Accelerating Zero Trust for Critical Systems

Operators of critical systems are under constant threat—confronted by sophisticated adversaries targeting specialized OT and IoT assets, insecure credentials, and disjointed access controls. Xage Security and Forescout have partnered to deliver a modern Zero Trust solution with Secure Remote Access (SRA) at its core—ensuring organizations can securely connect users to critical OT devices and systems from anywhere.

By combining Forescout's device discovery with Xage's distributed enforcement of least-privilege access, the joint solution delivers robust protection, streamlined operations, and continuous compliance.

Overview

Xage and Forescout form a unified security architecture optimized for secure access to any environment, even the most complex and sensitive critical infrastructure and manufacturing operations.

Forescout's contextual visibility is combined with Xage's Zero Trust enforcement to control access down to the individual user-session—enabling secure employee and third-party access to specific OT devices or applications without exposing broader networks.

Key Benefits

- **Comprehensive Asset Visibility:** Real-time discovery of all IT, OT, IoT, IIoT, and IoMT devices.
- **Secure Remote Access Without VPNs:** Session-based, time-limited access to specific assets—no VPNs or jump hosts.
- **Granular Zero Trust Control:** Enforce access by user and context.
- **Agentless, Scalable Protection:** Secure any device—legacy or modern—without agents.
- **Resilient Offline Enforcement:** Maintain access control at the edge, even when disconnected.
- **Real-Time Threat Detection & Incidence Response:** OT-specific threat indicators built on more than 14 years of OT/ICS threat research.
- **Streamlined Compliance:** Meet NERC CIP, TSA, and IEC mandates with ease.

FORESCOUT

Continuously discovers and classifies devices, building a detailed asset and risk profile.

xage SECURITY

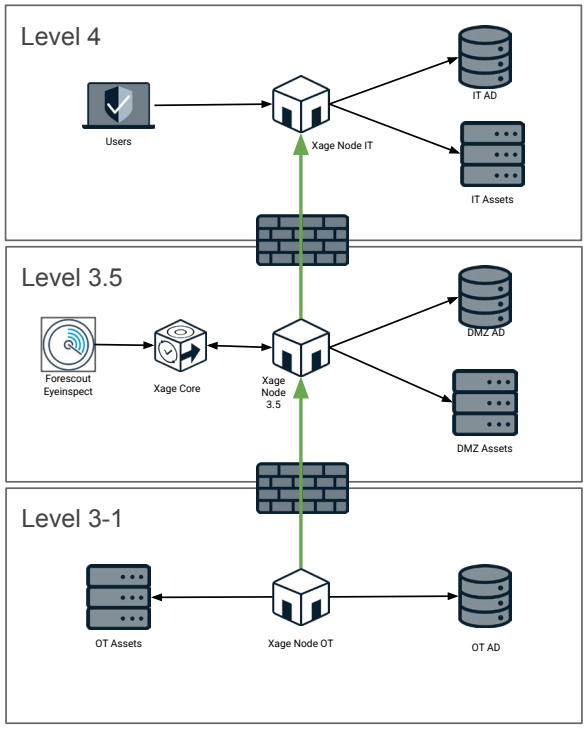
Provides secure remote access and applies access policies for devices discovered natively and by Forescout.

Use Cases

- **Device Discovery & Asset Inventory:** Forescout's passive and active discovery capabilities identify all devices on the network—including specialized OT and IoT systems. These asset details are ingested by Xage to enhance the living inventory of protected endpoints, ready for policy assignment.
- **Gap Analysis of Unprotected Assets:** With Xage and Forescout integrated, customers can compare protected vs. unprotected devices—identifying unmanaged endpoints that lack access controls or segmentation. Devices can be added to protection policies via Xage.
- **Secure Remote & Local Access:** Xage enforces least-privilege access down to the device level. Users—whether internal employees, vendors, or contractors—receive time-bound, MFA-protected access to specific devices or applications, not whole networks. No VPNs or jump servers are needed.

How It Works

1. **Discovery & Context Gathering:** Forescout scans and profiles every connected asset across IT, OT, and IoT layers.
2. **SRA Policy Mapping:** Xage consumes enriched asset metadata via API and maps users to systems/devices based on least-privilege access models.
3. **Session-Based Enforcement:** Xage applies access policies at the edge, granting access per session, with full auditing and revocation capabilities.



About Xage Security

Xage Security is a global leader in zero trust access and protection on a mission to pioneer a secure tomorrow. Control access and prevent attacks in the cloud, in the data center, at the remote operational edge anywhere on Earth, and even in orbit with the Xage Fabric Platform. Xage is easy to manage and can be deployed in a day, giving users easy and secure access to the assets they need from anywhere, while preventing advanced adversaries and insider threats at every stage of the attack chain. Learn why organizations like the U.S. Space Force, PETRONAS, and Kinder Morgan choose Xage at xage.com.

About Forescout

For more than 20 years, Fortune 100 organizations, government agencies, and large enterprises have trusted Forescout as their foundation to manage cyber risk, ensure compliance, and mitigate threats. The Forescout 4D Platform™ delivers comprehensive asset intelligence, continuous assessment, and ongoing control over all managed and unmanaged, agented and un-agentable assets across IT, OT, IoT, and IoMT environments. Forescout's open platform makes every cybersecurity investment more effective with seamless data integrations and automated workflow orchestration across more than 100 security and IT products. Forescout Research – Vedere Labs is the industry leader in device intelligence, curating unique and proprietary threat intelligence that powers Forescout's platform.