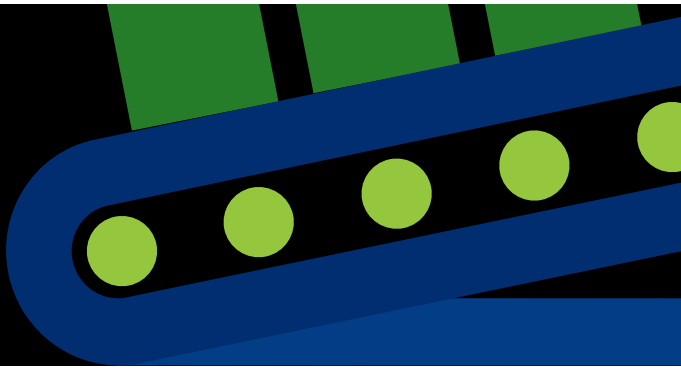
FORESCOUT
Active Defense for the Enterprise of Things™

Splunk & eyeInspect

Rapidly detect and mitigate OT threats with enhanced security intelligence



Industrial organizations are under pressure to secure and monitor their growing OT and industrial control system (ICS) networks with fewer resources. To accomplish this, asset owners require cohesive visibility into devices and network operations in a manageable, digestible way. Currently, this requires multiple tools and resources. Common challenges include:

- Slow and incomplete threat/incident response times
- Inefficient implementation and enforcement of compliance tasks
- Complex integrations with SIEMs and other enterprise tools
- Elevated risk of downtime of critical business operations

Best-in-class OT security monitoring for Splunk

To prevent operational disruptions, OT asset owners must know what devices are on their networks and monitor them to detect threats in real time. The Forescout OT Network Security Monitoring App for Splunk enhances your Splunk-based security operations and asset management practices with device inventorying, threat detection and response workflows for faster and more effective risk mitigation.

Data from Forescout eyeInspect (formerly SilentDefense™) is automatically mapped to the Splunk Common Information Model (CIM) and Splunk OT Asset Data Model, enabling more rapid OT asset inventory, alert and vulnerability intelligence across both cyber and operational perspectives.

"By 2025

75%

of OT security solutions will be interoperable with IT security solutions and delivered via multi-function platforms."[1]

GARTNER

Integration Components

Dashboards

Three pre-built Splunk Enterprise dashboards are included to provide timely flexible OT threat mitigation and streamlined asset management.

Widgets

Configurable widgets streamline threat detection, simplify threat analysis and reduce mean time to response (MTTR) to OT threats.

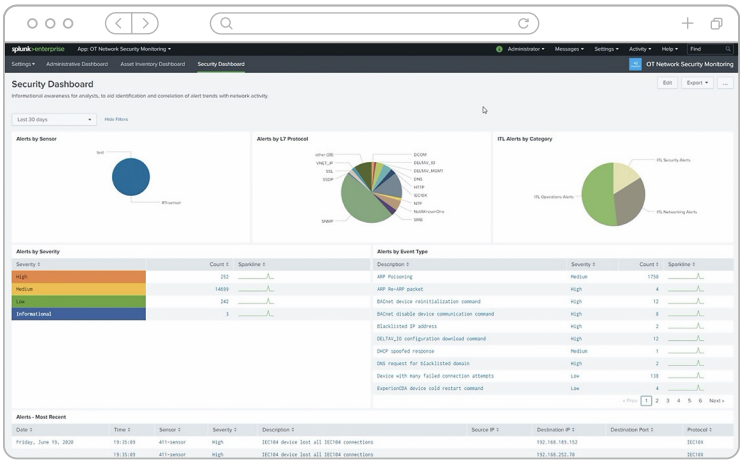
Automatically mapped data for rapid insight

Forescout eyeInspect data can be easily leveraged by other Splunk Apps such as Splunk Enterprise Security and OT Security Add-on for Splunk to further enhance OT analytics and incident management.

PRIORITIZE ALERTS

Address alerts according to business impact

Easily integrate OT-specific alerts with greater context into Splunk. The solution combines detailed OT asset inventory information mapped to the Splunk OT Asset Data Model and alert data mapped to the Splunk CIM alert component to prioritize risks and vulnerabilities according to urgency and risk level.



The Security Dashboard

Identify OT alert trends and correlate them with other network activities to enable device compliance enforcement as well as anomaly and threat detection. Analysts and asset owners receive granular threat intelligence behind each alert on a single dashboard, driving faster and more informed remediation action.

CUSTOMER BENEFITS

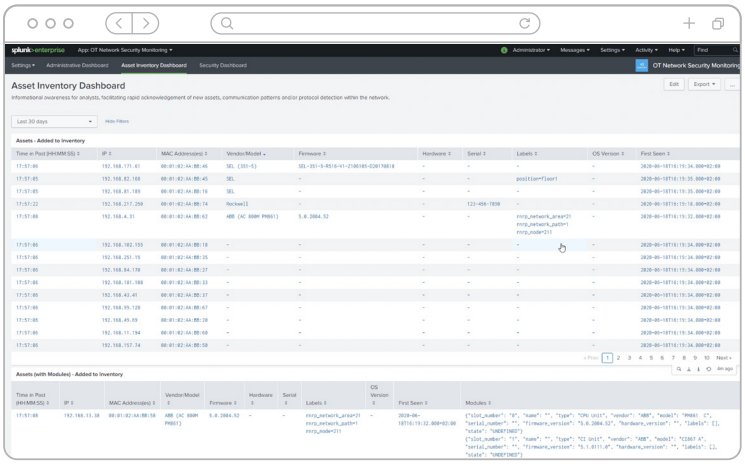
- Continuously maintain an accurate OT asset inventory
- Enable accurate detection and prioritization of OT threats for remediation from within Splunk
- Gain real-time intelligent alerting with highly configurable Splunk messages leveraging information gathered from eyeInspect
- Reduce MTTR to cyber and operational threats by providing contextual asset information
- Immediately identify changes in the network and asset configurations
- Seamlessly correlate data from large multisite eyeInspect deployments while maintaining the context of data origin

MANAGE ASSETS

Streamline asset compliance

The app enables asset managers to:

- Rapidly prioritize investigations and acknowledge new assets
- Assess asset configurations, communication patterns and protocol usage within the network
- Easily generate reports for regulatory compliance



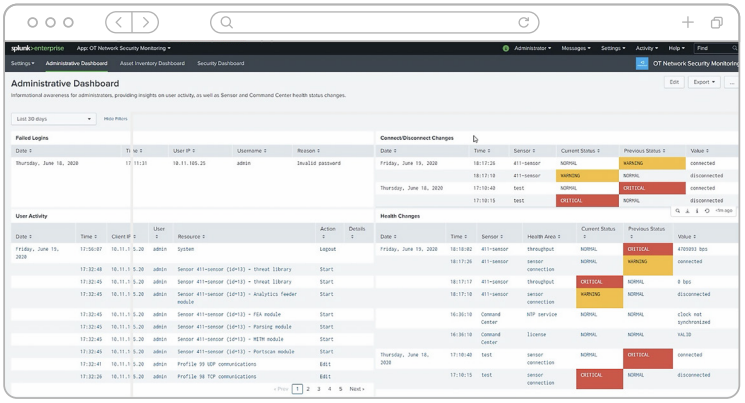
Asset Inventory Dashboard

Asset owners and analysts instantly access high-value device information to enhance the detection of unexpected changes occurring on the network.

MAINTAIN PROTECTION

Manage security appliances at a glance

Maintain system availability and continuously detect undesired user activity to ensure you are always protected.



Administrative Dashboard

Gain deep, real-time insights into your OT security system health status and user activity performed on your eyeInspect appliances.

PRE-BUILT DASHBOARDS

Security dashboard

Identify alert trends and correlate with network activity for faster detection of anomalies, cyber threats, dangerous commands sent to OT devices and device misbehavior.

Asset inventory dashboard

Access high-value device context to identify unexpected network changes, prioritize investigations and quickly acknowledge new assets, communication patterns or protocols.

Administrative dashboard

Gain insights into system hygiene and user activity performed on Forescout eyeInspect appliances to prevent system failure and detect undesirable user activity.

Why Forescout

The Forescout OT Network Security Monitoring App for Splunk is the only app to consider for industrial users of Splunk who require continuous, more comprehensive OT asset intelligence and threat detection capabilities. This solution is an extension of the Forescout platform and Splunk integration that combines continuous IT, IoT and OT device intelligence with incident detection, management and response capabilities. The result is a highly context-aware, automated closed-loop security system with a complete audit trail. Together, Forescout and Splunk help organizations greatly reduce risk and increase operational efficiency across all device types, network tiers and global locations.

Learn more about Forescout's partnership with Splunk

Click here to learn more.
Download the app.

1. Gartner Market Guide for Operational Technology Security, January 13, 2021

splunk>

The Forescout OT Network Security Monitoring App for Splunk is the ideal solution for industrial asset owners who want to integrate rich OT asset intelligence and threat detection data from across all OT sites within Splunk. Users can leverage the exceptional OT asset and threat data from Forescout eyeInspect to increase compliance and defend their OT/ICS networks.

Don't just see it. Secure it.™

Contact us today to actively defend your Enterprise of Things.

forescout.com/solutions/operational-technology salesdev@forescout.com toll free 1-866-377-8771

FORESCOUT
Active Defense for the Enterprise of Things™

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