FORESCOUT

Microsoft

# FORESCOUT + MICROSOFT: BETTER TOGETHER

Detect true threats and secure every asset across your clinical network with continuous asset and network protection.

## YOUR EVERYDAY BATTLE

Healthcare providers face daily struggles to safeguard their clinical networks to ensure patient safety and data protection. With so many connected devices and diverse motives driving bad actors, the healthcare industry has become a cyber battleground. Advancements in technology-enabled healthcare have led to an explosive growth of interconnected IoT, OT, IT, IoMT and medical devices, all to improve patient care and outcomes. Along with these advancements come risks and an ever-increasing attack surface.

This increasing attack surface:

- Prevents healthcare organizations from fully identifying what they need to protect
- Limits the ability to maintain and satisfy healthcare regulations and compliance
- Restricts the ability to validate identity regardless of an asset's location, user or device type

Resource constrained teams are facing alert and tool fatigue due to the plethora of cyber ecosystem tools that do not work together effectively to detect threats in today's complex environments.

## 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.

**67%**
Healthcare organizations fell victim to ransomware

**53%**
Healthcare organizations paid the ransom to recover their data

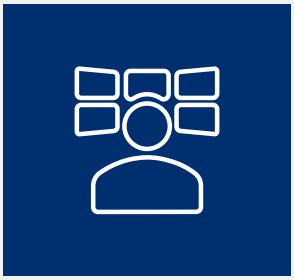
**$11M**
The average cost of a healthcare data breach

# FORESCOUT + MICROSOFT: BETTER TOGETHER

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

### Design and Assure Your Zero Trust Network

- Discover and classify all assets – IT, IoT, OT, IoMT and medical, in real-time
- Identify when they connect and disconnect, and where they are located
- Proactively ensure compliance and security posture by continuously validating against compliance frameworks and security best practices
- Dynamically control network and resource access by asset, persona or network location with strict policy controls

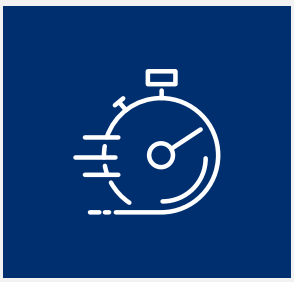


### Modernize Your Security Operations

- Detect and isolate relevant incidents – and eliminate the noise, so that analysts can focus on true threats and increase productivity
- Automate routine tasks and workflows to reduce security teams' workload and eliminate errors from manual intervention
- Receive ongoing threat intelligence to streamline investigations and adapt to evolving threats

### Automate Threat Detection & Response

- Reduce risk of operational disruptions by limiting unnecessary exposure and remediating threats across the environment
- Combine signature, behavior and anomaly-based detection techniques and map threat to industry-standard kill chain frameworks, such as MITRE ATT&CK
- Eliminate silos from the security tool stack by converging capabilities into a unified SaaS experience, reducing MTTR



### Increase Security Operations Productivity

- Meet budget constraints by optimizing IT and security operations with a consolidated solution
- Lower costs associated with analyst burnout, turnover, recruitment and training

# FORESCOUT + MICROSOFT: BETTER TOGETHER

For decades, Forescout and Microsoft have collaborated to address critical cybersecurity challenges facing healthcare organizations, with a focus on protecting all assets from the ever-evolving threat landscape.

Forescout and Microsoft allow you to proactively defend against threats by combining expertise in cyber risk and compliance management with the threat detection and response capabilities needed to protect your entire clinical environment, no matter the asset — IT, IoT, OT, IoMT and medical.

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

| ACTIONABLE PROACTIVE SECURITY | TRUE THREAT DETECTION | RISK & THREAT CONTAINMENT |
|---|---|---|
| Eliminate security blind spots as your clinical technology stack grows. Map your attack surface and understand your risk and exposure across all assets.<br><br>Mitigate your risk by remediating compliance and security gaps of network and endpoint devices before an incident occurs. | Extend your threat visibility from managed IT assets into unmanaged devices such as IoT, OT, IoT and medical. Eliminate noise so that analysts can focus on true threats. Have complete coverage of known and unknown threats and be certain you can detect them and respond quickly and effectively. | Reduce the blast radius and minimize impact of threats to your business with real-time network and host-based controls. Reduce dwell time with automated analysis and control workflows, orchestrating actions with the other security tools to close the gap quickly. |

# FORESCOUT + MICROSOFT INTEGRATIONS

## 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

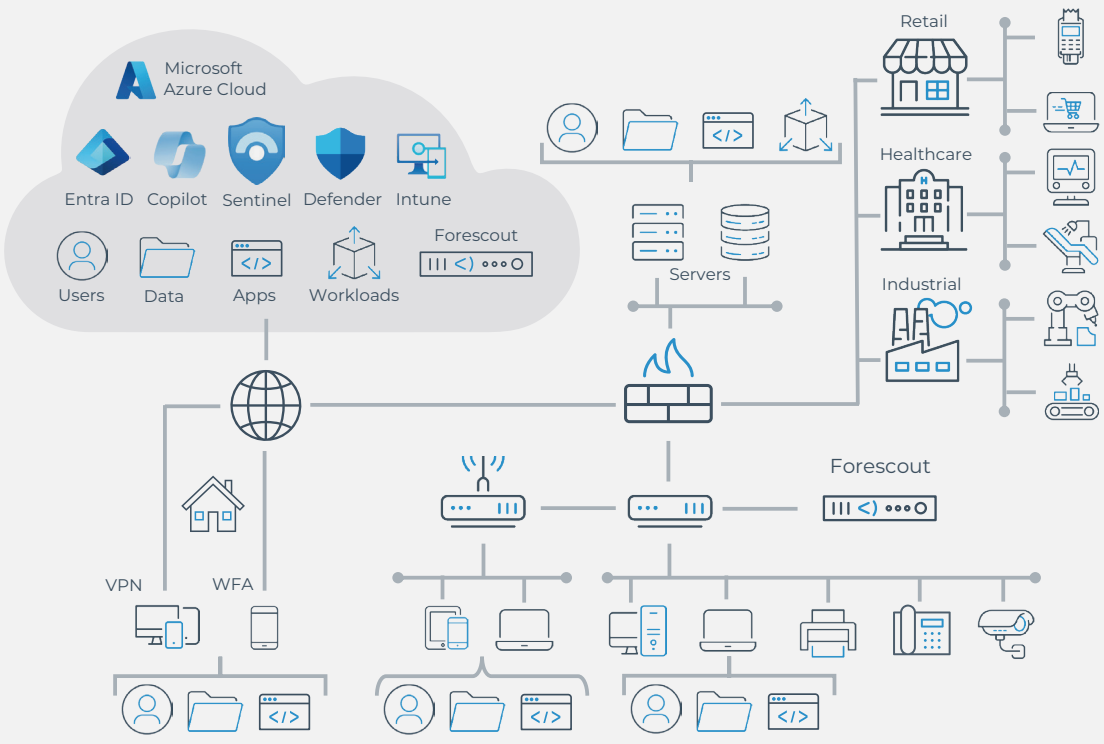
Security teams need an ally as they hunt for the latest threats. Make sure they have the best chance by bringing Forescout's asset intelligence to their CoPilot in the fight. Give CoPilot real-time insight into risks, threats, misconfigurations and compliance issues across all assets.

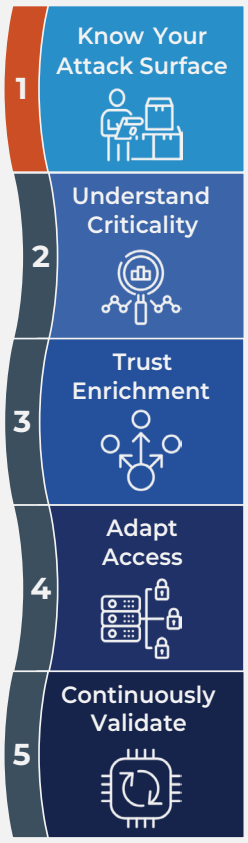
## Microsoft Azure

### 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 & NETWORK PROTECTION




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

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