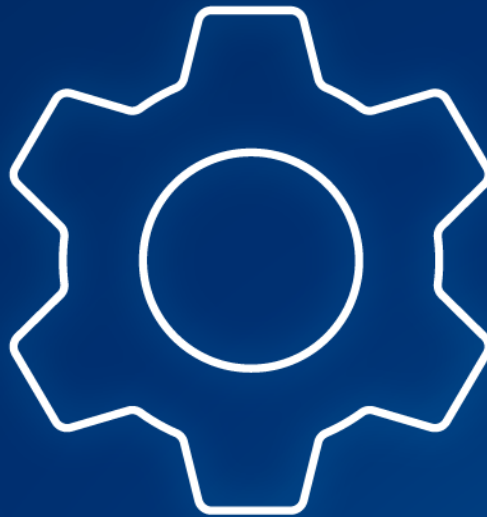


SOLUTION BRIEF

Intelligence and Control for Un-agentable Assets

Eliminate Blind Spots With Forescout's Comprehensive
Device Visibility



 **FORESCOUT®**

Intelligence and Control for Un-agentable Assets

Eliminate blind spots with Forescout's Comprehensive Device Visibility

Without agentless visibility that includes real-time contextual awareness of every device on the network, companies are forced into a reactive defense posture that's best described as security whack-a-mole. The Forescout 4D Platform™ provides 100% visibility of all devices all the time – with or without agents – to proactively identify, segment and enforce security across the Enterprise.

Challenges

Your network is changing. Fast. An explosion in device numbers and diversity has radically altered the device landscape. Internet of Things (IoT) devices and operational technology (OT) environments now connect to the corporate network. Many employees work from home, and some connect to the cloud in an effort to do more with less.

Simply put, **the modern enterprise has quickly evolved into an enterprise city 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
- Mobile, BYOD and work-from-home employees make agent-dependent security a time-consuming, futile security strategy
- IoT devices and OT systems – today's fastest-growing categories of devices joining networks – don't support agents
- Agent-based protection creates rogue-system and cybercriminal-friendly blind spots on your network

“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 featureset 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 2020¹

The Solution

The Forescout 4D Platform™ lets you continuously see every IP-connected device across the growing Enterprise of Things and proactively respond to security posture changes in real time. It deploys quickly on any heterogeneous network – with or without 802.1X.

- **Choose from 20+ active and passive techniques** and gain the flexibility to mix and match discovery and assessment methods to meet your business needs
- **Obtain complete coverage across all locations**, networks and device types – physical and virtual
- **Give security operations and IT staff complete visibility of IoT and OT systems** as well as mobile and work-from-home devices
- **Flexible and non-disruptive** – choose centralized, distributed or hybrid deployment options that run on your existing infrastructure – without upgrades, deployment delays or vendor lock-in
- **Share visibility insights and automate workflows** with other leading security and IT management solutions to dramatically reduce mean time to detect and respond while increasing ROI from existing tools

**WHO ARE YOU?**

- Employee
- Partner
- Contractor
- Guest

**WHO OWNS YOUR DEVICE?**

- Corporate
- BYOD
- Rogue

**WHAT TYPE OF DEVICE?**

- Windows, Mac
- iOS, Android
- Virtual machine
- Non-user devices, IoT, OT

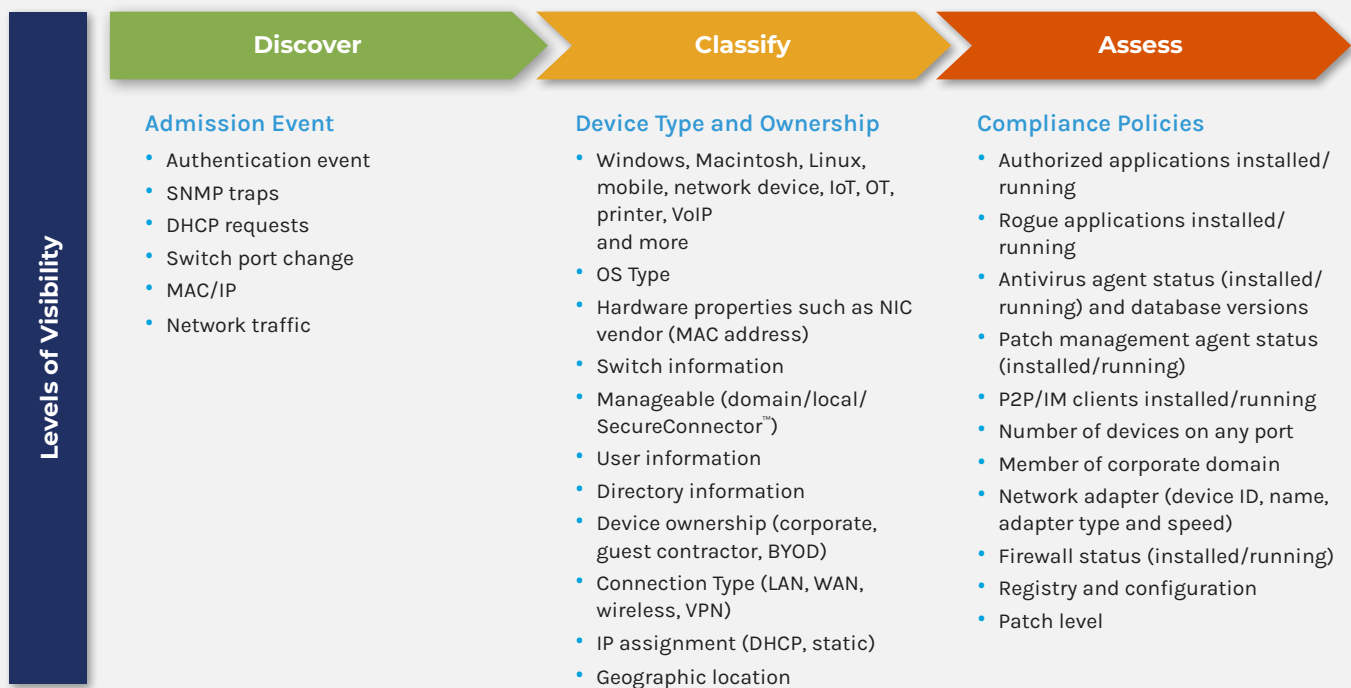
**WHERE/HOW ARE YOU CONNECTING?**

- Switch/Port/PoE
- Wireless/Controller
- VPN
- IP, MAC
- VLAN

**WHAT IS THE DEVICE HYGIENE?**

- Configuration
- Software
- Services
- Patches
- Security Agent

Agentless discovery and classification are essential first steps to knowing who and what is connected to your evergrowing Enterprise of Things. The Forescout 4D Platform™ answers essential questions about connected devices and continuously monitors their compliance status to enforce policy-based access control.



Accurate, in-depth visibility requires three core capabilities: discovery, classification and security posture assessment. The Forescout 4D Platform™ continuously assesses devices, providing exceptional detail in these categories that is always up to date.

Auto-classify New Devices and Understand Risks

Auto-classifying devices and understanding which types are vulnerable to threats are essential for creating security policies for network access, device compliance and network segmentation. However, the explosive growth in new device types and operating systems joining enterprise networks makes it challenging to identify, assess and classify these devices – particularly IoT devices and OT systems that don't support software agents.

The Forescout 4D Platform™ leverages the **Forescout Device Cloud**, the world's largest data lake of crowd-sourced device intelligence. It provides a cross-industry single source of truth on the device fingerprints, behavior and risk profiles of

all unique assets on your Enterprise of Things by analyzing more than 12 million enterprise customer devices.

Gain an Accurate Inventory of Every Connected Device

By providing comprehensive visibility and an accurate, real-time inventory of what's on your network, the Forescout 4D Platform™ gives you the tools to understand business risks better and make spot-on security and business decisions about your networked assets.

- **Avoid manual, error-prone and expensive inventory processes.** Automate asset database/configuration management database (CMDB) updating while eliminating time-consuming manual inventorying.
- **Enhance operational efficiency.** In addition to feeding the CMDB with real-time asset intelligence, the Forescout integration with ServiceNow® lets you automatically create an IT or security incident record to automate remediation/workflows.
- **Accelerate incident response.** IT service and security operations teams need rich device context to prioritize and remediate issues – quickly and with confidence. The Forescout 4D Platform™ provides rich visibility and enables policy-driven remediation.

“We started implementation at lunchtime and when I fired up my computer that evening, 97 percent of our environment had already been discovered and classified. Within seven hours, we had detailed visibility of our global environment.

That's impressive.”

—Joseph Cardamone, Sr.
Information Security Analyst
and N.A. Privacy Officer,
Haworth International

Visualize Device Intelligence in Real Time

The Forescout 4D Platform™ provides your security operations and incident response teams with a consolidated, real-time view of your device landscape along with classification, connection and compliance context. The Forescout Device Intelligence Dashboard is easily customizable for other IT functions such as risk, compliance and executive reporting.



How Our Agentless Visibility Adds Value to Your Business:

By providing comprehensive visibility and an accurate, real-time inventory of what's on your network, the Forescout 4D Platform™ gives you the tools to understand business risks better and make spot-on security and business decisions about your networked assets.

- 1 Non-disruptive deployment lets you maintain user productivity/critical business services.
- 2 Accurate visibility and posture assessment reduce risks of security breaches and business disruption.
- 3 Accurate visibility enhances network security while helping you demonstrate compliance.
- 4 Increase security operations productivity with context-aware, real-time device visibility and security automation.
- 5 Agentless posture and risk assessment: no agents to deploy, manage or repair.
- 6 Rapid time to value: gain 100% device visibility in days.
- 7 Vendor-agnostic: use your existing infrastructure and tools.
- 8 No forced software or hardware upgrades.
- 9 Flexible deployment across heterogeneous networks: no vendor lock-in.
- 10 Plug-and-play integrations with leading IT and security products boost ROI.
- 11 Avoid 802.1X complexity, deployment delays and operational costs.
- 12 Move from complete visibility to control, segmentation and Zero Trust.

Take the Next Step:

- Request a [Forescout Demo](#)
- Read our [Agentless Visibility and Control white paper](#)

¹ IDC, Worldwide NAC Market Shares, 2019: Diverse Market Demands Expand NAC's Addressable Market, May 2020