The ForeScout – Bromium Joint Solution

Improve defenses against advanced threats and automate threat response

ForeScout and Bromium have teamed up to deliver a powerful solution for risk mitigation and threat defense. With this joint solution organizations can reduce their attack surface, identify advanced threats, scan for indicators of compromise (IOCs), and automate threat response. As a result, you can limit malware propagation, minimize data breaches, avoid costly investigation and protect your reputation.

See

- Discover devices the instant they connect to your network without requiring agents
- Profile and classify devices, users, applications and operating systems
- Continuously monitor connected devices, including corporate, BYOD and IoT endpoints

Control

- Allow, deny or limit network access based on device posture and security policies
- Reduce attack surface by ensuring endpoints have up-to-date security defenses
- Initiate remediation and risk mitigation actions on malicious or infected endpoints

Orchestrate

- Quarantine infected endpoints identified by your ATD system to prevent lateral malware propagation
- Scan endpoints connecting to your network for IOCs identified by your ATD system
- Automate system-wide response to quickly mitigate threats and data breaches

The Challenges

Visibility. According to industry experts, a vast majority of successful attacks exploit well-known vulnerabilities and security gaps on endpoints. Most organizations are unaware of a significant percentage of the endpoints on their network because they are either not managed (BYOD, guest and IoT), have disabled or broken agents, or aren't detected by periodic scans (transient devices). As such, you are unaware of the attack surface on these devices.

Threat Detection. Today's cyber threats are more sophisticated than ever and can easily evade traditional security defenses. Multi-vectored, stealthy and targeted, these 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. To detect these advanced threats, zero-day attacks and infected endpoints, you need new security controls that do not rely on signatures.

Response Automation. The velocity and evasiveness of today's targeted attacks, coupled with increasing network complexity, mobility and BYOD, are creating the perfect storm for IT security teams. Without an automated system to continuously monitor and mitigate endpoint security gaps, valuable time is lost performing these tasks manually. And without the ability to automatically and quickly respond to attacks and security breaches, you are leaving the window open for cyber threats to propagate within your network and exfiltrate data.

How it Works

ForeScout CounterACT™ and Bromium vSentry work together to quickly detect and contain advanced threats, and break the cyber kill chain.

ForeScout CounterACT is a network security appliance that provides IT organizations with the unique ability to see devices, including non-traditional devices, the instant they connect to the network. CounterACT provides policy-based control of these devices and works with ForeScout ControlFabric™ Architecture to orchestrate information sharing and automate operation among disparate security and IT management tools.

Bromium vSentry, installed on an 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 attacks to ForeScout CounterACT in real time. CounterACT leverages this threat information and enables you to scan the network for IOCs, determine the extent of infection on your network and contain infected endpoints. This disrupts the cyber kill chain and prevents further lateral threat propagation and data exfiltration.

When Bromium vSentry detects malware and determines that a device within your network has been compromised, it informs ForeScout CounterACT about the affected system(s) and IOCs. Based on your policy, CounterACT leverages the IOC information from Bromium to scan other endpoints that are attempting to connect or are already connected to your network for presence of infection. Additional endpoints may be infected because they are either unmonitored corporate devices, or personal devices (BYOD) not within the scope of Bromium vSentry. As such, these infected endpoints aren't detected by Bromium.

Regardless of whether CounterACT discovers infected endpoints from Bromium or via IOC scanning, it can automatically take policy-based mitigation actions to contain and respond to the threat. Various actions can be performed depending on the severity or priority of the threat, such as quarantine endpoints, initiate direct remediation, share real-time context with other incident response systems, initiate a scan by another third party product, or notify the end user via email or SMS.

1. An infected system connects to the network.
2. Bromium informs CounterACT
3. ForeScout CounterACT scans other endpoints on corporate network for IOCs
4. CounterACT isolates other infected endpoints and initiates appropriate risk mitigation actions.

Learn more at
www.ForeScout.com

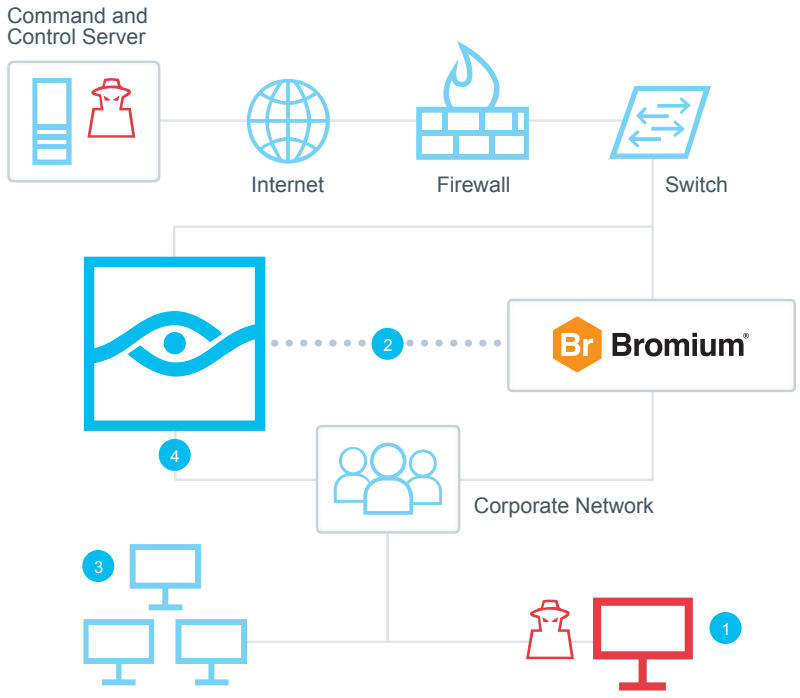

Figure 1: ForeScout CounterACT receives IOCs from Bromium vSentry and takes threat mitigation actions.

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591
Fax 1-408-371-2284

Version 1_16