What's New Forescout 8.1

As the digital transformation continues unabated, organizations are connecting increasing numbers of smart devices to their networks to automate business operations and boost efficiency. Whether IoT, IIoT or OT, these devices bring unprecedented growth and diversity to enterprise networks.

> “By 2021, 70% of OT security will be managed directly by the CIO, CISO or CSO, up from 35% today.”
> *– Gartner, May 2018*

To drive this business transformation, organizations must increase the connectivity and information sharing between previously disparate networks. This is accelerating the convergence of IT and OT, and creates new data flows between campus-connected IT devices, cloud-based applications and operational technology systems. Despite the benefits, this increases business risk, as threat actors can move laterally across newly interconnected networks to access sensitive information or cause business disruption.

The convergence of IT and OT puts new demands on CIOs and CISOs who are now tasked with protecting this entire business ecosystem. IT teams are no longer responsible for just managing user devices, applications and data—they are responsible for running secure and streamlined business operations. To take on this challenge, they need complete device visibility and control.

Forescout 8.1: Unified Device Visibility and Control for IT and OT Security

Forescout 8.1 is the first unified device visibility and control platform for converging IT and OT networks. It enables organizations to gain complete situational awareness of all devices in an interconnected environment and to orchestrate actions that mitigate both cyber and operational risk.

- New capabilities such as visibility into Cisco ACI, Microsoft Azure and Belden industrial switching environments extend coverage across data center, cloud and OT networks, providing organizations the line of sight they need across IT and OT domains.
- Extensive auto-classification enhancements for IoT and OT devices, vulnerability assessment for industrial control systems (ICS) and rogue device detection increase cyber resilience of both IT and OT networks.
- New orchestration capabilities for segmentation with Fortinet firewalls and Cisco DNA-Center, and incident response with ServiceNow extend the ability to automate controls and drive security operations efficiency.
- These capabilities can now be deployed at an unparalleled scale of 2 million devices in a single deployment that spans physical, virtual, cloud or hybrid environments.

Enterprise Scale

Manage 2 million devices in a single deployment spanning physical, virtual, cloud or hybrid environments

Device Discovery

New visibility into Microsoft Azure, Cisco ACI and Belden industrial switching environments, as well as visibility into lower layers of the OT network stack

Auto Classification

New deep packet inspection of over 100 IT and OT protocols powers auto-classification of medical, industrial, building automation and IoT devices

Risk Assessment

New OT and ICS vulnerability assessment, and rogue device detection to identify and stop impersonators helps increase cyber resilience

Control Automation

New orchestration for network segmentation with Fortinet firewalls and Cisco DNA-Center, and incident response with ServiceNow ITSM and Security Operations

Expanded Device Discovery

Security begins by understanding with confidence what is on the network. This means identifying all devices the moment they connect to the network. In 2019, 900 million more physical and virtual devices are expected to be on enterprise networks. The vast majority of this growth is coming from IoT and OT devices, and public and private cloud instances.

> “By 2023, the average CIO will be responsible for more than 3 times the endpoints they managed in 2018”
> – *Gartner, September 2018*

- Forescout 8.1 continues to expand visibility in these areas to provide a unified view of all your devices across campus, data center, cloud and OT networks.
- Multi-cloud visibility now includes Microsoft Azure, adding to existing capabilities for AWS and VMware
- Integration with Cisco ACI provides visibility into SDN environments for data centers
- Integration with the Belden industrial switching portfolio provides expanded visibility into OT networks
- Passive monitoring in lower layers of the OT network stack provides visibility into supervisory, process control and instrumentation devices

Superior Auto-classification

IoT and OT device diversity makes it challenging for organizations to accurately identify and catalog them. Without granular classification, it is difficult to create and enforce targeted policies to secure these devices.

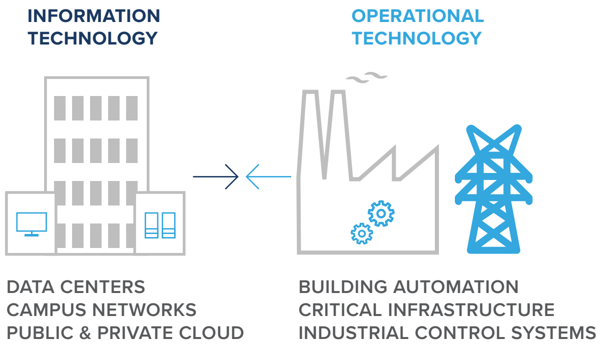
Forescout 8.1 includes extensive enhancements that allow you to auto-classify more of your devices and leverage this context for policy enforcement:

- Expanded coverage to identify more than 500 OS versions and over 5000 device vendors and models
- Healthcare device classification for over 350 medical technology vendors, including the Global Top 20
- New deep packet inspection of over 100 IT and OT protocols to auto-classify thousands of industrial automation devices across manufacturing, energy, oil and gas, utilities, mining and critical infrastructure
- Improved classification efficacy, velocity and coverage powered by the *Forescout Device Cloud* with more than 8 million devices across IT, IoT and OT

Cross-domain Risk Assessment

OT vulnerability assessment

With the growing connectivity between IT and OT networks it is important to understand the risk profile of devices in both domains. Vulnerable devices on either side can be compromised, allowing threats to traverse domains and cause business disruption and financial loss.



- Forescout 8.1 adds OT and ICS vulnerability assessment to existing Windows vulnerability assessment capabilities,
  giving you insight into the high-risk devices on your network
- Frequent updates from Forescout provide up-to-date information about the latest ICS common vulnerabilities and exposures (CVEs) to identify vulnerable devices and orchestrate remediation actions
- For vulnerable industrial and operational devices that can only be patched or remediated within scheduled maintenance windows, Forescout can enforce mitigating controls such as segmenting these devices into “safe” network zones until such time they can be remediated

Rogue device detection

Another challenge due to the explosion of IoT and OT is device impersonation and MAC address spoofing. Threat actors looking to gain access to networks can target a larger pool of MAC addresses since IoT and OT devices are often included in lengthy whitelists for enabling network access. These devices often have unsecured display screens that can reveal their MAC address to the casual passerby. Impersonators can easily masquerade as legitimate devices to access the network and cause disruption or get sensitive information.

Forescout 8.1 includes new patent-pending rogue device detection to identify and stop impersonators using MAC address spoofing techniques.

- Continuous network monitoring detects multiple spoofing scenarios across wired and wireless networks including concurrent connection, same-location replacement and different-location replacement attempts
- Forescout identifies victim and impersonator devices, and based on policy, can block spoofing attempts to prevent malicious access
- Forescout allows you to demonstrate MAC spoofing resilience to auditors and improve audit compliance

Control Orchestration and Automation

IT security teams are inundated with increasing numbers of security and compliance issues reported by security tools that either lack sufficient device context for prioritization or automation capabilities to enforce controls. As a result, highly skilled security teams waste time manually troubleshooting low-impact issues, unable to focus on proactive risk reduction or fast threat response. Forescout 8.1 gives you both the device context as well as the ability to orchestrate actions and automate controls.

> "By 2021, 70% of enterprise organizations will include security automation, orchestration and response capabilities, either through their SIEM or a dedicated platform, up from less than 5% in 2018"
> – *Gartner, December 2018*

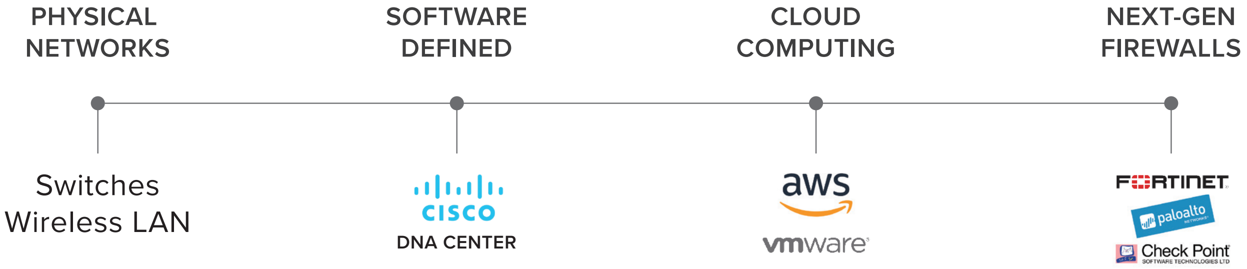
Network segmentation

As organizations define their next-generation security architectures for IoT and OT, segmentation plays a leading role. Unlike traditional devices, IoT and OT devices cannot be regularly patched or secured through agents. Hence, segmenting these devices into logical security zones is an essential risk-mitigation strategy.

ForeScout 8.1 enables you to orchestrate segmentation across multiple enforcement technologies, including several new integrations:

- Automation of segmentation controls with Fortinet firewalls, adding to existing orchestration with Palo Alto Networks and Check Point for heterogeneous support of next-generation firewalls
- Orchestration of segmentation controls with Cisco DNA-Center, adding to existing integrations with software-defined and cloud networking technologies such as VMware NSX and AWS

Cross-domain network segmentation



Incident response automation

IT and security teams are increasingly looking at response automation as a way to tackle low-risk issues so their skilled resources can focus on risk mitigation and other high-impact business outcomes.

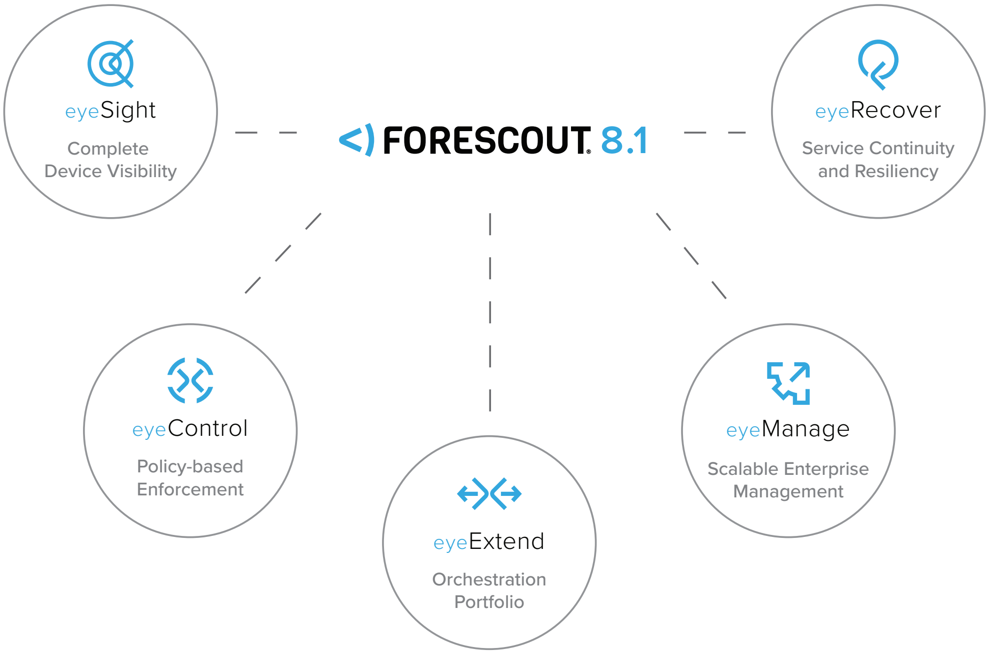
Forescout 8.1 now integrates with ServiceNow ITSM and Security Operations products to automate and accelerate incident response.

- New orchestration with ServiceNow ITSM automates service incident creation and policy-based response for configuration compliance
- New orchestration with ServiceNow Security Operations automates security incident creation and threat response for high-risk or compromised devices
- Enhanced orchestration with Service CMDB updates Configuration Items (Cis) after incident remediation is completed to facilitate closed-loop service and security management workflows

A Scalable and Flexible Platform

ForeScout 8.1 provides unparalleled scale and deployment flexibility to meet the stringent requirements of large enterprise environments.

- With a single installation, you can manage up to two million physical or virtual devices spanning your campus, data center, cloud and OT networks.
- A modular product suite provides flexibility based on your evolving business requirements. Starting with Forescout eyeSight for device visibility, each additional product brings powerful capabilities for control automation, security orchestration, operational resiliency and OT security.
- For purchasing flexibility all Forescout software products are now available as either a perpetual license or a term-based subscription.



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