ForeScout

Organizational Challenges

- Improve overall network security
- Protect sensitive data against external threats
- Ensure access and availability to employees, contractors and customers
- Comply with internal policies and external regulations
- Maintain the value of existing security investments

Technical Challenges

- Discover unknown devices on the network that are not outfitted with software agents
- Discover and monitor virtual instances and cloud workloads
- Identify device type and location, user identity and role, and level of compliance
- Prevent infected or noncompliant devices from spreading malware
- Prevent targeted attacks from stealing data or forcing network downtime
- Automate network access control to provide the right action(s) for each situation without human involvement
- Measure effectiveness of security controls and demonstrate compliance with regulations

Network Access Control

Gain real-time visibility and control of devices the instant they join the network

Explosive growth in devices and device types continues unabated. Many can't be seen or managed by agent-based methods or traditional NAC tools, allowing unauthorized devices to access your network and probe for vulnerabilities. Take control with a visibility platform that can see every type of device on the network and enforce your policies.

The Challenge

Today's enterprise networks serve a vast array of traditional and non-traditional devices and other endpoints—everything from PCs, tablets and smartphones to industrial controls, virtualized servers, wireless access points and cloud-based applications. And, without a doubt, the scope of device-related challenges will expand as BYOD, IoT, operational technologies (OT), hybrid IT environments and hacker sophistication continue to make gains. So, your network access control (NAC) solution must manage the corporate- and employee-owned devices that you're aware of, as well as the increasing numbers of unauthorized, "under-the-radar" devices.

As an IT or security systems manager, you have to know whether the devices and systems attempting to access your network, or already on there, meet your organization's security standards.

The ForeScout Solution

The ForeScout platform offers comprehensive NAC capabilities and more, based on real-time visibility of devices the instant they access the network—regardless of where that network exists within your extended enterprise. It continuously scans networks and monitors the activity of known, company-owned devices as well as unknown devices such as personally owned and rogue endpoints.

And it lets you automate and enforce policy-based network access control, endpoint compliance and mobile device security. The vast majority of IoT and OT devices on your network don't include—or can't handle—software agents. That's why the ForeScout platform offers agentless discovery technologies and passive monitoring techniques to avoid business disruption. It also provides an extensive range of automated controls that preserve the user experience and keep business operations running to the maximum extent possible.

The foundation of ForeScout platform intelligence and functionality can be summed up in three words:

See Agentless discovery and profiling offers the unique ability to identify devices the instant they connect to your network, without

> **ForeScout provides JPMorgan Chase with enhanced visibility and control across the hundreds of thousands of devices connected to our corporate network."**
> — Rohan Amin, Global CISO, JPMorgan Chase & Co.

ForeScout NAC Use Cases:

- Control access to confidential data based on device and user profiles
- Prevent infected or noncompliant devices from spreading malware
- Automatically enforce actions for identified situations without human involvement

requiring software agents or previous device knowledge. The ForeScout platform profiles and classifies devices, users, applications and operating systems while continuously monitoring managed devices, virtual endpoints, cloud workloads, personally owned devices and other systems. It can even tell whether IoT and other devices are using factory default and commonly used credentials that can be easily hacked.

Control Once you understand the compliance posture of every device, you need an automated way to allow, deny or limit network access based on your security policies. Because the ForeScout platform integrates with your wired/wireless switches, VPN concentrators, cloud-based management systems and next-generation firewalls, it can dynamically assign devices to network segments—using real-time device context—to address changes in device behavior, security posture or network modifications. By assessing and remediating malicious or high-risk endpoints, the ForeScout platform mitigates the threat of data breaches and malware attacks that would otherwise put your organization at risk. In addition, by continuously monitoring devices on your network and controlling them in accordance with your security policies, the ForeScout platform streamlines your ability to demonstrate compliance with industry mandates and regulations.

NOTIFY	CONFORM	RESTRICT
Send email to end-user	Move to guest network	Quarantine device (VLAN, Virtual FW)
Send on-screen notification	Change wireless user role	Turn off switch port
Redirect to web page	Assign to self-remediation VLAN	Block wireless or VPN access
Request end-user acknowledgement	Restrict rogue devices/infrastructure	Use ACLs to restrict access
Send email to administrator	Start mandatory applications/process	Terminate unauthorized applications
Send Syslog/CEF messages	Update anti-virus/security agents	Disable NIC/dual-homed
Open help desk ticket	Apply OS updates/patches	Disable peripheral device
Share context with other IT systems	External drive compliance	Trigger remediation actions/systems

The ForeScout platform can enforce the appropriate level of control—from modest to stringent—based on your security policies.

Orchestrate The ForeScout platform integrates with more than 70 network, security, mobility and IT management products* via ForeScout Base and Extended Modules. This ability to share real-time security intelligence across systems and enforce a unified network security policy reduces vulnerability windows by automating system-wide threat response. What's more, it lets you gain higher ROI from your existing security tools while saving time through workflow automation.

Redefining Network Access Control

Three characteristics make the ForeScout platform different from other NAC solutions:

Agentless: No endpoint agents are required to see or control your IoT devices, OSs, OT systems and virtual instances.

Continuous: The ForeScout platform continuously monitors device behavior and compliance status as devices come and go from your network

Heterogeneous: No forced network upgrades. No vendor lock-in. Use your existing network infrastructure and third-party security solutions—with or without 802.1X authentication.

The ForeScout platform gathers rich contextual insights regarding the endpoint, its location, who owns it and what's on it. It can ensure:

- Unauthorized devices and unsanctioned applications are not on your network
- Authorized devices are configured with the latest operating systems, up-to-date antivirus software is installed and running, and vulnerabilities are properly patched
- Encryption and data loss prevention agents are working
- Users are prevented from running unauthorized applications or peripheral devices on the network

When endpoints don't measure up to organizational standards, the ForeScout platform automatically initiates one or more policy-based enforcement and remediation actions ranging from an email notification of noncompliance to mandatory remediation (such as software updating) to outright quarantine or access prevention. There's no need for human intervention or manual labor associated with managing guest access, locating systems and opening or closing network ports. Network access is controlled according to policy.

For more than 2,900 enterprises in over 80 countries,* ForeScout provides intelligent, cost-effective network access control that meets the highest standards for security and regulatory compliance as well as ease of use and deployment.

The ForeScout platform is sold as either a virtual or physical appliance that deploys within your existing infrastructure and typically requires no changes to your network configuration. It installs out-of-band, avoiding latency or issues related to the potential for network failure, and can be centrally administered to dynamically manage up to two million endpoints from one Enterprise Manager console.

Learn more at
www.ForeScout.com

ForeScout

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

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

*As of June 30, 2018