Managing Multisite Industrial Security Infrastructure

with Cisco Cyber Vision Site Manager and Splunk

As industrial operations span multiple sites, security teams face a critical challenge: fragmented visibility into their operational technology (OT) security posture and inefficient management of the OT security infrastructure. Manual, site-by-site software updates are time-intensive and error-prone. Outdated software and threat intelligence create security gaps. Multiple consoles make it difficult for security teams to gain a comprehensive view and hinder effective OT security governance.

The operational consequences are severe: undetected cyberthreats, poor risk assessment, and resource-intensive threat response. OT security experts spend more time managing tools than reducing risks. With Cisco® Cyber Vision Site Manager and the Cyber Vision app for Splunk®, Cisco addresses these issues by providing centralized monitoring, automated updates, and aggregated views, enabling organizations to streamline OT security, meet compliance requirements, and improve threat detection and response.

Benefits

- Monitor the health of all sensors and troubleshoot issues across sites from a single console.
- Automatically keep all sites current with the latest software and threat intelligence
- Monitor your OT security posture across all industrial sites with advanced dashboards.
- Give the line of business custom dashboards that can blend insights from security and production tools.
- Give security analysts unified visibility across IT and OT domains to better detect threats.

Cyber Vision Site Manager: Enabling resilience in your OT security infrastructure

Centralized infrastructure visibility

Cyber Vision Site Manager delivers enterprise-wide visibility into every Cyber Vision Center and sensor across all industrial sites, enabling teams to monitor deployment status, connectivity health, performance metrics, and configuration compliance from a single console.

Automated software management

Eliminate manual, site-by-site updates through centralized software management. Coordinate rollouts across your entire infrastructure with scheduling controls that respect operational windows, helping ensure that all deployments stay current with the latest versions and features.

Consistent threat protection

Automatically distribute the latest threat intelligence feeds to your entire OT security infrastructure from one central location, helping ensure that vulnerabilities, intrusions, and threats are properly identified across all industrial sites.
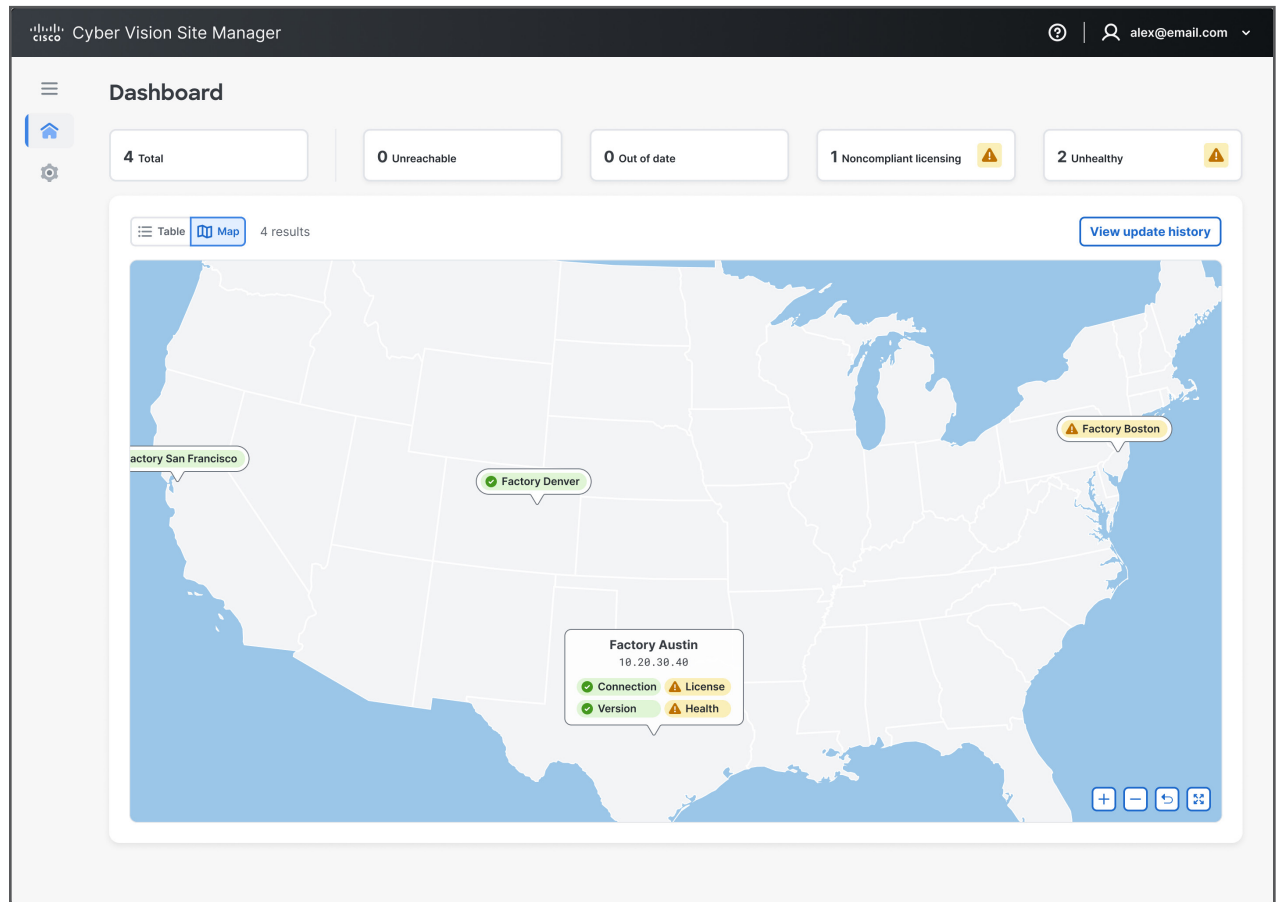

Figure 1. With Cyber Vision Site Manager, you manage your multisite OT security infrastructure in one console

Cyber Vision app for Splunk: Empowering teams with OT security insights

Centralized view to drive security governance and compliance

Benefit from Splunk's advanced search, analytics, and data visualization capabilities to monitor your global OT security posture and drive OT security governance. Prebuilt and customizable dashboards aggregate Cyber Vision security telemetry from all industrial sites into a single interface for enterprise-wide visibility.

Understand risk to reduce the OT attack surface

Transform vulnerability management from a site-by-site exercise into a strategic, enterprise-wide program. Unified dashboards provide comprehensive visibility into security weaknesses across all industrial assets, with prioritized risk scoring based on asset criticality, exploitability, and operational context.

Advanced dashboarding to surface operational insights

Develop custom dashboards for specific industrial use cases and stakeholder needs—from plant floor managers monitoring local asset health and network performance to regional directors tracking cross-site comparisons and operational metrics.

Seamless integration with the Splunk SIEM

The Cyber Vision application for Splunk enables a seamless integration into Splunk's Security Incident and Event Management (SIEM) platform to ingest OT security telemetry from all your industrial sites, giving analysts a complete view of the attack chain.

Figure 2.   The Cyber Vision app for Splunk offers dashboards to monitor the OT security posture across all sites and meet the needs of OT teams

Start securing your industrial operations with Cisco today

Talk to a **Cisco sales representative** or channel partner and visit **cisco.com/go/ OTsecurity** to learn more.

The Cisco advantage

For more than 20 years, Cisco has been helping industrial organizations around the globe digitize their operations, working with manufacturers, power and water utilities, energy companies, mines, ports, railways, roadways, and more. Today, Cisco offers a market-leading portfolio of industrial networking equipment plus a comprehensive suite of cybersecurity products, integrated tightly together with a deep understanding of OT requirements. It's a rare combination.

By designing, developing, and testing products together, Cisco enables IT and OT teams to achieve advanced outcomes while reducing the complexity, time, and gaps incurred by the need to make point products work together. Our solutions come with comprehensive design and implementation guides that will help you reduce risk, accelerate implementation, and make the most of your technology stack. Browse our library of validated design guides here: **cisco.com/go/iotcvd**.