Bromium vSentry and ForeScout CounterACT Integration

Key Benefits

PREVENT ZERO-DAY ATTACKS

Prevent zero-day attacks from targeting enterprise endpoints through Web, email, or USB on or off the corporate network

LEARN MALWARE INTENT

Automated real-time threat intelligence for unknown attacks targeting end users with comprehensive attack kill-chain data

IDENTIFY COMPROMISED ASSETS

Leverage threat intelligence to identify already compromised assets within the enterprise

AUTO REMEDIATION

Automated removal of malware from previously infected endpoints

The Challenges

Zero-day protection

Prevent zero-day attacks from targeting enterprise endpoints through Web, email, or USB on or off the corporate network.

Real-time threat intelligence

Enterprises need real-time threat intelligence on zero-day attacks targeting their endpoints. On seeing an attack for the first time a security team needs to understand the attack and block it using network and endpoint controls. Existing endpoint technologies provide no such real-time insights to the security team.

Risk assessment & mitigation

On receiving threat intelligence on a new attack, enterprises need to identify existing assets which may be compromised and remediate them. Current security and management infrastructure doesn't provide an automated mechanism to perform this analysis.

Bromium and Forescout—Protecting Enterprise Endpoints From Targeted Attacks

The Bromium® vSentry® and Forescout CounterACT solution protects enterprises from zero-day attacks targeting endpoints. vSentry, installed on the endpoint, uses hardware-level isolation to prevent malware from infecting or persisting on enterprise desktops. Bromium Live Attack Visualization and Analysis (LAVA™) identifies advanced attacks without the need for signatures and provides actionable intelligence on these "unknown" attacks.

The solution protects the enterprise from zero-day malware, which is undetectable through traditional security layers, thereby eliminating the risk of a security compromise at the endpoint from key attacks vectors—Web, email, and USB. The cost of remediation and incidence response for endpoint infections is drastically reduced. The solution enables the security and IT teams to empower users with unrestricted access to the Web thereby increasing productivity.

Bromium®

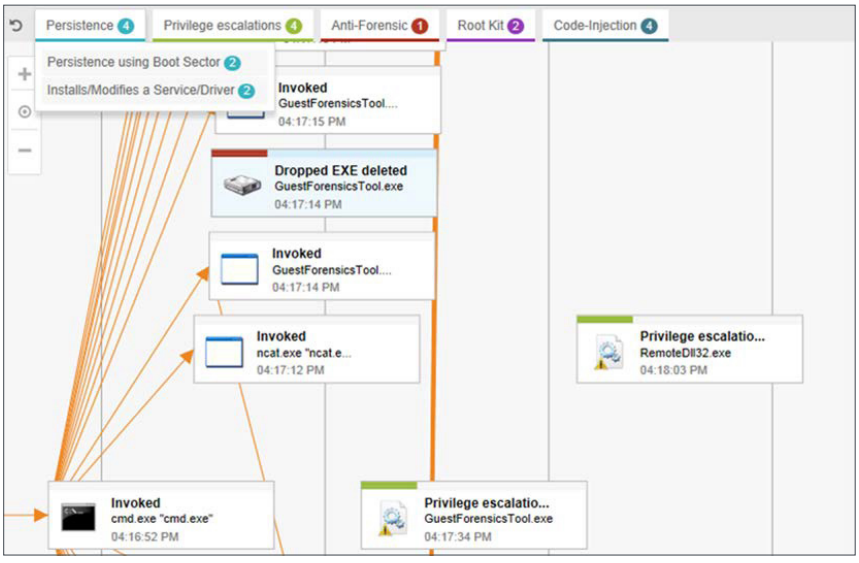
About Bromium

Bromium has transformed endpoint security with its revolutionary isolation technology to defeat cyber attacks. Unlike antivirus or other detection-based defenses, which can't stop modern attacks, Bromium uses micro-virtualization to keep users secure while delivering significant cost savings by reducing and even eliminating false alerts, urgent patching, and remediation—transforming the traditional security life cycle.

Forescout CounterACT leverages LAVA threat intelligence to identify and remediate compromised devices not protected by Bromium within the enterprise. Bromium LAVA collects real-time threat intelligence about the attack by monitoring the execution of malware within the micro-VM. The entire attack kill chain is identified including hashes of malware executables and command-and-control IP addresses.

This information is automatically sent to the Forescout CounterACT engine through syslog protocol. Forescout CounterACT leverages the real-time LAVA threat intelligence to identify existing compromised devices within the enterprise. By leveraging its enterprise-wide visibility CounterACT can detect infected devices in real time as well as do automatic remediation. From the LAVA intelligence automatic signatures get created and published to other endpoint and network security products to increase defense in depth.

LAVA REAL-TIME ATTACK ANALYSIS



Bromium, Inc.
20813 Stevens Creek Blvd
Cupertino, CA 95014
info@bromium.com
+1.408.213.5668

Bromium UK Ltd.
Lockton House
2nd Floor, Clarendon Road
Cambridge CB2 8FH
+44.1223.314914

For more information go to www.bromium.com
or contact sales@bromium.com

SB.Forescout.US-EN.1510