Solution Brief

The ForeScout-ArcSight Joint Integration

Improve real-time visibility over managed and unmanaged devices while automating network access control and threat response

See

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

Control

- Allow, deny or limit network access based on device posture and security policies
- Assess and remediate malicious or high-risk endpoints as determined by your SIEM product
- Improve compliance with industry mandates and regulations

Orchestrate

- Receive contextual information from your SIEM product and pro-actively take appropriate action
- Automate common workflows, IT tasks and security processes across systems
- Leverage the integration between ForeScout and your SIEM product to provide real-time view of threats across the enterprise

ForeScout has partnered with HP ArcSight to deliver a unique and powerful risk management solution. With this joint solution, you can achieve a more accurate understanding of your security risk posture and respond more quickly to remediate risky endpoints. The result is stronger security and greater operational efficiency.

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 tool.

The Challenges

Visibility. Any serious attempt to manage security risk must start with knowledge of who and what is on your network, including visibility to whether the devices on your network are compliant with your security standards. 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. According to industry experts, a vast majority of successful attacks exploit well-known vulnerabilities and security gaps on endpoints connected to your network.

Threat Detection. Today's cyber attacks are more sophisticated than ever. Multi-vectored, stealthy and targeted threats easily evade traditional security defenses such as firewalls, intrusion prevention systems, anti-virus platforms, and secure web and email gateways. Originating from highly motivated and well-funded threat actors and nation states, these attacks are focused on acquiring sensitive personal information, intellectual property or insider information. As the attackers have gained the upper hand, organizations are being compromised at an accelerating rate. In order to effectively detect and block these sophisticated threats, new security controls that do not rely on signatures are needed.

Response Automation. The velocity and evasiveness of today's targeted attacks, coupled with increasing network complexity, mobility and BYOD, are creating a perfect storm for any incident response program. Without an automated system to monitor, install, update and reactivate security agents on managed systems, valuable time is lost performing these tasks manually. Without the ability to apply security controls to unmanaged endpoints (BYOD, guest and IoT), you are increasing your attack surface and putting your infrastructure at risk. And without a system 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

The joint solution combining the HP ArcSight platform and ForeScout CounterACT provides a real-time view of enterprise-wide threats that can originate from non-compliant endpoints, and rapidly remediates them to reduce overall business risk. The result is an automated risk management solution that provides stronger security and greater operational efficiency.

When CounterACT discovers infected endpoints, it can receive instructions from ArcSight and 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.

The unique capabilities of the integration between ForeScout CounterACT and HP ArcSight allows ArcSight to correlate real-time endpoint information provided by ForeScout with real-time activity from other devices, security products and applications. This allows ForeScout the ability to exercise immediate control over devices on the network. The HP ArcSight console can be used as the centralized command and control system in the security operations center to provide a real-time view of enterprise-wide threats across the enterprise.

1. Device connects to the network.
2. CounterACT informs ArcSight of device status.
3. CounterACT receives instructions from ArcSight based on policy.
4. CounterACT allows or denies access based on compliance assessment.

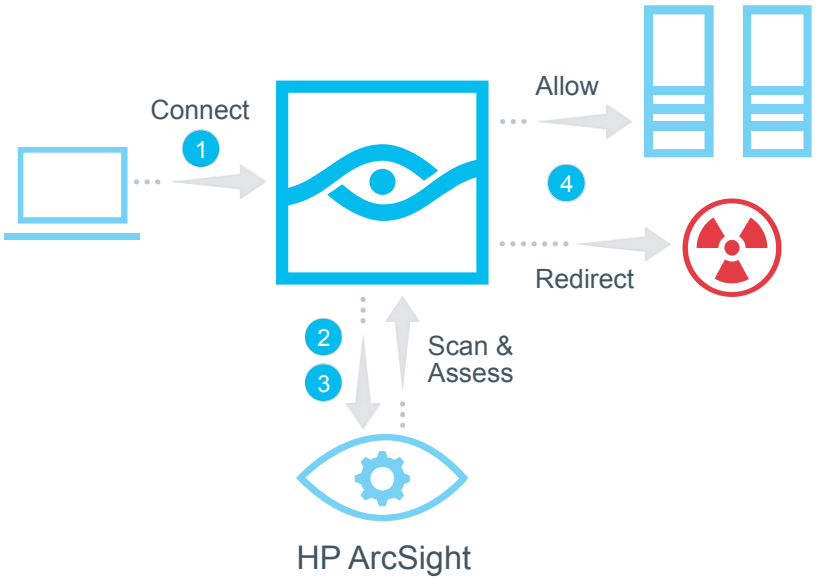

Figure 1: ForeScout CounterACT and HP ArcSight work in concert to assess and manage devices as they access the network.

Learn more at
www.ForeScout.com

ForeScout™

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 3_16