risk endpoints and remediate threats instantly

Automated workflows
Automate incident response workflows beyond quarantine

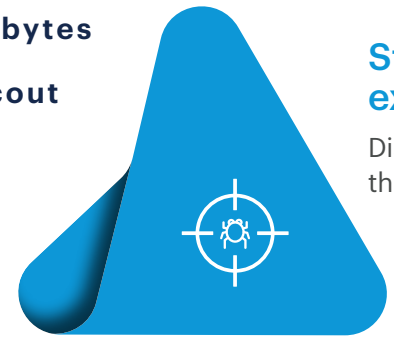
Revs up incident response

Assess high-risk endpoints and remediate threats instantly

Reduces exposure to new threats

Automate response workflows beyond quarantine

Malwarebytes + Forescout



Stops zero-day exploits

Discover threats across the enterprise in real-time

FORESCOUT

Security operations and incident response challenges

Limited endpoint visibility

Although most organizations have established strong perimeters and network anomaly detection between their business-critical hosts and the Internet, many still lack the visibility into individual endpoints across the enterprise. These endpoints may have disabled or broken security agents installed that prevent threats from being detected by periodic scans.

Incomplete threat detection

Today's threats are more sophisticated than ever before and can easily evade traditional security defenses. Multi-vectored, stealthy, and targeted attacks are focused on acquiring sensitive personal information and intellectual property. Compromised endpoints and data breaches can often remain undetected for weeks or months, allowing threat actors to collect a wealth of critical data on their targets or launch second and third waves of attack.

Manual incident response workflows

Many businesses have invested in security, event monitoring, and threat correlation tools to manage alerts on potential incidents. Unfortunately, most of these are disparate technologies that are ill-equipped—if not flat-out 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.

Malwarebytes and Forescout Benefits

Malwarebytes integrates with Forescout to help businesses accelerate incident response, stop zero-day exploits, and reduce exposure to emerging threats. Our combined solution provides two-way communication between Forescout and the agentless, headless Malwarebytes Breach Remediation tool. Once deployed, the integrated solution delivers enterprise-wide threat sweeping, threat assessment, infection analysis, and automated on-demand incident response.

Increase visibility into emerging threats

Discover threats and exploit attempts across the enterprise with real-time visibility. Profile and classify threats based on severity, device, and remediation action.

Detect and remediate threats

Allow, deny, or limit network access based on detected threats and remediation response stage. Assess high-risk endpoints and remediate threats instantly.

Automate threat response

Share contextual insights into discovered threats across the network. Automate incident response workflows beyond quarantine.

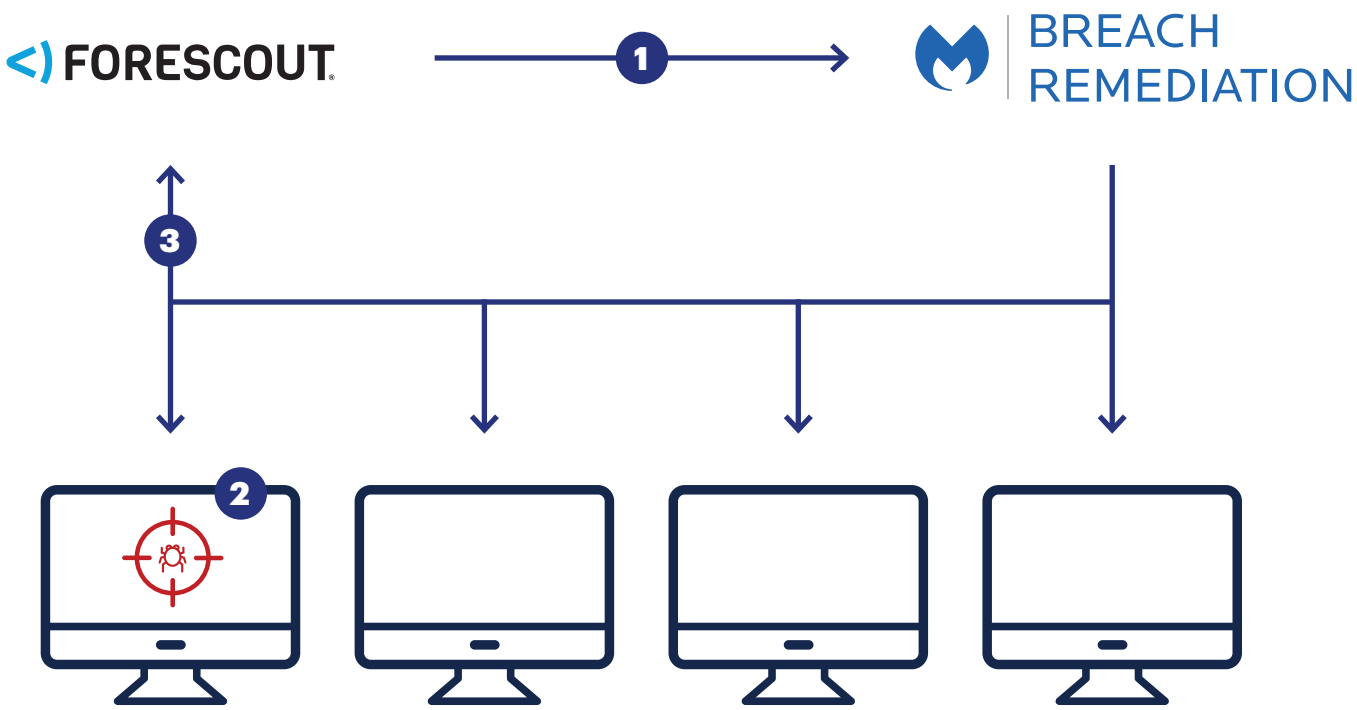
Malwarebytes integration with Forescout provides businesses with comprehensive and up-to-date information on network threats. In addition, it offers automated response to indicators of compromise (IOCs) while providing dynamic threat detection that reduces an organization's attack surface.

Using Forescout, administrators can easily and rapidly deploy either Malwarebytes Endpoint Security or Malwarebytes Breach Remediation onto all Windows and Mac endpoints. Advanced threats, including zero-day exploits and ransomware, are automatically detected and removed. Security teams gain improved visibility across the enterprise due to shared reporting of discovered and remediated threats.

Use case: rapid threat response

In a hypothetical scenario, nine endpoints are infected with TrickBot, after an employee opens a malicious attachment from a phishing email, which launched the initial infection. TrickBot then spreads laterally on the network, infecting either other endpoints. Here is how Forescout and Malwarebytes handle the infection:

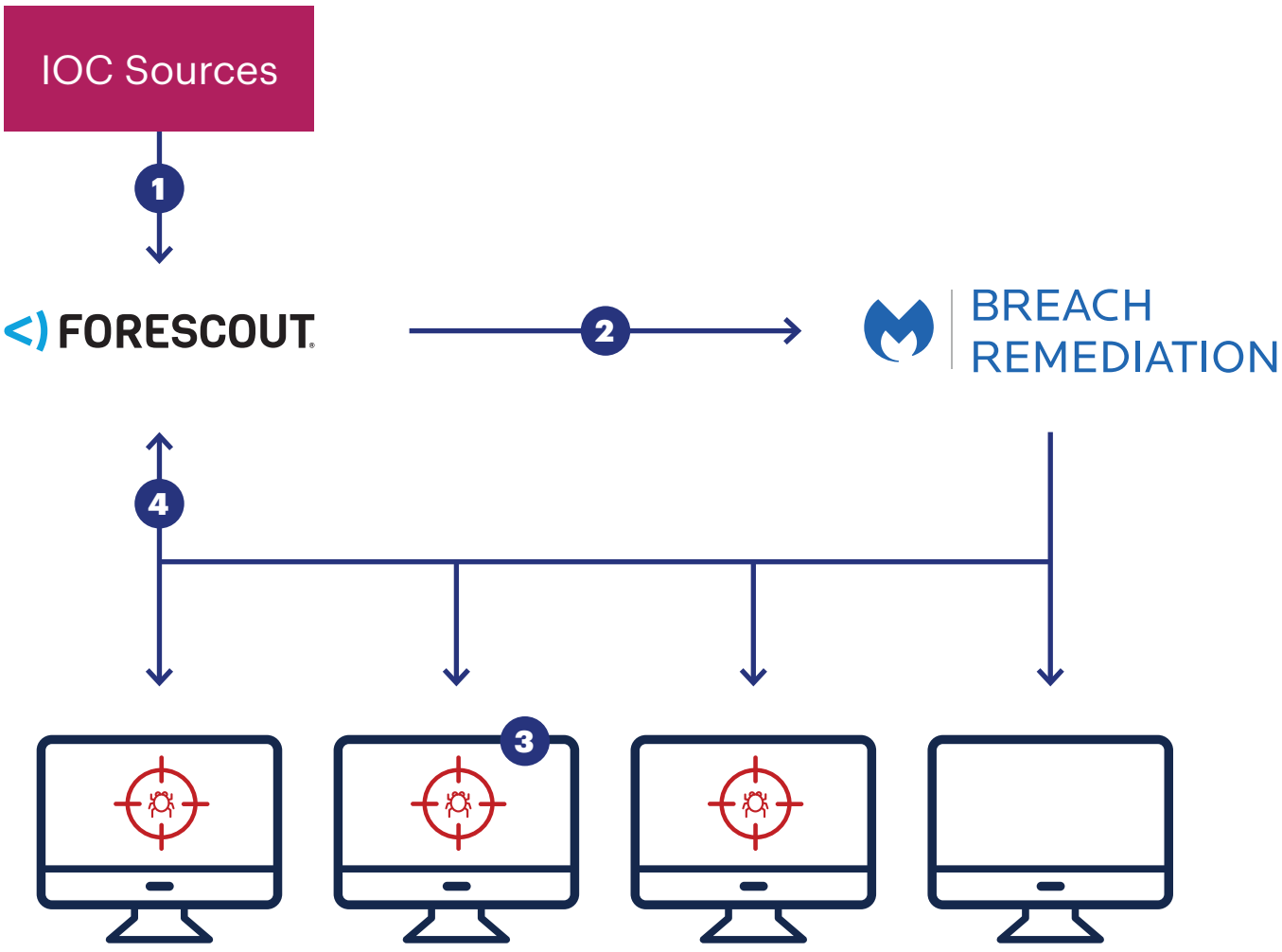
1. **Forescout silently deploys Malwarebytes Breach Remediation** to compromised hosts and simultaneously denies or limits network access based on policy, detected threats, and remediation response stage.
2. **Malwarebytes Breach Remediation** scans, detects TrickBot, and thoroughly removes the threat from the compromised hosts.
3. **Forescout receives a detection event summary and threat remediation status** from Malwarebytes Breach Remediation, which dissolves post-scan. Forescout subsequently allows the healthy hosts network access.



Use case: active threat hunting

In common scenarios, security teams leverage 3rd party IOC intelligence to proactively hunt threats across their network before infections occur or spread. Here is how Forescout and Malwarebytes handle this:

1. **Third-party IOC threat intelligence** feeds Forescout with the latest and most prevalent malware threat data, to be used in targeted threat hunting across the network.
2. **Forescout silently deploys Malwarebytes Breach Remediation** onto enterprise hosts.
3. **Malwarebytes Breach Remediation** scans and detects several zero-day exploits, information-stealers, and rootkits. The agentless program thoroughly removes threats from compromised hosts using zero-hour behavioral heuristics and incorporated third-party IOC threat intelligence.
4. **Forescout receives the detection event details and remediation status** from Malwarebytes Breach Remediation, which dissolves post-scan.



Summary

Malwarebytes and Forescout have integrated to help businesses develop a stronger security posture, from the network-level down to individual endpoints. This combined solution provides two-way communication between Forescout and Malwarebytes Breach Remediation tool to stop zero-day exploits, reduce exposure to emerging threats, and improve incident response.

GET STARTED TODAY

Visit malwarebytes.com/integrations to find the technical user guide and download Malwarebytes Breach Remediation for Forescout.

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.