FORESCOUT®

Active Defense for the Enterprise of Things.

Modern NAC

Agentless, flexible and non-disruptive Zero Trust security for your Enterprise of Things.

Today's enterprises need a way to implement and maintain Zero Trust access for their many network types and array of connecting things—campus computers, visitors' devices, work-from-home laptops, IoT, OT and smart devices. They need a modern network access control (NAC) platform that can:

- Continuously identify all connecting things
- Assess their posture
- Enforce access policies
- Automatically implement controls for noncompliance or unusual behaviors

Zero Trust is easier said than done

Controlling all the things connecting to enterprise networks is daunting. IT and security architects implementing these systems face challenges that include:

- Earlier NAC solutions didn't succeed due to complexity or risks of negative impact on business operations
- The IoT and OT devices proliferating on enterprise networks can't be authenticated or controlled with traditional agents
- 802.1X-based controls aren't feasible across multivendor networks
- Scheduled network scans don't account for spoofing attempts and other threats that can emerge at any time
- Many Zero Trust access alternatives are too costly and/or require too much 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**

Forescout: the best-in-class modern NAC solution

If the challenges above sound familiar, now is an excellent time to evaluate network access control from Forescout. We can meet your needs and exceed your expectations through:

The most comprehensive visibility

Get 100% visibility of all devices connected to your extended networks, in real time, due to our 20+ active and passive techniques.

Zero Trust for all connecting devices

Contain breach impact through continuous agentless monitoring and a unified policy engine that dynamically segments and isolates all things connecting to your enterprise.

Non-disruptive deployment, with rapid value to your network

Gain full visibility in days and automated control in weeks thanks to agentless software that doesn't need infrastructure upgrades or 802.1X configuration.

Proven for enterprise-class extended networks

Our thousands of satisfied Fortune 1000 customers, some with 2 million endpoints, vouch for the capabilities and confidence Forescout gives them in keeping their networks secure.

EXTEND THE VALUE OF YOUR SECURITY & 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

> **"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

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 help 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

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 support 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 missing, broken or non-functional 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

> **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**

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
- Enforce flexible controls across wired, wireless and VPN infrastructure – with or without 802.1X

> [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

Don't just see it. Secure it.

Contact us today to actively defend your Enterprise of Things.

forescout.com/platform/eyeControl

salesdev@forescout.com

toll free 1-866-377-8771

[1] The Zero Trust eXtended Ecosystem: Networks Strategic Plan: The Security Architecture And Operations Playbook, Forrester Research, January 2, 2019

[2] Forrester Wave^{TM}: Zero Trust eXtended Platform Providers, Q4 2019

FORESCOUT
Active Defense for the Enterprise of Things.

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