FORESCOUT

Solution Brief

Modern NAC

Identify all devices, assess security posture and enforce access control across heterogeneous networks

> "NAC tooling today is best suited to aid in isolating devices and unapproved entities (users, segments, devices, etc.) from "touching" the network. Use these newer NAC technologies, from vendors such as Forescout, to aid in keeping unknown and likely unpatched items off of your Zero Trust networks."[1]
>
> — Chase Cunningham, Principal Analyst, Forrester Research

Today's networks require a modern network access control (NAC) solution capable of much more than simple device authentication. The modern NAC must identify devices, assess posture and compliance, enforce access control across heterogeneous networks, continuously monitor all connected devices and automate response when noncompliance or unusual behaviors are detected.

Challenges

As business and cyber demands continue to evolve, organizations require much more from a NAC solution to address these challenges:

- Unmanaged devices outnumber managed devices on many networks and can't authenticate using traditional methods
- Growing numbers of unmanaged devices introduce additional risk, including blind spots
- Multivendor networks are commonplace, necessitating 802.1X alternatives
- Remote corporate and BYOD systems connecting to the network create new security management challenges
- Inability to automate security, compliance and access policies results in higher operating costs and excess manual effort

"We were told we could deploy the Forescout platform in an afternoon. I looked at one of my team members, and we both rolled our eyes. Then we actually deployed it in a few hours!"

— Mike Roling, CISO,
State of Missouri

The Solution

If these challenges sound familiar, now is an excellent time to evaluate network access control. The Forescout platform is redefining what NAC is and what it can do to solve the organizational and cyber challenges facing your organization. And with Forescout, the modern NAC is non-disruptive and easy to deploy. You receive comprehensive visibility of all devices within days of starting implementation, with policy-based controls often functional within weeks.

Our modern NAC platform delivers foundational network security capabilities that go far beyond simple authentication. These new capabilities include granular device/user identification, posture and compliance assessment, continuous device monitoring, flexible control options and automated response.

Traditional NAC approaches cannot securely authenticate non-traditional systems connecting to campus networks today, such as Internet of Things (IoT) devices. They also rely on agents for assessing posture and compliance of traditional computers. Forescout's detection and profiling capabilities accurately identify, classify and assess all of these devices so you can create context-aware access policies. The Forescout platform works with or without agents, with or without 802.1X and continuously monitors all devices on your network.

Identify: Discover, classify and inventory all connected devices

With the Forescout platform, security and IT operations teams gain 100% real-time visibility of all IP-connected devices the instant they access the network—for an accurate, real-time asset inventory.

- Choose from 20+ active and passive discovery and profiling methods to match your business environment and ensure continuous network availability
- 12M+ device fingerprints in the Forescout Device Cloud give you high-fidelity, three-dimensional device classification capabilities to determine device function, OS, vendor and model, and more
- Gain complete coverage across all locations, networks and device types—without blind spots—with or without 802.1X authentication

"The amount of information we get back from the Forescout platform is incredible. It is by far the best tool I have ever used to find, identify and control systems properly. It has been beyond valuable to us."

— Joseph Cardamone,
Sr. Information Security Analyst,
Haworth International

Comply: Assess security posture and compliance

Agent-based security tools are blind to managed devices with missing, broken or non-functional agents. Plus, since IoT devices can't install security agents, these tools can't assess them—further expanding the attack surface. But with the Forescout platform, you can automate the posture assessment and remediation of all IP-based devices upon connection and continuously after that.

- Find and fix managed devices with broken or missing agents from your existing security tools
- Detect device noncompliance, posture changes, vulnerabilities, weak credentials, IoCs, spoofing attempts and other high-risk indicators—all without agents
- Assess and continuously monitor unmanaged devices, including those that can't accept agents, for enforcing security compliance

Extend the Value of Your Security and IT Investments

Most security tools simply flag violations and alert your staff. The Forescout platform includes plug-and-play modules that extend visibility and control capabilities to:

- Share real-time device context with your security and IT management tools
- Orchestrate workflows and automate response actions
- Continuously assess security posture and enforce compliance of auto-remediated devices

Learn how at forescout.com/platform/eyeExtend.

"[Forescout's] platform and capabilities for IoT/OT security shine above those of the competition. Maximum visibility, leading to maximum operational control and, ultimately, security, is the crux of Forescout's approach to Zero Trust."[2]

—Forrester Research

Connect: Enforce access policies across heterogeneous networks

The Forescout platform enforces Zero Trust security based on device and user identity, device hygiene and real-time compliance status without requiring hardware or software upgrades to infrastructure.

- Provision least-privilege access to enterprise resources based on user role, device type and security posture
- Prevent unauthorized, rogue and impersonating devices from connecting
- Address internal audits and external regulations with confidence, knowing that the security controls you have in place enforce compliance while keeping users productive

Why Forescout:

1. Fast, flexible, non-disruptive deployment.
2. Agentless posture and risk assessment.
3. Rapid time to value and rapid ROI.
4. Vendor-agnostic—use your existing infrastructure.
5. No software or hardware upgrades.
6. Integrations with leading IT and security products.
7. Avoid 802.1X complexity and operational costs on wired networks.
8. Enterprise-class—scale to 2 million endpoints.
9. Robust policy engine automates incident response to accelerate MTTR.
10. Forrester Zero Trust platform.

Take the next step:

- Request a Forescout Demo
- Visit our NAC Solution Page

***Notes**

1. The Zero Trust eXtended Ecosystem: Networks Strategic Plan: The Security Architecture And Operations Playbook, Forrester Research, January 2, 2019
2. Forrester Wave™: Zero Trust eXtended Platform Providers, Q4 2019

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