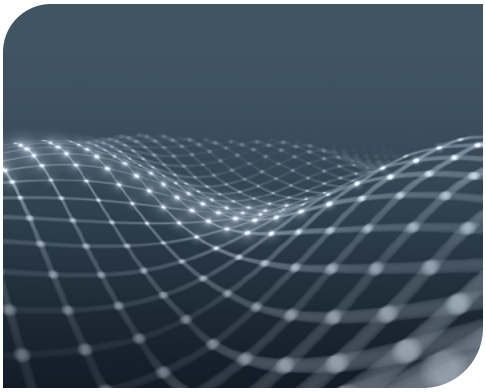


Forescout Continuum Platform

Align Your Digital Reality and Your Security Framework

Digital transformation has led to explosive growth in IT, IoT, IoMT and OT/ICS assets connecting to organizational networks. Innovations such as remote access, distributed operations and mobile workforces have improved efficiency – while expanding the cyberattack surface. This is your digital reality: the sum of everything connected to your network, from campus to cloud and data center to edge.

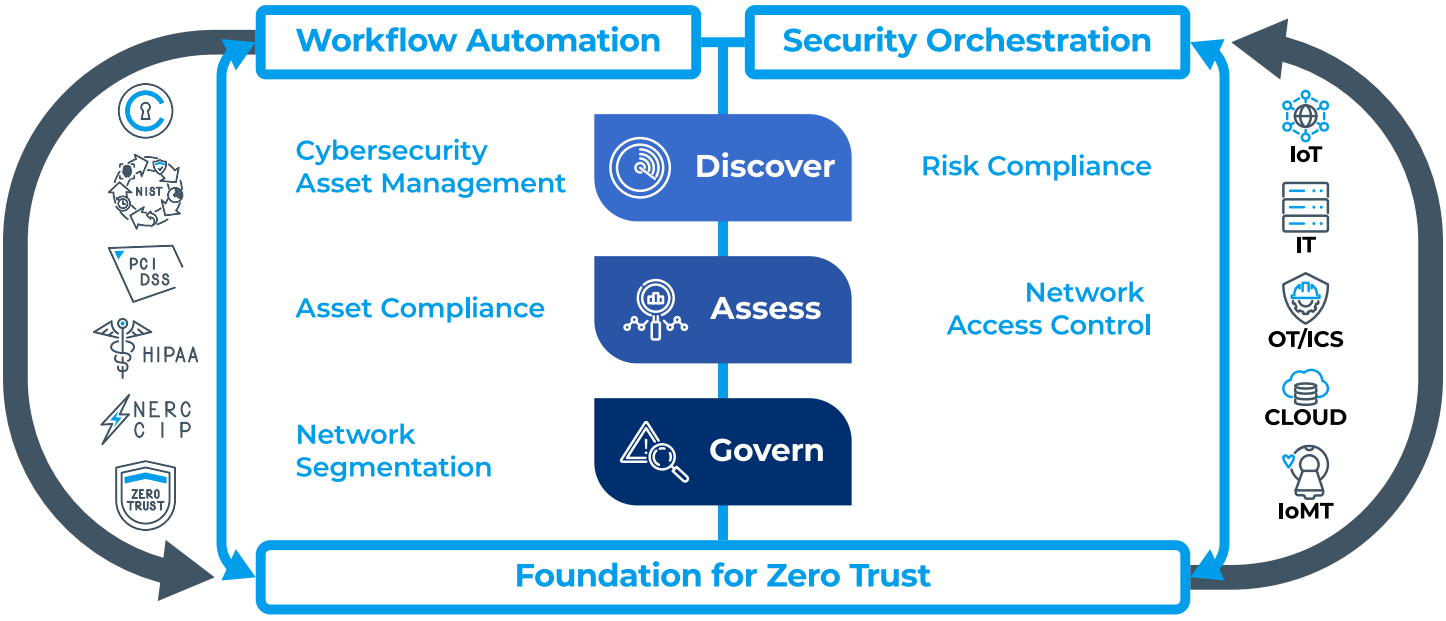
Every organization also has its own security framework – a mix of industry best practices, board mandates and regulatory requirements, combined with your security policies and risk management practices. The goal is for your digital reality to align with your security framework.

Unfortunately, constant changes drive your digital reality out of alignment with that framework. They include everyday changes such as device decay, software failure and staff turnover as well as mega events like corporate mergers and acquisitions, which can introduce massive change all at once.

These changes constantly widen the gap in security risk posture, which translates into business risk: your next disruption, audit failure, operational safety concern, or production outage. Meanwhile, the security talent pool is shrinking, and IT teams are stretched thinner than ever.

You can't expect to eliminate risk. But you absolutely can manage it with a platform that automatically and continuously addresses this gap and keeps you in alignment.

Forescout Continuum



"Forescout is a **force multiplier**. The **visibility and automation** ability that it gives the security department, it's **invaluable**."

— CISO, major Florida medical center

Every environment is different, but the steps to aligning your digital reality with your security framework follow the same continuum:

Cybersecurity asset management: What is connecting to your ecosystem and where it is located, physically and logically? Visibility is the foundation – you can't protect what you can't see.

Asset compliance: Is the asset agentable? If so, are the correct agents installed and configured correctly? Who's logged in? Are unauthorized applications running? You must be certain that assets are in the desired state.

Risk compliance: Is the asset critical to the business? Is it vulnerable? Is it operating as expected? You can't remediate what you aren't aware of.

Network segmentation: What are the asset's communication habits? What other asset types does it communicate with, over what ports and protocols? Context-aware segmentation policies can reduce the attack surface without disrupting desired communication flow.

Network access control: Should communication be limited or blocked? Proactive controls can authorize access and assign users and devices to network segments or quarantine devices based on their security posture.

Security orchestration: What insights can we obtain about the asset from other cybersecurity solutions? Is the asset properly patched? Is malware present? You can't make sound decisions without all available information.

Workflow automation: What's the right action or chain of actions? You want to use collective insights among security products to drive the right actions through automated ticketing, automated cyber asset management, automated remediation and so on.

These steps are straightforward in theory but not in practice. Most IT teams cannot assess all devices in real-time and confirm that each is compliant. You've invested in potentially dozens of security tools to manage your network, but that means information is fragmented, and you lack a single source of truth. Outdated, point-in-time snapshots can't be trusted. Even if you could identify noncompliant devices, you have limited capacity to apply policy controls and enforce continuous compliance across a mix of network and security infrastructure technologies.

You need a single platform that automates every step in the cybersecurity continuum. You need a force multiplier.

Discover – Assess – Govern

The Forescout Continuum Platform automatically aligns your digital reality with your security framework by automating the discovery, assessment, and governance across all cyber assets in your environment.

Discover

and inventory all cyber assets on your network, continuously.

Complete cybersecurity asset management requires continuous discovery and classification of every device across your IT, IoT, OT, and IoMT landscape. Beyond knowing how many assets are connecting, you need to know what they are, how they're connected (wired/wireless), where they're located physically (building, closet, switch, port), and logically (VLAN, IP address), and what their purpose is.

Forescout is the only vendor that offers continuous discovery of all cyber assets using more than 30 active and passive techniques, including passive deep packet inspection of sensitive OT/ICS and IoMT assets. Forescout Continuum also uses out-of-the-box wireless, switch, and VPN integrations to discover all assets, whether they are communicating or not, across all locations and networks.

Data collected from these techniques is referenced against data about over 15 million devices in Forescout's Device Cloud. In addition, asset classification is enriched with automated context and insights from Forescout's Vedere Labs to supply the most accurate classifications based on more than 150 attributes.

Features

Asset compliance – On-connect, agentless validation of cyber asset state against security frameworks to ensure security investments are deployed and running

Risk identification and prioritization – Real-time, multi-faceted risk analysis and mitigation for all connected cyber assets based on asset trends and threat feeds

Asset grouping and traffic flow mapping – Dynamic grouping of cyber assets by type and role to map traffic flows and cross-talk between groups

Actionable insights from the world's largest device cloud database

Forescout's Device Cloud is enhanced with advanced machine learning to deliver actionable insights and real-time knowledge and activity from Forescout's millions of assets under management. Vedere Labs, Forescout's threat intelligence and research team also leverages the Device Cloud for advanced intelligence to alert customers and the broader security community about emerging risks.

Assess

cyber asset compliance and risk hygiene, continuously.

Given the broad range of asset types in every organization, assessing compliance requires various passive discovery and active scanning or integration techniques. Security teams typically rely on dozens of risk assessment products to accommodate every need. But who is watching the watchers?

Forescout Continuum is the only platform that continuously identifies and mitigates risk across all cyber assets in your digital terrain. The platform enhances your investment in security tools by helping to ensure they are deployed, configured and working correctly, and orchestrating communication among them.

With cybersecurity asset compliance, it's not enough to ensure your systems and processes are operating in accordance with security frameworks and regulations. You're still subject to failed audits and penalties unless you can prove compliance. With automated device assessment and policy enforcement, satisfying audit and report requirements is a byproduct of continuously compliant security operations.

Cut through the noise with auto-prioritized remediation

Forescout Continuum includes a cloud-based, multi-factor risk scoring service that displays a contextualized list of threats prioritized based on probable impact. The service analyzes risk for every asset on the network across indicators like vulnerabilities, exposed surfaces, open ports, Purdue level, etc., and calculates a single, aggregated score for each. Instead of sifting through 10,000 alerts, you see the 10 alerts that need attention now. By correlating risk scores with traffic flows between devices Forescout Continuum also assesses the blast radius to critical assets.

Features

Proactive remediation – On-connect, agentless validation of cyber asset state against security frameworks to ensure security investments are deployed and running

Risk identification and prioritization – Real-time, multi-faceted risk analysis and mitigation for all connected cyber assets based on asset trends and threat feeds

Asset grouping and traffic flow mapping – Dynamic grouping of cyber assets by type and role to map traffic flows and cross-talk between groups

A strong foundation for zero trust

Zero trust is a security design approach, not a single solution or technology that can be bought through a single vendor. Forescout Continuum sets the stage for zero trust security by automating enforcement of least-privilege access policies based on user, device, connection, posture and compliance for all cyber assets — with or without 802.1X, and without infrastructure upgrades or changes. A centralized policy management and decision point (PDP) for your enterprise-wide zero trust architecture reflects all available information needed to execute the right actions across heterogeneous policy enforcement points (PEPs).

Govern

cyber assets proactively to minimize the attack surface and breach impact, continuously.

Governance requires an array of options for swift mitigation or remediation and knowing which option to use based on all available intelligence. They include automated remediation, network access control, segmentation, CMDB updates and cross-product orchestration. Forescout Continuum automates response workflows to enforce security policies natively and via other security tools using pre-built integration modules. Actions are based on shared device, user and contextual insights for all cyber assets, managed and unmanaged. All the information needed to create granular enforcement policies is at your fingertips.

Business disruption is the quickest way to sabotage your security project. Forescout Continuum enforces flexible mitigation actions, from modest to stringent, to protect vulnerable, high-risk and compromised devices while keeping mission-critical assets online. The platform also lets you simulate policies and monitor traffic flows before turning them on, so you can flag violations that could have unexpected consequences across the network and make changes safely.

Features

Proactive remediation – Misconfigurations fixed upon assessment for continuous compliance without extensive triaging

Accelerated response – Policy enforcement and incident response actions at machine speed to contain threats, minimize propagation and mitigate risks

Automated workflows – Device compliance enforced natively and via orchestration with other security tools

Forescout Continuum builds on 20+ years of Forescout innovations that protect many of the world's largest companies and most trusted organizations in finance, government, healthcare, manufacturing and more.

The platform:

- Builds on a proven solution widely deployed across thousands of companies and government organizations, including 27% of the G2K, to secure the most complex environments at scale.
- Seamlessly integrates with existing network infrastructure using a flexible architecture that scales to edge networks to identify all cyber assets in heterogenous, multi-vendor environments.
- Combines Forescout's existing innovations in agentless and non-disruptive security with new machine learning, cloud-scale risk analysis and cloud-managed sensor architecture.

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com