FIVE STEPS

TO SMARTER NETWORK SECURITY IN AN AI-DRIVEN ERA

A FORESCOUT eBOOK

TABLE OF CONTENTS

MEET THE Forescout 4D Platform™

The Forescout 4D Platform™ makes all five steps operationally achievable:

DISCOVER.
Real-time visibility into every connected asset across IT, OT, IoT, and IoMT.

ASSESS.
Continuous risk scoring that prioritizes what to fix first, enriched by Vedere Labs threat intelligence and third-party integrations.

CONTROL.
Automated policy enforcement and dynamic access control that keep threats from becoming breaches.

GOVERN.
Centralized policy management and continuous compliance evidence that proves it at scale.

It's not a question of whether or not your organization will be targeted. It's whether you'll see the attack coming.

The attack surface is expanding faster than most security teams can track. Enterprise networks now combine traditional IT devices with smart IoT sensors, operational technology assets that interact with the physical world, and medical devices that cannot tolerate disruption. According to Forescout Research – Vedere Labs, the riskiest devices in 2026 span all four of these categories: IT, IoT, OT, and IoMT. Attackers are deliberately crossing between them, using one environment to gain access to another. Focusing security on a single domain is not enough.

Unmanaged assets are hiding in the gaps between your tools. Attackers target them precisely because they know that you can't secure what you can't see. **And soon: frontier AI models. Claude Mythos, anyone? Volume and scale have new meaning. But the fundamentals remain the same. The network continues to be the immutable source of truth.**

Protecting against today's threats requires a different approach, one built on total visibility across every connected asset, continuous verification of every device's compliance and risk posture, and the ability to respond at the speed threats actually move. That destination has a name: **Universal Zero Trust Network Access (UZTNA**). Unlike traditional zero trust approaches that focus primarily on remote users and managed endpoints, UZTNA covers every asset type, managed and unmanaged, across IT and OT, IoT and IoMT. UZTNA enforces adaptive, least-privilege access policies based on real-time context, regardless of where a device connects or whether it supports an agent.

The five steps in this guide are the operational path to that posture.

STEP 1: KNOW WHAT YOU HAVE

Visibility and asset management lay the foundation for network security. You need to know what is connected, who uses it, where it is located, and what it communicates with.

Ask yourself: how many asset inventories do you have today?

You have endpoint tools. But today's attackers are targeting smart sensors in power-generating stations, IP cameras in retail locations, industrial controllers on assembly lines, and connected medical devices in clinical environments. These assets rarely support agents. They do not appear in your endpoint tools. So, they represent a significant portion of your real attack surface.

To fully understand your exposure, you need discovery methods that work across every asset type and every environment, including OT environments where passive, non-intrusive monitoring is the only safe approach.

Partial visibility = partial protection. If you want a single source of truth for 100% of network-connected devices, ask the network.

The Forescout 4D Platform™ uses 30+ active and passive discovery methods to deliver complete visibility across IT, IoT, OT, and IoMT environments. Assets are automatically classified based on deep device context, tracked over time, and surfaced in a single console across every location. Because you can't secure what you can't see. And seeing everything is where every other step begins.

DISCOVERY ACROSS EVERY ENVIRONMENT

The Forescout 4D Platform™ discovery methods fall into four categories:

» **Network integrations.** Connecting routers, switches, and wireless controllers provides asset discovery and critical contextual data across globally dispersed networks.

» **Network traffic monitoring.** Passive sensors perform deep packet inspection and identify device behavior without disrupting operations, essential in OT and clinical environments.

» **Scanners.** Active probing improves classification and uncovers information not visible through passive monitoring alone.

» **Third-party integrations.** APIs and data sharing with existing security and IT tools enrich asset intelligence and close inventory gaps across the environment.

CASE STUDY: "HOW BIG IS MY ATTACK SURFACE?"

A U.S. energy company came to Forescout trying to answer the question, "How big is my attack surface?"

As a baseline, the company only had visibility into its 50,000 agentable assets using Windows Defender and CrowdStrike. Over two years, they spent countless hours combining inventories from 32 separate security and IT tools. From this fragmented approach, they could identify closer to 200,000 connected devices - a substantial increase, but what if there was still more to discover?

Forescout was able to deploy in this environment and identify just over 235,000 total assets without deploying software agents, providing a single source of truth in only a few weeks' time. These previously unknown assets represented a 15% visibility gap over all previous security tools combined and an 80% gap over agent-based solutions. A gap like this poses a significant security risk that attackers can use to exploit vulnerabilities and infiltrate networks.

STEP 2: UNDERSTAND YOUR RISK

Visibility tells you what is on your network. Assessment tells you what to do about it.

Knowing an asset exists is only the beginning. Without understanding its vulnerabilities, configuration gaps, behavior, and operational criticality, security teams are left treating every alert and vulnerability equally. In an environment with thousands of connected assets across IT, OT, IoT, and IoMT, that approach fails fast.

Traditional vulnerability management makes this harder, not easier. It is built around known CVEs and managed endpoints. It does not account for unmanaged IoT devices without a patch path, OT assets running outdated firmware, or medical devices whose criticality makes any disruption unacceptable. Risk is not equal across your environment, and your assessment approach needs to reflect that.

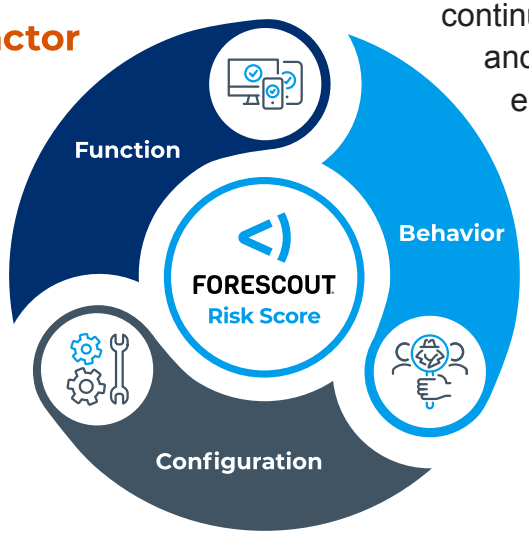
Visibility without risk context is just inventory. The goal is actionable intelligence.

71%

actively exploited vulnerabilities in 2025 were not in CISA Known Exploited Vulnerabilities catalog

Forescout Multifactor Risk Score

1. **Configuration:**
   - Vulnerabilities (CVE's)
   - Exploitability (EPSS)
   - Exposed Services
2. **Function:**
   - Device Criticality
3. **Behavior:**
   - Internet Exposure



$$\text{Risk Score} = f(\text{Detected Risk Indicators}, \text{Device Criticality})$$

The Forescout 4D Platform™ assesses every discovered asset continuously, correlating vulnerabilities, device criticality, and behavioral indicators into a multifactor risk score for each asset, updated dynamically as the environment changes. That score is what separates prioritization from guesswork: remediation efforts focus on the assets that pose the greatest actual risk, based on exploitability, business impact, and exposure context. This is continuous exposure management in practice: not a quarterly vulnerability scan, but an always-current view of which assets combine real exploitability. For devices that cannot be patched, the risk score informs compensating controls directly.

Critically, this assessment loop does not stop at reporting. When a device's risk score crosses a defined threshold, it can trigger an automated policy response. Assessment and control are not separate workflows. In the Forescout 4D Platform™, they are part of the same continuous loop.

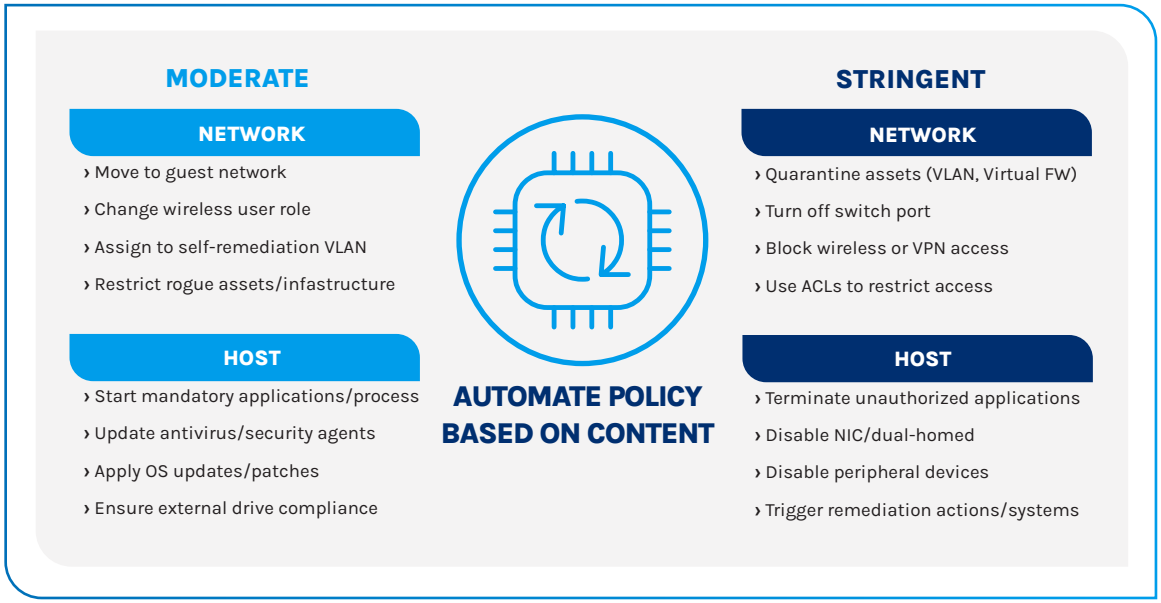
STEP 3: CONTROL NETWORK ACCESS

Knowing what is on your network and understanding its risk sets the stage for the most fundamental question in network security: what should actually be allowed on your network, and what should not?

Controlling access is not simply a matter of authentication. Many assets connecting to enterprise networks today, OT sensors, IoT devices, medical equipment, building automation systems, have no concept of a user identity to authenticate. Traditional approaches, such as 802.1X with MAC address bypass lists, reduce access control to a credential that is trivially easy to spoof.

If you can't verify an asset's compliance with your security policies, it doesn't belong on your network.

A better approach assesses compliance and risk posture before granting access, then continuously reassesses. A device that was compliant yesterday may not be compliant today. This is the operational meaning of Universal Zero Trust Network Access: not a one-time gate, but continuous verification applied to every asset, regardless of type or location.



The Forescout 4D Platform™ enforces UZTNA through policy-based controls that scale from notification through to full restriction, applying equally to managed and unmanaged assets across IT, OT, IoT, and IoMT with no agent required. And because access decisions are informed directly by the risk scores established in Step 2, policy enforcement adjusts automatically as a device's risk profile changes.

STEP 4: LIMIT MOVEMENT AND COMMUNICATION

Controlling which assets access your network is essential. Controlling what they can reach once they are on it is what contains a breach when one occurs.

When an attacker exploits a foothold, their objective is to move toward something worth extorting:

Flat, under-segmented networks make that journey short. Access control is the first line of defense. Segmentation is structural reinforcement.

The question is not whether an attacker can get in. It is how far they can go when they do.

Effective segmentation starts with understanding how assets are actually communicating. The Forescout 4D Platform™ maps real traffic flows across your environment and lets teams simulate policy changes against actual data before deployment, so segmentation reflects how your network operates, not how you think it does. The same traffic intelligence reveals which high-risk assets are reachable from likely attacker entry points, turning the abstract question of exposure into a concrete map of attack paths worth closing first. Policies apply at macro and micro levels, reducing the blast radius of any incident to the smallest possible scope.

WHY SEGMENTATION PROJECTS FAIL

» **Can't visualize traffic flows before enforcing policy.**

» **Blocking legitimate communication disrupts operations.**

» **Projects stall before implementation.**

Simulating policy changes against real traffic data is what gets segmentation done.

THE INTELLIGENCE BEHIND EVERY STEP: FORESCOUT VISTAROAI™

The four steps you have worked through represent the operational foundation of a strong security posture. Executing them continuously, across thousands of assets, with a stretched team, requires intelligence that works alongside you every day.

That is what Forescout VistaroAI™ delivers.

VistaroAI is embedded across the Forescout 4D Platform. It does not wait for questions or rely on prompts. It applies pre-programmed security skills that continuously evaluate your environment and organize findings into clear, role-specific priorities. SOC analysts focus on event investigation and active threats. Network operators focus on policy enforcement and operational stability. Compliance officers focus on control gaps and compliance validation. Each role sees what they are accountable for, and is ready to be acted on.

VistaroAI recommends. Your team decides. Human judgment stays at the center.

What VistaroAI Brings to Each Step

1 **DISCOVER:**
» Surfaces what has changed and what requires attention.

2 **ASSESS:**
» Translates risk scores into prioritized, role-specific action queues.

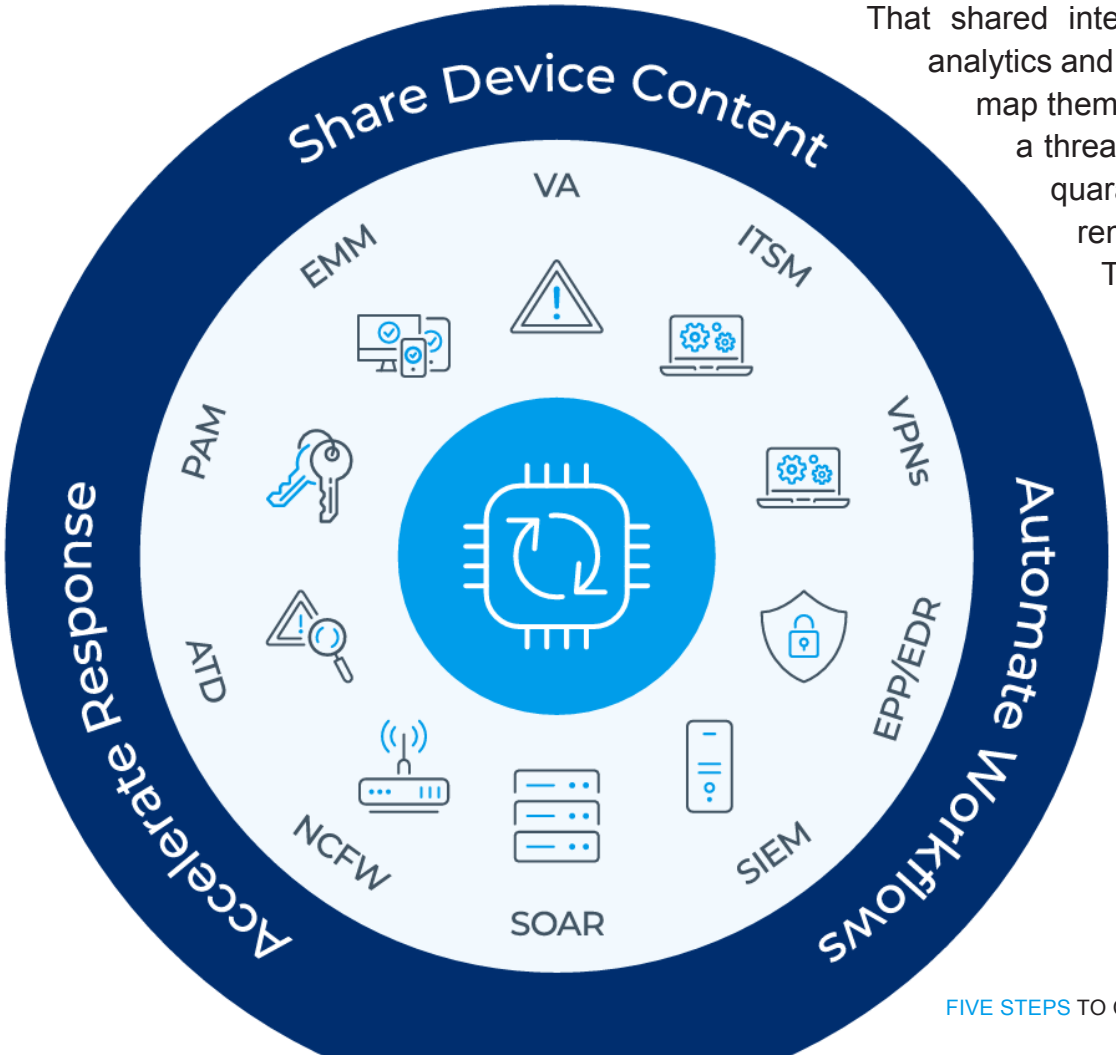
3 **CONTROL:**
» Flags access anomalies and policy violations in real time.

4 **GOVERN:**
» Reveals lateral movement risk and coordinates automated enforcement with human-in-the-loop oversight.

STEP 5: AUTOMATE YOUR RESPONSE — AND GOVERN CONTINUOUSLY

No security team operates from a single tool. The Forescout 4D Platform™ integrates with 180+ security and IT products, sharing asset intelligence and orchestrating workflows across your existing stack. Every tool you have already invested in becomes more effective because it is working from the same real-time asset intelligence.

Attackers automate. Your response should, too.



That shared intelligence drives automated response. Behavioral analytics and Vedere Labs threat intelligence identify threats and map them to known adversary techniques in real time. When a threat is confirmed, response is immediate: devices are quarantined, segmentation is enforced, violations are remediated, without waiting for manual intervention. The result is measurable reduction in time to detect and time to respond.

The controls you think you have are not the controls you actually have. Continuous validation is the difference.

The same continuous monitoring also governs your posture. Control gaps are identified in real time. Compliance evidence is collected automatically.

Audit readiness becomes always-on, not a pre-audit sprint.

PUTTING IT ALL TOGETHER

You can't secure what you can't see. And attackers know exactly where you aren't looking.

The five steps in this guide are how you close those gaps: from visibility and risk assessment, through access control and segmentation, to automated response and continuous governance. Each step builds on the one before it. Together they deliver a continuously operating security posture, not a one-time project.

Your journey to Universal Zero Trust Network Access starts here.

The Forescout 4D Platform™ with VistaroAI™ are what make it operational, continuously, across every asset in your environment.

For over 25 years, organizations and governments worldwide have trusted Forescout to secure their networks. From pioneering Network Access Control (NAC) to delivering Universal Zero Trust Network Access (UZTNA), Forescout leads the evolution of enterprise network security across IT, OT, IoT, and IoMT environments. The Forescout 4D Platform™ delivers comprehensive asset intelligence, continuous risk assessment, and dynamic control, over all managed and unmanaged assets, enhanced by the proprietary threat intelligence research of Vedere Labs. Leveraging agentic AI workflows with human-in-the-loop actions, Forescout continuously analyzes threats, orchestrates response, and integrates seamlessly with 180+ security and IT products.

FORESCOUT

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771 Tel (Intl) +1-408-213-31911 Support +1-708-237-6591
Learn more at Forescout.com