FORESCOUT

Forescout Assist for OT/ICS

Key Benefits

- No more wading through alerts and noise, so IT/security teams and OT engineers can focus on high-fidelity threats and risks
- Reduced risk of a cyberattack impacting safety, equipment, operations and service provision
- Improved utilization of OT/ICS devices and less downtime
- Cost-effective way to scale your security operations without adding headcount
- Less time and effort to provide proof of compliance to auditors

Key Features

- 24/7 security monitoring
- Risk and threat mitigation recommendations
- Enhanced correlation rules for eyeInspect
- Human-led threat hunting
- Data retention, asset posture and configuration history, and data analytics

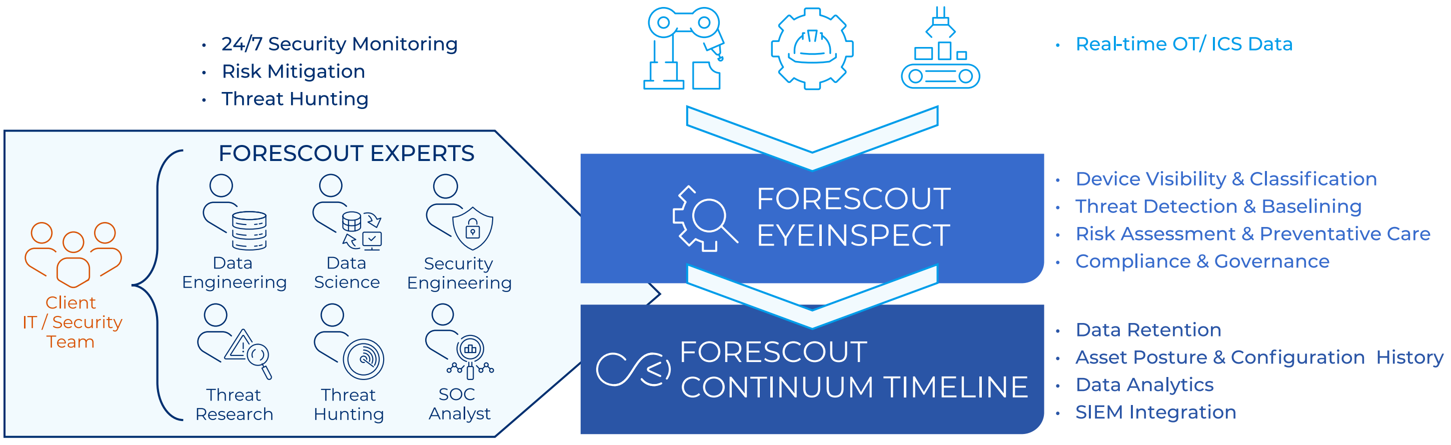
Forescout Assist for OT/ICS is a subscription service designed for IT/security teams that lack the resources to fully leverage the inherent value provided by Forescout eyeInspect.

From its 24/7 security operations centers (SOCs), Forescout security experts – including data scientists and engineers, security analysts and engineers, and threat researchers and hunters – operate as an extension to your IT/security team to remotely monitor the alerts being generated by eyeInspect. The team identifies cyber risks and threats, then triages and investigates them. The issues that truly warrant attention are escalated to you, along with recommended containment and remediation guidance. All activities are supported by SLAs and customizable runbooks.

As part of your subscription, Forescout security experts will also conduct human-led threat hunting exercises to help further reduce cyber risk. Moreover, the service leverages Forescout Continuum Timeline, giving you search and historical analytics of all IP-connected assets in your digital terrain.

Forescout Assist for OT / ICS

24/7 security experts that triage, investigate and help mitigate risks and threats identified from Forescout eyeInspect



- 24/7 Security Monitoring
- Risk Mitigation
- Threat Hunting

FORESCOUT EXPERTS

Data Engineering, Data Science, Security Engineering, Threat Research, Threat Hunting, SOC Analyst

Client IT / Security Team

- Real-time OT/ ICS Data

FORESCOUT EYEINSPECT

- Device Visibility & Classification
- Threat Detection & Baselining
- Risk Assessment & Preventative Care
- Compliance & Governance

FORESCOUT CONTINUUM TIMELINE

- Data Retention
- Asset Posture & Configuration History
- Data Analytics
- SIEM Integration

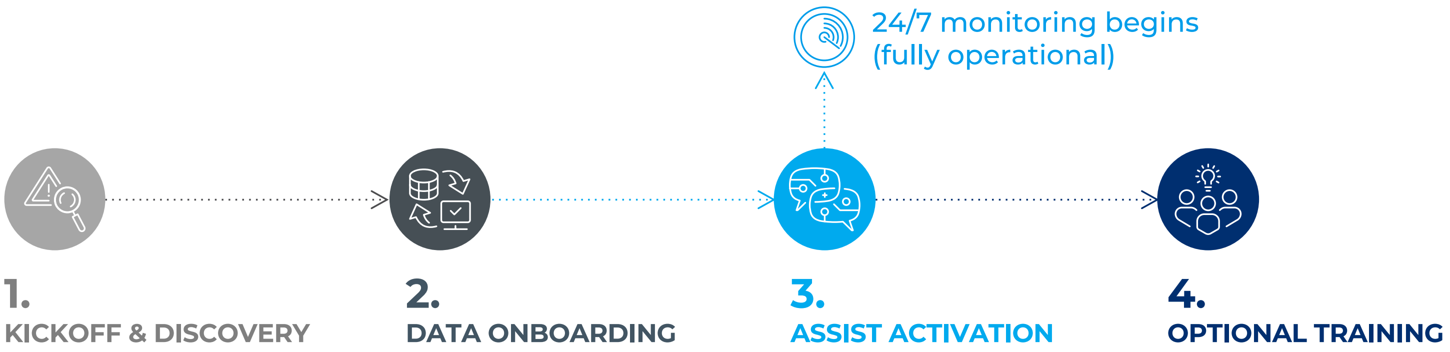
The Package

A Forescout Assist for OT/ICS annual subscription includes all of the elements below:

24/7 Security Monitoring	
Threat monitoring & triage	• Monitor detected threats for suspicious activity • Triage detected threats to determine response priority
Threat investigation	• Investigate detected threats to validate whether they are a true threat that warrants escalation • Document observables, attack attributes, root cause, infected assets, IOCs, etc.
Incident escalation & remediation	• Escalate confirmed, true threats as security incident cases once potential impact determined • Provide containment and remediation guidance to stop and recover from an attack
Risk Mitigation	
Risk analysis & triage	• Triage asset risks (compliance issues, policy violations, vulnerabilities) identified by eyeInspect
Risk evaluation & prioritization	• Evaluate discovered risks to determine response priority • Prioritize client response priority based on potential business/operational impact and provide bi-weekly/weekly response priority report.
Risk remediation	• Recommend remediation priority and outline steps to reduce risk in report
Threat Hunting	
Threat modeling	• Continuously discover security risks targeting critical business assets
Human-led threat hunting	• Prioritize and perform threat hunting based on critical assets, prevalent threat actors, threat intelligence and vulnerabilities • Document and escalate malicious findings as security incident cases

Getting Started

Forescout follows a four-step process to ensure a successful service engagement with clients.



24/7 monitoring begins (fully operational)

1. KICKOFF & DISCOVERY

2. DATA ONBOARDING

3. ASSIST ACTIVATION

4. OPTIONAL TRAINING

1. A **Kickoff and Discovery** call with key client stakeholders is held to confirm client goals, priorities and IT environment; to review the keys to a successful Assist service; and to answer any questions.
2. **Data Onboarding** ensures that eyeInspect data flows into Forescout Continuum. Forescout data engineers validate that the data is being parsed, cleansed, normalized and enriched, then review and validate, with clients, that the required log sources have been fully onboarded.
3. **Assist Activation** is a virtual meeting with the Forescout security operations team responsible for the daily monitoring, triage and investigation. The service level agreement, runbooks and escalation procedures are reviewed and client access to the platform is confirmed. Once step 3, has been completed, Forescout Assist will be live, and experts will be actively monitoring your environment, mitigating risks and conducting threat hunting exercises.
4. **Optional Training** of the Forescout platform is intended for organizations that want to actively participate in the threat and risk detection, investigation process. This instructor-led, two-hour virtual course covers all the basics, including how to perform searches, investigate threats, interact with cases, and view and interpret dashboards.

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