FORESCOUT

Microsoft

FORESCOUT + MICROSOFT FOR POWER AND UTILITIES: BETTER TOGETHER

Gain complete asset intelligence and control to secure critical infrastructure and maintain operational resilience.

THE HIDDEN STRUGGLE

Power generation and utility operators face relentless challenges to secure their critical infrastructure, ensuring reliable service delivery while protecting against ever-evolving cyber threats. As industrial environments embrace digital transformation, integrating IT, OT and IoT devices to enhance operational efficiency, the sector has become a prime target for cyberattacks. The push toward smart grids, renewable energy sources, and automation has exponentially increased the number of connected assets, expanding the attack surface and exposing vulnerabilities. With critical services at stake, these risks have become a significant concern for utilities worldwide.

The complexity of securing critical infrastructure leads to challenges such as:

▶ Fragmented visibility across OT and IT systems, making it difficult to manage devices and optimize operations.

▶ Compliance headaches, with evolving regulations like NERC CIP requiring strict security controls and risk management.

▶ Gaps in network monitoring across operations, third parties, and transient devices make it harder to detect anomalies and cyber threats before they escalate.

Security teams are already stretched thin, struggling with disconnected tools and limited oversight. Securing modern energy infrastructure requires a smarter, more cohesive approach that reduces blind spots and strengthens visibility and control across operations.

YOUR SOLUTION SIMPLIFIED

Continuous asset protection with real-time visibility and control of every asset and threat — anywhere.

With Forescout and Microsoft, you can identify and assess every asset. Contain and control every risk in any location. Detect and respond to every threat — including unmanaged assets — continuously and in real-time.
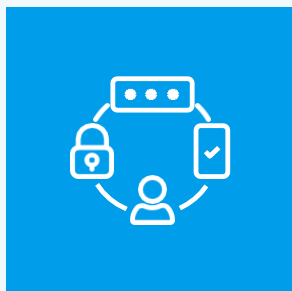
42%
Surge of ransomware on utility companies over the past year

70%
Increase in cyberattacks on U.S. utilities in 2024

$11M
the average cost of a healthcare data breach

FORESCOUT + MICROSOFT: BETTER TOGETHER

Forescout and Microsoft together give you an unparalleled, comprehensive solution that reduces complexity, saves time and improves security.

▶ **Asset Intelligence: Know What's on Your Network and What It's Doing**

- **Discover and classify all assets** across IT and OT environments in real time, ensuring full visibility into their behavior and risk posture.

- **Unify asset insights** by consolidating properties like location, vulnerabilities, and compliance status into a single, actionable view.

- **Streamline asset lifecycle management** with automated tracking, alerts for configuration changes, and risk-based prioritization.
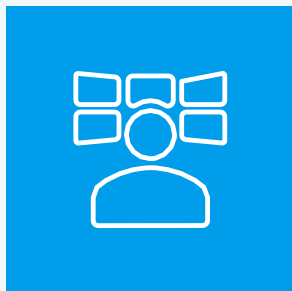
▶ **Network Monitoring: Detect Anomalies and Secure Operations in Real Time**

- **Continuously monitor network activity** to identify unauthorized access, misconfigurations, and operational disruptions before they escalate.

- **Gain deep traffic insights** with passive and active monitoring techniques, including deep packet inspection (DPI) and behavioral analysis.

- **Improve oversight of third-party and transient devices** by ensuring visibility into all network interactions, even across segmented environments.

▶ **Compliance and Risk: Maintain Security and Meet Regulations**

- **Validate security controls** across IT and OT environments to ensure continuous compliance with industry standards and regulations.

- **Automate policy enforcement and reporting** to simplify audits, reduce manual effort, and maintain real-time compliance visibility.
- **Proactively manage risk** by tracking vulnerabilities, enforcing segmentation, and monitoring changes to reduce attack surfaces and limit exposure.
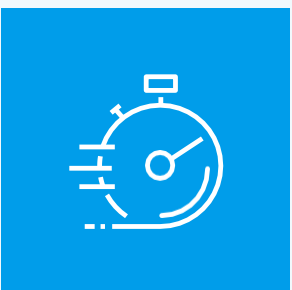
▶ **Identify and Stop Threats Before They Disrupt Operations**

- **Detect cyber and operational threats in real time** using deep packet inspection, event correlation, and anomaly detection across IT and OT environments.

- **Leverage intelligence-driven detection** with curated threat feeds, IoCs, and industrial-specific TTP analysis to uncover hidden risks.

- **Streamline incident response** with automated event classification, noise reduction, and seamless case management to help security teams act faster.

FORESCOUT + MICROSOFT: BETTER TOGETHER

For decades, Forescout and Microsoft have collaborated to tackle the most pressing cybersecurity challenges in power generation and utilities, ensuring the protection of critical infrastructure from evolving threats.

Together, Forescout and Microsoft empower energy, power, and utility operators to proactively secure critical infrastructure, combining expertise in cyber risk and compliance management with advanced threat detection and response—protecting IT, OT, and industrial control systems across the entire ecosystem.

With Forescout and Microsoft, you simplify security by quickly, accurately and confidently identifying, detecting and blocking threats, with less tools.

ENTERPRISE-WIDE ASSET INTELLIGENCE	CONTINUOS COMPLIANCE & RISKMANAGEMENT	SECURITY & OPERATIONAL RESILIENCE
Gain full visibility into IT and OT assets across power plants, substations, and control centers. Identify and classify assets in real time, ensuring precise tracking of device behavior, vulnerabilities, and operational status. Make smarter security and operational decisions by mapping dependencies, monitoring asset lifecycles, and consolidating risk insights into a unified view.	Ensure continuous compliance with NERC CIP and industry regulations by automating policy enforcement and monitoring security controls across IT and OT environments. Reduce regulatory and operational risk by tracking vulnerabilities, enforcing segmentation policies, and detecting compliance gaps before they impact critical systems.	Detect cyber and operational threats before they disrupt operations. Leverage network monitoring and anomaly detection to quickly identify unauthorized activity and misconfigurations. Strengthen resilience by proactively securing industrial operations, reducing downtime, and ensuring the reliability of essential systems.

FORESCOUT + MICROSOFT INTEGRATIONS

The unique asset intelligence and control capabilities of the Forescout platform integrate with the Microsoft product suite to provide comprehensive cyber security defenses for all assets, risks and threats in clinical environments.

Microsoft Defender for Endpoint
Protect your assets and close gaps

Secure blind spots in your network by validating that Microsoft Defender is installed, running and up to date on every applicable device. Mitigate risks by starting, deploying or updating the latest Microsoft Defender definitions or version. Leverage Microsoft Defender asset threat intelligence to contain or mitigate threats in real-time.

Microsoft Intune / Endpoint Configuration Manager
Continuous management of every agent-able asset

Extend Microsoft's reach to all agent-able and non-agent-able devices and gain visibility into legacy Windows OS's, Linux and Mac OS to create a true, real-time and up to date inventory of every asset. Validate that agents and profiles are deployed and running.

Entra ID / Active Directory
Zero Trust Assurance for your entire network

Increase your Zero Trust maturity by integrating Forescout's complete asset intelligence with Microsoft's Entra ID's users and identities. Extend your Zero Trust controls with powerful conditional access based on user, asset, location, type and risk data to make sure every asset has the right level of access.

Microsoft Sentinel
Unified Security Operations for managed and unmanaged assets

Cut through the noise with enhanced managed asset telemetry to allow security teams to quickly triage incidents with certainty. Extend your threat coverage to IoT, OT, IoMT and medical assets and leverage specialized threat intelligence to have a unified threat view in a single pane of glass.

Microsoft CoPilot
### Enhance your security team's efficiency with Forescout asset intelligence

Security teams need an ally as they hunt for the latest threats. Make sure they have the best chance by bringing Forescout's asset intelligence to their CoPilot in the fight. Give CoPilot real-time insight into risks, threats, misconfigurations and compliance issues across all assets.

Microsoft Azure
Real-time visibility and control of Microsoft Azure workloads

Don't leave your visibility and control at the perimeter. With Forescout and Microsoft you have visibility and real-time control of your Azure workloads to not only secure your assets but keep cloud costs in control from potential threats.

CONTINUOUS ASSET INTELLIGENCE AND CONTROL
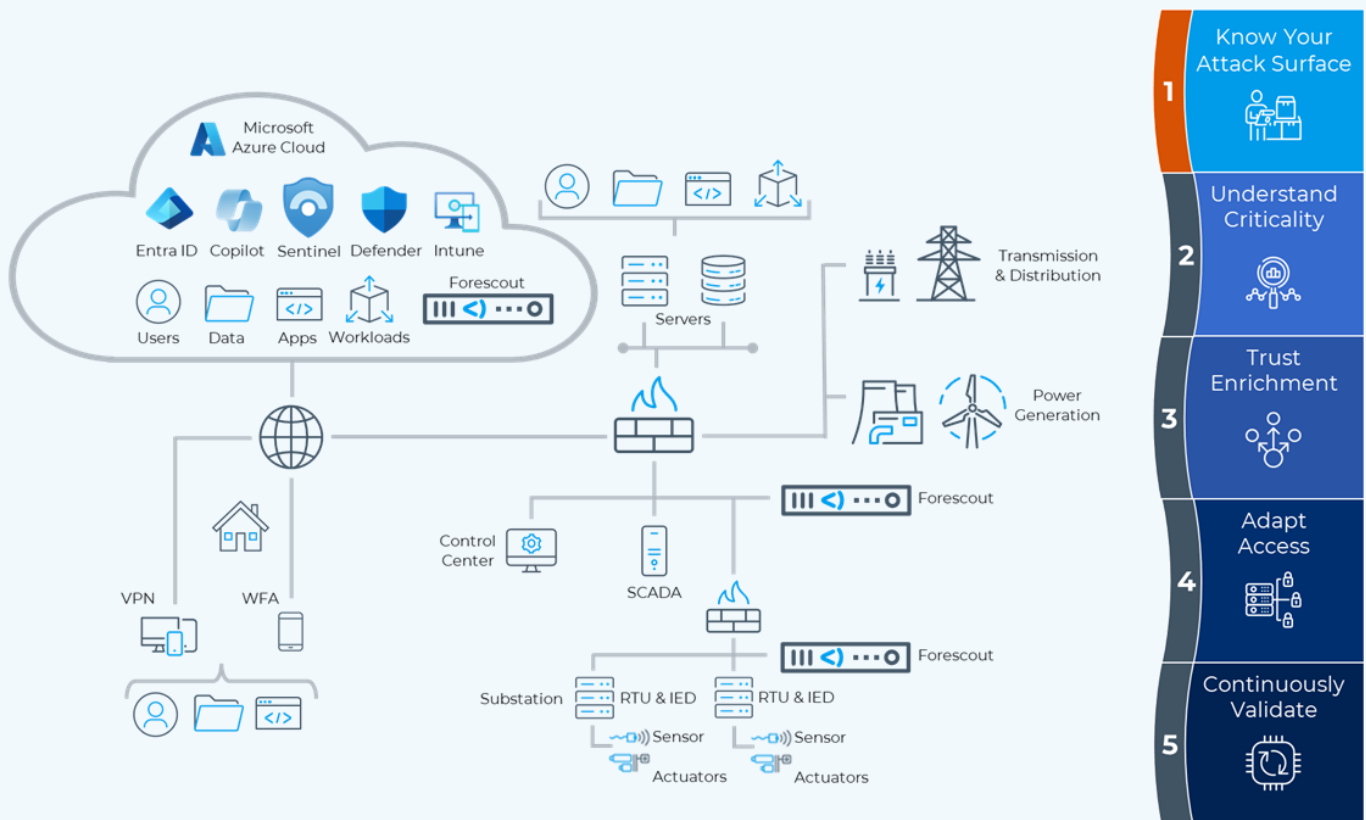
The Forescout and Microsoft partnership benefits organizations looking to simplify their security operations and maximize their overall security posture. Contact us today to learn more about how the Forescout and Microsoft partnership can help you.

See it in action. Take a test drive. Schedule a demo today.

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