FORESCOUT
Active Defense for the Enterprise of Things.

Modern Network Access Control

Why agentless device visibility and control are foundational to effective cybersecurity

Device Visibility and Control: Why You Need It

The ability to discover, classify, assess and control every device that connects to your network is the essential precondition for achieving **Zero Trust security**. Only with real-time knowledge of every physical and virtual endpoint on every segment, granular insight on posture and security state, and automated, policy-based remediation and access control can you reliably help ensure system and data security while responding quickly and accurately to incidents.

100%
REAL-TIME VISIBILITY

Attackers are continuously searching for unmanaged and unsecured devices, and they will eventually find and exploit your blind spots. Agentless visibility and control are the cornerstones of security and compliance. They also play critical roles in addressing numerous business challenges. For example, continuous, in-depth device visibility produces an accurate, **real-time asset inventory** which empowers security and IT personnel to reduce operational costs while helping to ensure regulatory compliance and avoid failed audits.

Why Visibility and Control Are Hard to Obtain

The conventional method of managing network endpoints was a software agent installed on every device. This worked well enough when most endpoints were static, company-owned PCs or servers. But mobility, diversity of device types and virtualization have made contextual visibility and control far more complicated.

An explosion in device numbers and diversity has radically altered the device landscape. Cyber-physical systems such as Internet of Things (IoT) devices and operational technology (OT) systems now connect to the corporate network. Many employees work from home, and some connect to the cloud. The modern enterprise has quickly evolved into an **Enterprise of Things**, and most of these things are not capable of supporting management agents. Even for those that do, an agent-based approach is problematic:

- Agent-based systems don't work when agents are missing, broken or disabled
- Agent-based and 802.1X-based methods result in blind spots on your network and create operational complexity, often resulting in incomplete deployments
- Siloed tools for device compliance lack a unified view, perpetuating blind spots
- Unmanaged devices outnumber managed devices on many networks and can't authenticate using traditional methods
- Mobile, BYOD, guest and work-from-home employees make agent-dependent security time-consuming and ineffective
- Multivendor networks are commonplace, necessitating 802.1X alternatives that don't require hardware or software upgrades

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]

DR. CHASE CUNNINGHAM
PRINCIPAL ANALYST, FORRESTER RESEARCH

The Forescout Solution for Modern NAC

Forescout Technologies has pioneered an agentless approach to network access control (NAC) that addresses the challenges prevalent in today's dynamic and diverse environments. The Forescout platform

offers a continuous, unified view of all your devices across campus, data center, cloud and OT networks. It provides continuous, granular visibility into:

- Campus network devices: Laptops, tablets, smartphones, BYOD/guest systems and IoT devices
- Data center infrastructure: Virtual machines, hypervisors, physical servers and other virtual and physical networking components
- Public and private cloud infrastructure: AWS®, Microsoft® Azure® and VMware® virtual machines
- OT and industrial control systems (ICS): Medical, industrial and building automation devices
- Physical and software-defined network infrastructure: Switches, routers, firewalls, VPNs, wireless access points and controllers

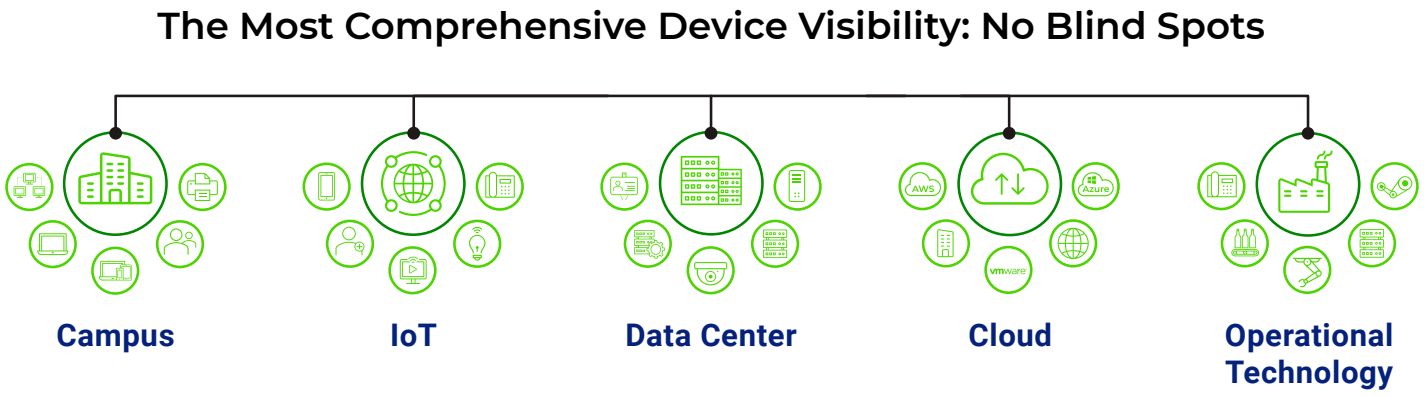


Figure 1: Forescout device visibility scales across the extended enterprise to provide a detailed, real-time asset inventory of every thing that connects to your network.

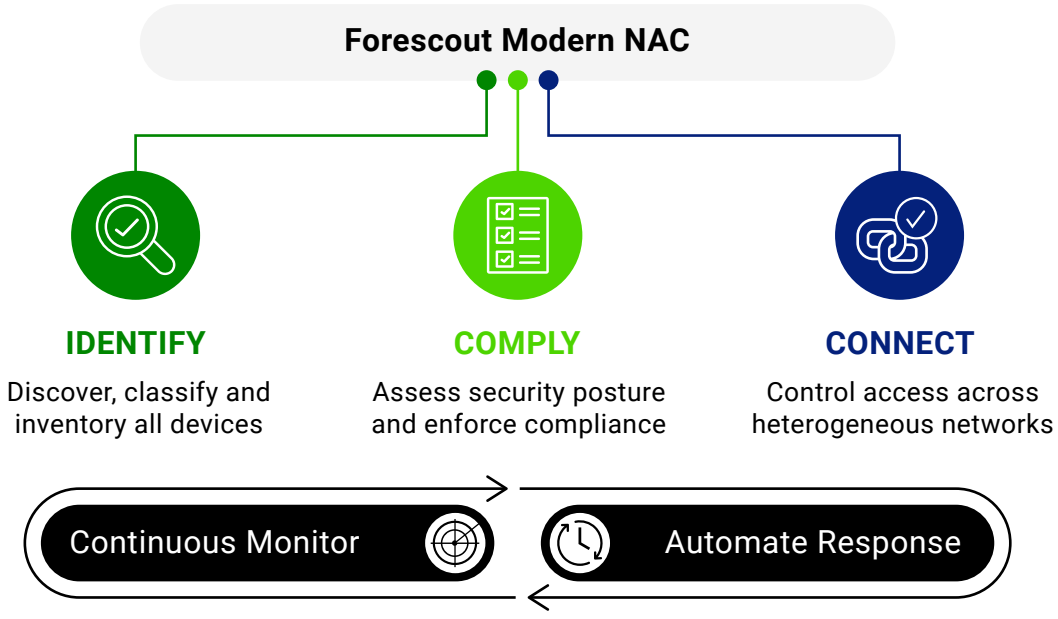


Figure 2: Forescout's modern NAC solution brings essential capabilities to any heterogeneous network without requiring software agents or 802.1X authentication.

What We Do

Forescout's modern NAC solution lets IT organizations:

- Choose from 20+ active and passive techniques for the most comprehensive agentless device discovery across all locations, networks and devices types – no blind spots
- Accurately auto-classify devices based on device function, operating system and version, and vendor and model
- Automatically create and maintain a real-time asset inventory of every IP-connected device on your extended network
- Assess and continuously monitor the security posture of all devices – without agents
- Conform to security policies and industry mandates by automating endpoint remediation
- Enforce flexible network controls based on authentication, user role, device type and security posture – across any heterogeneous wired, wireless or VPN network
- Enforce least privileged access control for Zero Trust security

How We Identify Every Device on Every Network

The Forescout platform provides more than 20 configurable information-gathering techniques that leverage deep integration with leading IT and OT network switches, routers, wireless access points, firewalls, VPN concentrators and data center and cloud solution providers. The platform listens passively to network traffic, parsing many different protocol streams, and can interact directly with both network infrastructure and endpoints. Forescout visibility techniques include:

- Methods that are **passive to the network and end device**. Examples include receiving SNMP traps from switches and wireless controllers, monitoring a SPAN port and parsing protocol streams in the traffic (Forescout provides deep packet inspection for more than 150 IT and OT protocols), collecting and analyzing flow data, or evaluating DHCP requests and HTTP user agent traffic. If 802.1X is implemented, Forescout also monitors RADIUS requests using a built-in or external server.
- Methods that are **active on the network infrastructure**. Examples include polling switches, VPN concentrators, wireless controllers and private and public cloud controllers for a list of connected devices and VMs. For user and device data, the Forescout platform queries directory services, web applications or external databases.
- Methods that are **active on the end device**. Examples include scanning network segments for connected devices using Nmap, remotely inspecting Windows devices using WMI, or Mac and Linux devices using SSH and endpoint profiling using SNMP queries.

Device Visibility Techniques

PASSIVE TECHNIQUES	ACTIVE TO INFRASTRUCTURE	ACTIVE TO END-DEVICE
SNMP traps	Physical network infrastructure polling	Agentless inspection Windows (WMI, RPC, SMB)
SPAN traffic • DHCP requests • HTTP user-agent • TCP fingerprinting • Medical protocol parsing (20 protocols) • ICS OT protocol parsing (70+ protocols)	Controller-based network infrastructure integration • Juniper Mist • Cisco ACI, Cisco Meraki	Agentless inspection macOS, Linux (SSH)
Flow analysis • NetFlow • Flexible NetFlow • IPFIX • sFlow	Private cloud (virtual infrastructure) integration • VMware	Nmap
DHCP requests (via ip helper)	Public cloud integration • AWS • Azure	SNMP queries to endpoints
HTTP user agent (via URL redirect)	Query directory services (LDAP)	Agent-based inspection (SecureConnector)
RADIUS requests	Query web applications (REST)	
MAC OUI	Query external databases (SQL)	
	Orchestrations (ITSM, UEM, EPP, EDR, VA)	

Figure 3: Forescout device visibility methods

The Advantages of Multiple Device Visibility Methods

Because it offers many different discovery methods that are easily configured at set-up (and easily modified afterward), the Forescout platform is uniquely flexible, efficient and effective.

Cost-effective, simplified deployment in large environments: The ability to choose from 20+ active and passive techniques provides flexibility to gain full device visibility in any heterogeneous network, regardless of network complexity, size or number of remote locations – all without the need for infrastructure (software /hardware) upgrades

or deploying a local appliance at every remote site/office.

No blind spots: It is not uncommon for enterprise customers to have remote locations that can't deploy additional appliances or provide SPAN traffic. Our ability to leverage multiple passive and active techniques addresses any network limitations and provides 100% device coverage without blind spots.

Passive-only discovery, classification and assessment for critical healthcare and OT/ICS networks: Critical networks are often inappropriate environments for active probing and scanning techniques that could potentially disrupt medical and process control systems. The Forescout platform provides device visibility across critical healthcare and OT networks through a combination of entirely passive techniques, including monitoring SPAN traffic for deep packet inspection across more than 150 IT, healthcare and OT-specific protocols. What sets the Forescout solution apart is that once it accurately identifies devices, it can selectively apply active methods on specific devices for additional assessment without risking business disruption.

Insight beyond discovery – classification and assessment: The ability to layer passive and active profiling techniques allows the Forescout platform to do much more than simply identify a connecting device by MAC and IP address. Classification is the process of acquiring and correlating many layers of context to create a richly detailed profile of each device. Assessment is the process of comparing discovered device-state properties against security policies as the basis for access control and remediation decisions. Both methods deserve closer examination.

Intelligent Auto-Classification

The complete context for every device is key to granular policy creation. You need to know each device's operational purpose to decide how it is best secured and managed. The growth and diversity of devices make manually gathering this context nearly impossible, and creating policies without proper context puts operations at risk. Forescout auto-classifies traditional, IoT and OT devices using a multi-dimensional classification taxonomy to identify device function and type, operating system and version, and vendor and model.

The platform auto-classifies:

- More than 575 different operating system versions
- Over 5,700 different device vendors' products and models
- Healthcare devices from over 400 medical technology vendors
- Thousands of industrial control and automation devices used across manufacturing, energy, oil and gas, utilities, mining and other critical infrastructure industries

The Forescout Device Cloud powers the platform's auto-classification, ensuring this rich source of context continues to keep pace with device growth and diversity. As the world's largest data lake of crowd-sourced device intelligence, the Device Cloud provides a cross-industry single source of truth for fingerprints, behavior and risk profiles of all unique assets on your network by analyzing more than 12 million enterprise customer devices. Forescout Research publishes new profiles frequently to improve classification efficacy, coverage and velocity across your entire device landscape.

Agentless Posture Assessment and Auto-Remediation

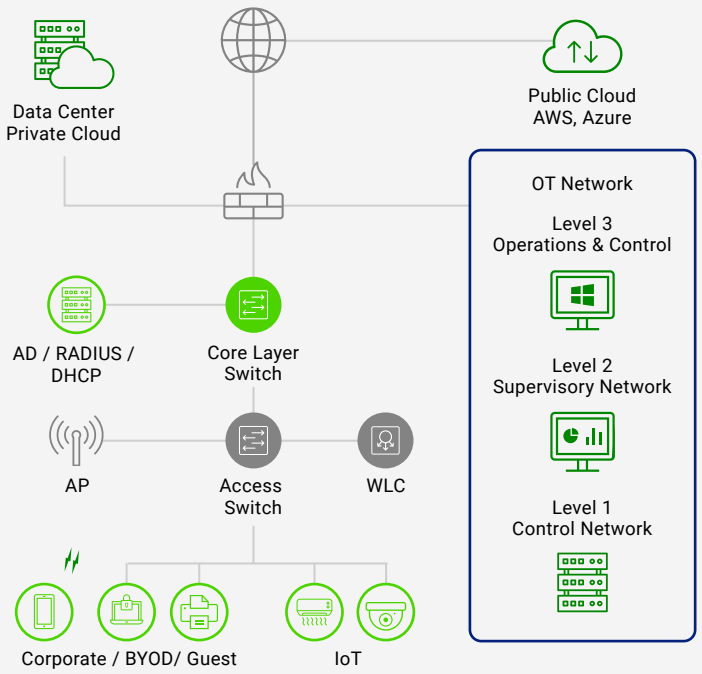
Device classification delivers operational context as to the purpose of a device—in effect, telling you what that device is. For a complete context, however, another lens is required in order to gauge the health and hygiene of each device. Forescout continuously monitors the network and assesses the configuration, state and security posture of connected devices to determine their risk profiles and whether they adhere to security and regulatory compliance policies. It answers critical questions, including:

- Are devices running approved operating systems, including the latest OS patches?
- Is security software installed, operational and up to date with the latest patches?
- Are any devices running unauthorized applications or violating configuration standards?
- Are devices using default or weak passwords (a particular risk for IoT devices)?
- Have rogue devices been detected, including those impersonating legitimate devices via spoofing techniques?
- Which of your connected devices are most vulnerable to the latest threats?

After answering these critical questions, the **Forescout platform enforces device compliance by automating device remediation** using native or third-party controls. Important capabilities include:

- Ensuring endpoints are properly configured and initiating remediation for critical configuration violations, including weak or default passwords
- Continuous assurance that security agents are functioning properly (installed, running and up to date)
- Disabling or blocking unauthorized applications that could introduce risk or put an unnecessary burden on network bandwidth or resource productivity
- Identifying high-risk vulnerabilities and missing critical patches and initiating remediation actions
- Proactively targeting remediation actions such as installing required security software, updating agents or applying security patches
- Implementing policies and automating controls for configuration compliance in cloud deployments, including AWS, Azure and VMware

Device Classification and Assessment



WHO?
- User
- Name
- Email
- Title
- Group
- Subscription/Account
- IAM Owner/Role

POSTURE?
- Apps
- Services
- Processes
- Versions
- Registry
- Patches
- Encryption
- Antivirus

WHAT?
- Function
- OS
- Vendor/Model
- IP Address
- Browser Agent
- Ports
- Virtual/Physical
- Mac Address

WHERE?
- Switch
- Controller
- Switch Port/SSID/VLAN
- AWS/Azure
- Region
- VNet/VPC
- Purdue Level

Figure 4: The Forescout platform quickly classifies devices by type, clarifies whether they are corporate-managed, unmanaged, IoT/OT, physical or virtual, and helps you assess their compliance status.

"IoT and network-enabled device technologies have introduced potential compromise of networks and enterprises. Each device introduces new avenues of code and assets that security teams must track and treat as untrusted infrastructure. Security teams must isolate, secure, and control every device on the network, continuously." [2]

FORRESTER

JUNE 8, 2020

Using Visibility to Enable Control

Every customer's networks are different. That's why their requirements vary, and security policies are unique. And that's why it's critical to deploy a flexible solution to secure all wired, wireless and VPN networks. For example, large enterprise customers commonly deploy Forescout's **non-802.1X solution on their wired networks**. They choose this option because it is easy to deploy, doesn't require hardware/software infrastructure upgrades or complex switch or endpoint configurations such as with 802.1X, and works in single or multivendor network infrastructure. This practice is consistent with Gartner's recommendation of using non-802.1X on wired networks for more straightforward deployment and lower operating costs. However, on wireless networks, it is standard practice to deploy 802.1X for authenticating corporate user-based IT devices. Forescout's hybrid and flexible deployment options easily support both of these best practices.

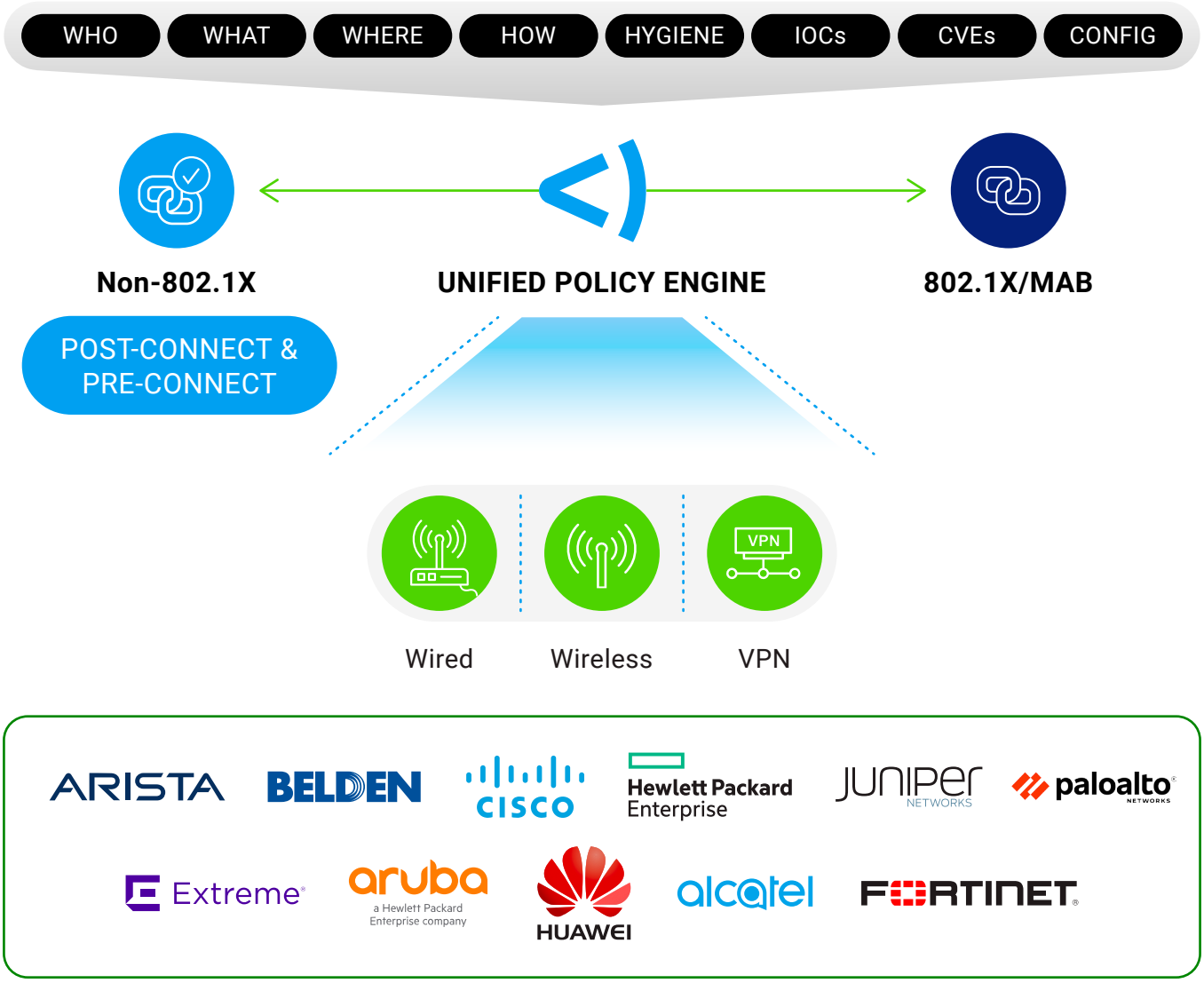


Figure 5: Forescout offers non-802.1X and 802.1X options for securing endpoints on multivendor wired, wireless and VPN networks.

Here are some of the key benefits of using the Forescout platform for securing network access:

Greater Flexibility

- Wide range of access control methods – with or without 802.1X
- Robust non-802.1X wired architecture – non-disruptive, easy to deploy, minimal configuration requirements, no infrastructure upgrades, post-connect and pre-connect options, rapid time to value and faster return on investment
- Unified policy engine to implement differentiated (guest, BYOD, corporate, IoT) and Zero Trust secure access

No Upgrades

- Works with existing infrastructure without software/hardware upgrades
- Works with your network infrastructure vendor of choice (e.g., switch, wireless controller, IaaS), reducing vendor lock-in
- Faster time-to-value and return on investment

Heterogeneous

- Direct integration (via SNMP, SSH, Telnet, RADIUS) with hundreds of switches and wireless controllers with different OS versions from 30+ network infrastructure vendors, allowing for network access enforcement in any multivendor network
- Flexible and non-disruptive solution lowers deployment, maintenance and operational costs
- Heterogeneous support enables an acquiring company to rapidly gain visibility and control into assets following a merger/acquisition

Enterprise-Wide Segmentation

- Leverage the Forescout platform's visibility insights to understand the segmentation state in real-time on any device, anywhere
- Design and simulate logical segmentation policies so you can gauge impact before enforcement
- Monitor segmentation hygiene in real time and respond to policy violations across the extended enterprise

Learn more about Forescout's enterprise-wide segmentation solution here.

BEST PRACTICES FOR NAC DEPLOYMENT

Forescout recommends these best practices for deploying NAC:

Wireless Network: 802.1X is a standard practice for authenticating corporate user-based IT devices on wireless networks. Once authenticated, Forescout identifies and agentlessly assesses device compliance for Windows, macOS and Linux-based computers. With Forescout's policy engine, customers can choose to auto-remediate and enforce appropriate network controls to comply with security policies (for example, notify the user, remediate, block and/or share context with third-party tools).

Wired Network: On wired networks, Forescout recommends non-802.1X architecture. Due to the complexity of deploying and managing 802.1X and MAB on wired networks, most customers choose a non-802.1X option. Customers start with device discovery, identification and posture/compliance assessment, and then enforce appropriate levels of network access using non-802.1X-based controls in any heterogeneous network. Note: Forescout fully supports 802.1X on wired networks as well.

Orchestrate with IT and Security Products

Throughout the network access control process, Forescout can work with your existing tools to exchange real-time device context and automate response workflows. Not only does this accelerate risk mitigation, it allows you to maximize the ROI from existing security and IT management investments. Through our out-of-box eyeExtend integrations and eyeExtend Connect App, we help customers quickly turn siloed security management into an automated, enterprise-wide response system that actively defends your Enterprise of Things.

Here are some of the benefits of orchestrating with existing security tools during the NAC process:

Share Device Context

- Share device context with your existing asset management tools to help ensure you always have the most up-to-date and accurate inventory (CMDB).
- Provide real-time device context to security operations teams and applications for incident correlation and prioritization

Initiate On-Connect Workflows

- Existing tools may miss the vulnerability assessment of transient devices due to point-in-time scans. Forescout works with security tools to trigger real-time vulnerability scans at connection time.
- Initiate patching and security updates immediately upon connection to reduce the attack surface

Assess Security Posture

- Verify existing security agents are functional and identify devices with risks and IoCs
- Detect stale or illegitimate privileged accounts on connecting devices

Automate Response Actions

- Contain, quarantine or block vulnerable, compromised and high-risk devices
- Initiate policy-based mitigation and remediation actions for incident response

> **Forescout currently dominates the agentless subset of the NAC market with 64.7% market share and is estimated to also account for the largest percentage of hybrid NAC deployments in the industry. This growth is largely due to Forescout's strong feature set focused toward meeting the demands of the higher growth portion of this market of unmanaged and un-agentable devices which require an agentless approach.**
>
> **IDC**
> **MAY 2020**[3]

Don't Just See It. Secure It.

Forescout's modern NAC solution offers an agentless, flexible and non-disruptive path to Zero Trust security. Check out these resources to learn more about how Forescout provides active defense for the Enterprise of Things:

Read Gartner's Market Guide for NAC: Learn why Gartner calls Forescout "One of the most popular NAC solutions in the market."

Visit Forescout's website: Learn more about Forescout's modern NAC solution, including the use cases it addresses, how it helps ensure device compliance and what Forescout customers have to say.

Take a test drive: Experience the before-and-after difference of the Forescout platform with a hands-on test drive that takes you through six powerful use cases.

Request a demo: Visit the Forescout demo page to request a personal demo and access a full complement of on-demand demos and video options.

1. The Zero Trust eXtended Ecosystem: Networks Strategic Plan: The Security Architecture And Operations Playbook, Forrester Research, January 2, 2019
2. Forrester Research, Mitigating Ransomware With Zero Trust: Bolster Your Defenses With Zero Trust Principles And Techniques, June 8, 2020
3. IDC, Worldwide NAC Market Shares, 2019: Diverse Market Demands Expand NAC's Addressable Market, May 2020

Don't just see it. Secure it.

Contact us today to actively defend your Enterprise of Things.

forescout.com/solutions/network-access-control salesdev@forescout.com toll free 1-866-377-8771

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