Forescout and Mist Systems

Visibility and Security Enforcement at the Edge of the Network to Achieve Artificial Intelligence-Driven Wired, Wireless and IoT Endpoint Compliance

Mist
A Juniper Company

With the proliferation of devices on today's networks and a highly mobile and transient workforce, IT and security teams are constantly challenged to track devices, their hygiene and security posture as they enter or leave the network. New devices such as unmanaged laptops, smartphones, tablets, Internet of Things (IoT) devices of all shapes and sizes, rogue devices, virtual servers and public cloud instances join your network nearly every hour. In addition, business that provide BYOD or guest environments are challenged with securing devices that are not in their control but still represent a threat to the network.

Challenges

Visibility. Serious efforts to manage security risk must start with knowing what devices are accessing the enterprise-wide network and the security posture for all devices. Most organizations are unaware of a significant percentage of endpoints on their network, primarily due to devices such as:

- Unmanaged guest and employee owned devices
- IoT devices
- Transient devices undetected by periodic scans
- Remote corporate devices not directly connected to the network

Endpoint Compliance. To achieve and maintain compliance with internal policies and external mandates, organizations need real-time solutions to assess device security state and identify security issues. Critical questions must be addressed such as: Are management and security agents installed and operational on corporate devices? Are BYOD, IoT and other devices that cannot be managed via agents compliant with security policies? Are high security risk indicators of compromise (IOCs) known with a plan for remediation? Can compliance be enforced on corporate devices that are not directly connected to your corporate network?

Securing Guest and BYOD Wireless Environments. Providing network access to guest and/or employee owned devices is expected in today's world. While benefits are gained by providing this access, organizations open themselves to considerable risk doing so. Individuals could engage in morally or ethically questionable activities on a business network or even illegal activity such as copyright infringing downloads. They may also accidentally or deliberately install malware or ransomware or visit phishing websites. Organizations need automated solutions to isolate non-compliant, high-risk and/or compromised endpoints and immediately initiate network and host remediation actions.

Benefits

- Maintain continuous visibility and authorized access for all IP-connected devices, including BYOD, guest and IoT
- Continuously enforce device configuration, network access and security policy compliance
- Automate incident incident response actions to mitigate and remediate threats
- Capitalize on Artificial Intelligence for continuous device profiling to enhance cybersecurity effectiveness

Highlights

- Automate wireless access controls based on Mist AI
- Enhance wireless access Mist AI with rich Forescout data to boost anomoly detection and policies
- Drive Forescout actions from Mist AI to mitigate and remediate threats
- Streamline security operations through automated API-driven workflows among Mist, Juniper and Forescout

The Forescout - Mist Solution

Mist, a Juniper® Networks company, and Forescout have partnered to bring automation and programmability to wireless network access control. The combined solution provides end-to-end visibility and operational simplicity with a completely programmable and automated network to mobile users and IoT devices while also laying a foundation for a more comprehensive artificial intelligence (AI)-driven security solution that leverages the combined products.

The Forescout - Mist combined solution monitors, profiles and authenticates headless devices and mobile clients connecting to the wired and wireless network based on their network traffic patterns, including smartphones, tablets, laptops, IoT devices (HVAC systems, security devices, displays, sensors, lights, etc.), robots and other connected platforms - without requiring an agent which allows visibility of all IP-connected devices. Once fingerprinted, only authorized access will be allowed. If anomalous or threatening behavior is observed, the following types of actions can be driven using Mist's AI engine in conjunction with the Forescout platform.

- **Notify:** Automatically notify IT personal via email, trouble tickets
- **Conform:** Change roles and remediate software as needed.
- **Restrict:** Quarantine devices, change VLANs or other policy settings

The Forescout visibility and control platform is integrated with Mist's WXLAN Policy engine, enabling the automated enforcement of policies for Mobile & IoT devices that can be on any network profile-802.1X, PSK or Open Guest Networks. Mist's comprehensive APIs provide streaming telemetry on device connections and client context, and ingest policies programmatically to enforce at the network edge from the Forescout platform to blacklist or quarantine the device.

In addition, Juniper's Connected Security solution integrates with the Forescout platform to remediate threats from infected hosts on Juniper Networks' devices, third-party switches, and wireless access points with or without 802.1X protocol integration.

About Mist, A Juniper Company

Mist built the first AI-driven wireless platform with the world's first virtual IT assistant. The Mist Learning Wireless LAN makes Wi-Fi predictable, reliable and measurable by providing unprecedented visibility into the user experience and by replacing time consuming manual IT tasks with proactive automation. In addition, Mist is the first vendor to bring enterprise-grade Wi-Fi, BLE and IoT together to deliver personalized, location-based wireless services without requiring battery-powered beacons. All operations are managed via Mist's modern cloud architecture for maximum scalability, agility and performance.

Find out more at www.mist.com.

About Forescout

Forescout Technologies is the leader in device visibility and control. Our unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environments and orchestrate actions to reduce cyber and operational risk. Forescout products deploy quickly with agentless, real-time discovery and classification of every IP-connected device, as well as continuous posture assessment. As of December 31, 2018, 3,300 customers in over 80 countries rely on Forescout's infrastructure-agnostic solution to reduce the risk of business disruption from security incidents or breaches, ensure and demonstrate security compliance and increase security operations productivity.

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

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

Learn more at Forescout.com