FORESCOUT

What's New Forescout 8.2

> "by 2023, the overall number of "connected" IoT devices worldwide will increase to over 35.2 billion"
>
> *- Worldwide IoT Forecast, 2019-2023, IDC*

The attacks of the past decade have taught us that a single weak spot in a network is all it takes to leave an organization vulnerable to breaches. As more IoT and other unmanaged devices connect to enterprise networks to drive digital transformation, there is an urgent need to balance innovation with the equally critical goal of securing these devices and safeguarding networks.

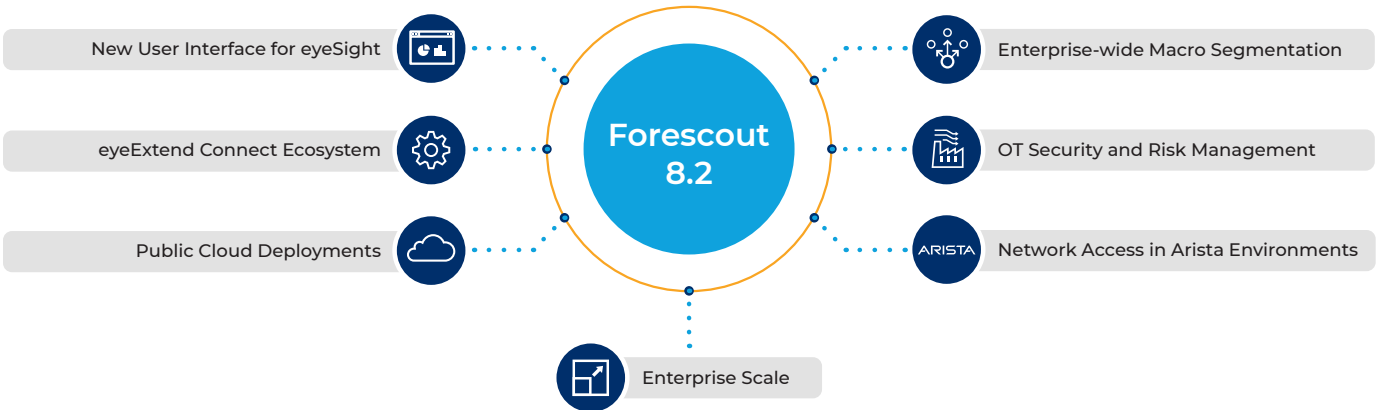
Without a complete picture of connected devices across network domains, the ability to act quickly to mitigate risks is all but lost. Legacy and vulnerable devices, noncompliant and misconfigured endpoints, and IoT and operational technologies must all be identified. Risks to all interconnected networks and all locations must be continuously assessed. With this complete visibility, comes the power to act: Fast.

Forescout 8.2: Identify and Act – Faster

Forescout 8.2 accelerates the ability to identify all connected devices, compliance gaps and risks on your network. It enables you to act confidently and quickly to mitigate security exposures and reduce mean time to respond (MTTR) across your extended enterprise networks.

Highlights of this latest release include:

- New persona-centric user interface for Forescout eyeSight with actionable device context to pinpoint, prioritize and proactively mitigate risks
- Forescout eyeExtend Connect, a new community-based app ecosystem that enables customers and partners to more easily build, consume and share apps to integrate with the Forescout platform
- New deployment flexibility and faster time to value for cloud-first organizations that want to deploy Forescout appliances in their AWS and Microsoft Azure public cloud environments
- Enterprise-wide segmentation with Forescout eyeSegment to enable organizations to confidently design and implement polices across multiple network domains and diverse enforcement points
- Integration with Forescout SilentDefense™, as well as integrated IT/OT sensors on the same appliance for unified visibility across IT and OT domains, including cloned networks with overlapping IP ranges
- Network access control via direct integration with Arista infrastructure without the need for agents or reliance on 802.1X for IT and IoT devices



New User Interface

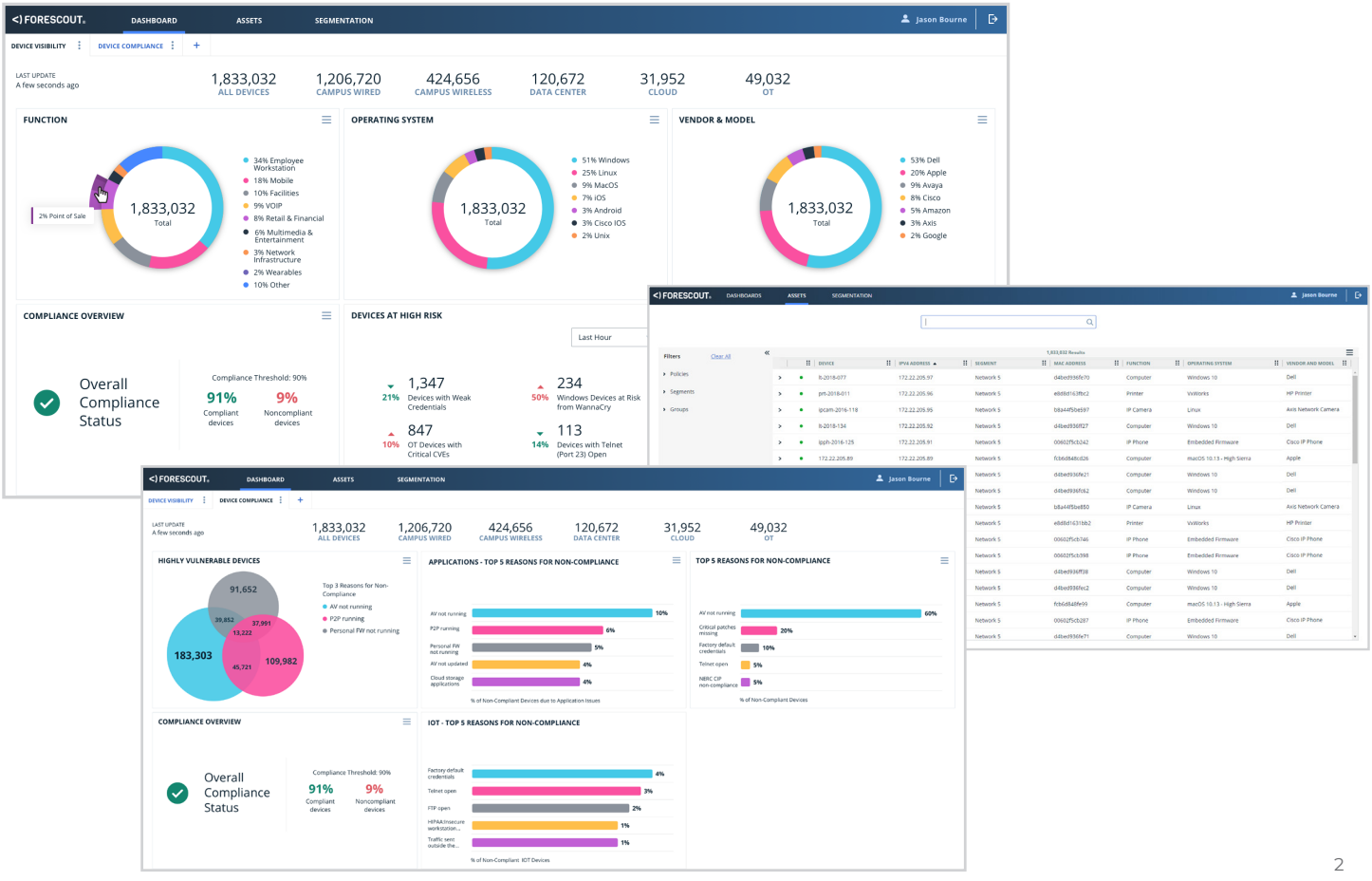
All stakeholders benefit from persona-centric context and actionable insights delivered via the new web-based user interface. Dashboards visualize connected devices, alert teams to areas of highest risk and highlight progress toward compliance goals. The real-time device inventory with rich drill-down capabilities lets operators find devices quickly to help your organization stay ahead of threats. Simple customization and sharing options make it easy to communicate risk across IT functions for fast response.

Get to insight faster. Out-of-the-box device visibility and compliance dashboards enable you to:

- Identify the function, operating system, vendor and model of all your connected devices
- Set a threshold for compliance and monitor against all active policies
- Pinpoint high-risk devices such as:
  - IoT devices with weak credentials, open ports or other misconfigurations
  - Windows devices with missing security updates or vulnerabilities
  - Devices with broken security agents or unauthorized applications
  - OT devices with critical common vulnerabilities and exposures (CVEs)
- Identify policy violations including the most frequent failures, as well as devices that are non-compliant across multiple policies (e.g. running P2P applications with no firewall or antivirus).

Proactively address gaps. Use the new web-based asset view to quickly:

- Search the entire device inventory across campus, data center, cloud and OT
- Filter by policy, network segment and any device property
- Pinpoint device location for faster MTTR



eyeExtend Connect App Ecosystem

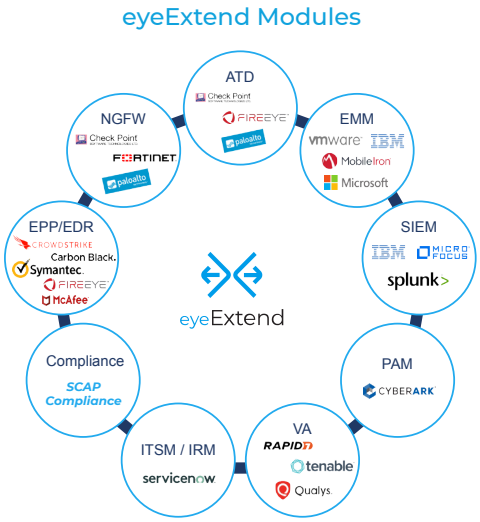
Customers leverage the Forescout platform to integrate with their other IT and cybersecurity technologies to share device context, orchestrate workflows and automate response. Forescout's current portfolio of eyeExtend modules provides out-of-the-box integrations with over 25 leading products and enables you to extend the value of your existing investments. In addition to these Forescout-built-and-supported offerings, Forescout 8.2 provides a new community-based app ecosystem to enable integrations with additional technologies.

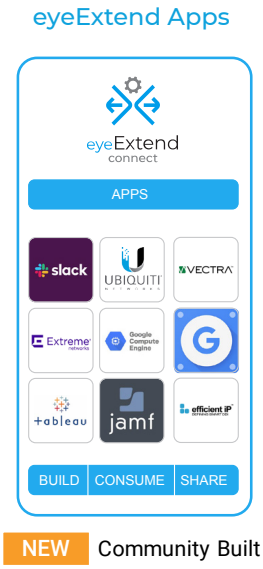
eyeExtend Connect harnesses the power of crowdsourcing and allows both customers and partners to quickly build, consume and share apps to connect with the Forescout platform. You can easily share device context with other tools, automate workflows and take action to accelerate system-wide response to reduce MTTR.

Easy to build. Gain the flexibility to create your own apps using universal Python scripting and JSON data exchange standard for faster time to value.

Easy to consume. Select from a variety of community-built apps that are easy to deploy and customize, and are portable across your network environments.

Easy to share. Contribute and learn from community best practices, share apps with your peers and leverage crowdsourcing to extend the value of your IT investments.





Enterprise-Wide Macro Segmentation

Forescout 8.2 complements eyeSegment with the latest innovations in eyeSight and eyeControl for enterprise-wide segmentation across multiple network domains and diverse enforcement points. With this seamless experience, you can confidently design and implement network segmentation and Zero Trust security at scale.

- Map and visualize traffic flows between a logical taxonomy of users, devices, applications and services
- Design, simulate and refine logical segmentation policies to understand impact before enforcement
- Monitor segmentation hygiene in real time and respond to policy violations
- Enforce segmentation controls with confidence across network domains and diverse enforcement points

Security and Risk Management in OT Environments

Leverage the integration between SilentDefense and Forescout 8.2 to address a variety of security and risk management use cases in OT and converged environments.

- Share OT device classification and vulnerabilities from SilentDefense with eyeSight and use the new eyeSight user interface for unified visibility across IT and OT networks
- Deploy integrated IT and OT sensors on the same appliance to discover and classify devices in converged environments
- Uniquely identify devices and enforce policies in cloned network environments that reuse duplicate IP address ranges across multiple sites, production lines or plants
- Use the latest capabilities of SilentDefense in OT environments including enhanced NERC CIP compliance reporting, selective and non-intrusive active inspection for deeper visibility, and an asset risk framework that aggregates multiple risk factors into impact-based scores

Network Access Control in Arista Environments

Forescout 8.2 includes direct integration with Arista infrastructure to enforce network access controls in Arista as well as heterogenous environments. This enables you to identify and regulate both IT and IoT devices, without the need for agents or reliance on 802.1X.

- Identify and assess all IoT and IT devices in real time when they connect to the network
- Provision appropriate network access based on eyeSight and third-party context, including device type, ownership, user role, device compliance and security posture
- Mitigate risks by automating a variety of network responses depending on the situation such as restricting, segmenting, quarantining or blocking devices

Public Cloud Deployments

Organizations taking a cloud-first approach to technology have been limited to on-premises physical or virtual deployments for device visibility and control. With Forescout 8.2, you can deploy Forescout sensor appliances and enterprise management in your Amazon Web Services or Microsoft Azure cloud environments without on-premises footprint. You also gain the flexibility to mix public cloud deployments with physical appliances and virtual appliances in VMware, Hyper-V or KVM private cloud infrastructure.

Physical | Virtual | Public Cloud | Hybrid

Blending any or all of the above

Enterprise Scale

Forescout 8.2 provides unmatched scalability to address the stringent requirements of large enterprises and keep pace with the explosive growth in connected devices across campus, data center, cloud, IoT and OT environments.

- Classify devices using the largest device cloud knowledgebase of 11M+ enterprise devices for more accurate and faster identification of connected IoT, OT and IT assets
- Manage two million devices in a single deployment, regardless of physical, virtual, cloud or hybrid implementations

FORESCOUT

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