The ForeScout-AirWatch Joint Solution

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
- Seamless enrollment & installation of MDM agents on unmanaged devices
- Improve compliance with industry mandates and regulations

Orchestrate

- Operational efficiency with automated enrollment
- Automate common workflows, IT tasks and security processes across systems
- Accelerate system-wide response to quickly mitigate risks and data breaches

ForeScout has integrated its automated security control platform for network access control (NAC) and endpoint compliance with AirWatch's Mobile Device Management solution. With this joint solution, IT organizations obtain better security, compliance and control for endpoints on an enterprise network.

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.

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

ForeScout CounterACT™ integrates with AirWatch 6.2 and later releases to address these challenges and complete the mobile security puzzle. Through this integration, you can leverage your existing AirWatch system within the broader context of unified security control that ForeScout CounterACT provides.

ForeScout CounterACT communicates bi-directionally with AirWatch through a connection known as the ForeScout Mobile Integration Module. This allows CounterACT to query AirWatch for device attributes — "Is this device enrolled? Is this device compliant?" This information can then be used as a basis for deciding whether to allow the device onto the network. From the CounterACT console, you can configure and enforce network security policies, monitor and report on policy adherence for devices in your organization — PCs, Macs, Linux, smartphones and tablets.

When used in conjunction with AirWatch, ForeScout CounterACT with the MDM Integration Module provides automated real-time detection of mobile devices, seamless enrollment and installation of MDM agents, just-in-time compliance checks and policy based access rules based on your security policies regardless of the device type.

1. Device connects to the network
2. CounterACT informs AirWatch of device status
3. If non-compliant, CounterACT initiates auto enrollment
4. CounterACT allows or denies access based on compliance assessment

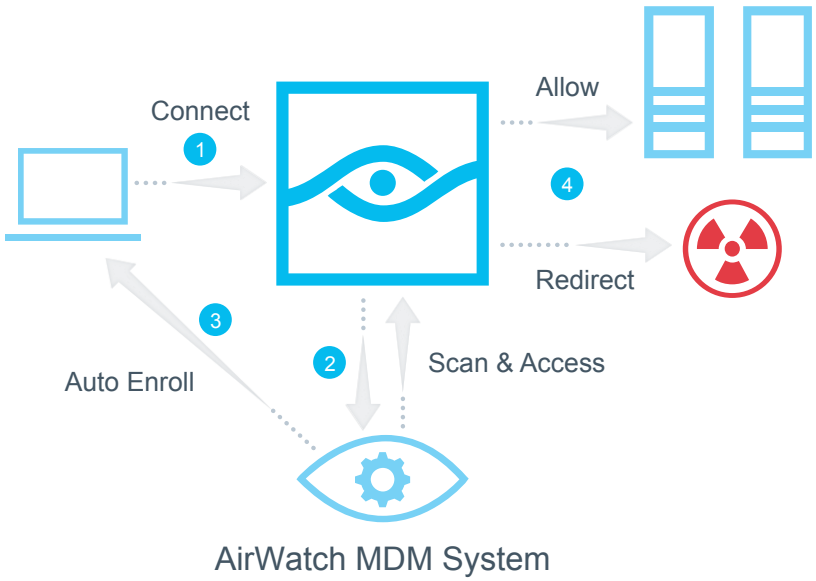

Figure 1: ForeScout CounterACT and AirWatch work in concert to assess and manage devices as they access the network.

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