Solution Brief

Model network access and compliance to de-risk IT/OT convergence

Build a network model by ingesting data from industrial/general-purpose firewalls and network infrastructure to validate access and comply with regulatory frameworks

Challenges

Critical National Infrastructure (CNI) providers face a daunting combination of cyber security challenges: The attack continuum that results from rapid acceleration in IT/OT convergence. Cyberattacks on CNI are increasing in frequency and sophistication. Stringent regulatory requirements necessitate a proactive approach to security posture. And a global skills shortage that makes it hard to recruit and retain the professionals needed to deal with the challenges.

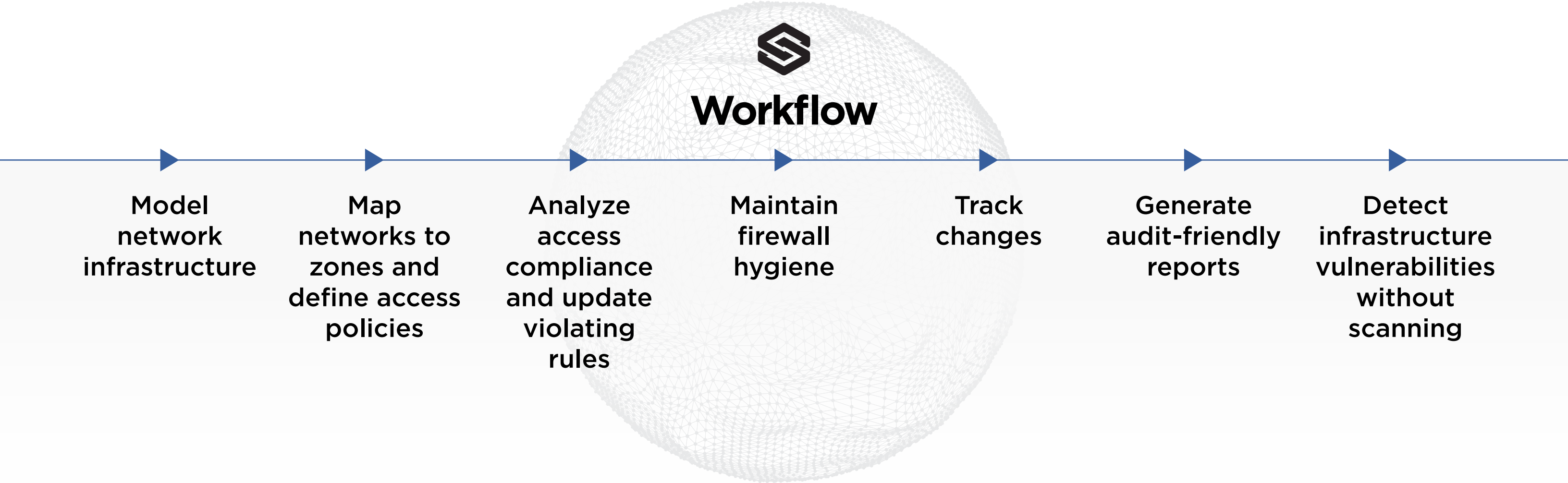
Process control networks today comprise a mix of general-purpose network infrastructure as well as specialized devices designed specifically for industrial environments. These ruggedized devices are used widely across the transportation and power generation sectors and upstream, midstream, and downstream oil and gas industries. They provide connectivity in even the harshest environmental conditions such as extreme pressure, vibration, or ambient temperatures and can be deployed in a range of small form factors.

Use cases

- **Network segmentation matches industrial zoning requirements**
- **Network visualization is based on infrastructure context and threat intelligence**
- **Prevents lateral movement of threats**
- **Device-independent analytics allow for easy simulation**
- **Automated workflows support change management**

To de-risk IT/OT convergence, CNI service providers must include data from both industrial and general-purpose networking and security devices in their overall security policy management system to solve the following challenges:

- **Imperfect network visualization** - Without a complete network model, the organization must rely on static scans and imperfect analysis efforts that rapidly become outdated and inaccurate.
- **Visibility blind spots** – If industrial firewalls and networking equipment are not included in the network model, blind spots in the converged environment create an unquantifiable and unacceptable risk to the organization.
- **Lack of network/access separation in-line with best practice recommendations** – The collection of configuration information for these devices is essential to achieve complete operational visibility, understand network separation, and comply with the best practice guidelines for control and segregation published in the ISA/IEC 62443 series of standards.
- **Poor firewall hygiene** – Firewall rulesets must be optimized to ensure compliance with industry-acknowledged and organization-specific regulations that govern access between IT and OT.
- **Inconsistent reports** – Without consistent, automated dashboards and reports, it is impossible to demonstrate compliance with the standards needed for regulatory approval.



Workflow

Model network infrastructure

Map networks to zones and define access policies

Analyze access compliance and update violating rules

Maintain firewall hygiene

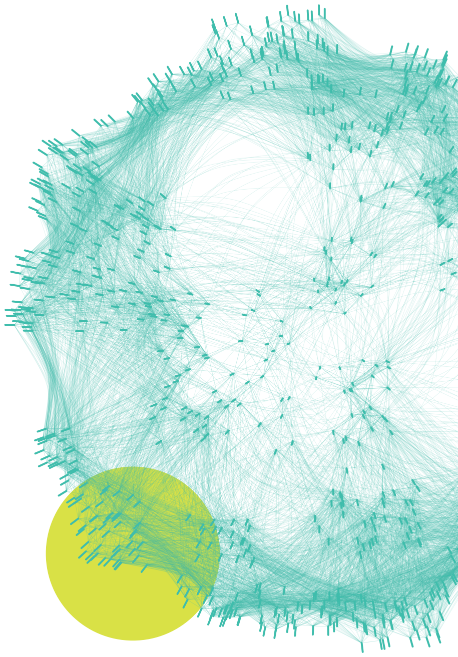
Track changes

Generate audit-friendly reports

Detect infrastructure vulnerabilities without scanning

Solution

The Skybox Security Posture Management Platform helps customers solve these challenges through a combination of Firewall Assurance and Network Assurance across the converged enterprise. It is the only platform that combines infrastructure context with threat visibility across the entire attack surface that spans the IT and OT environments.



Model network infrastructure

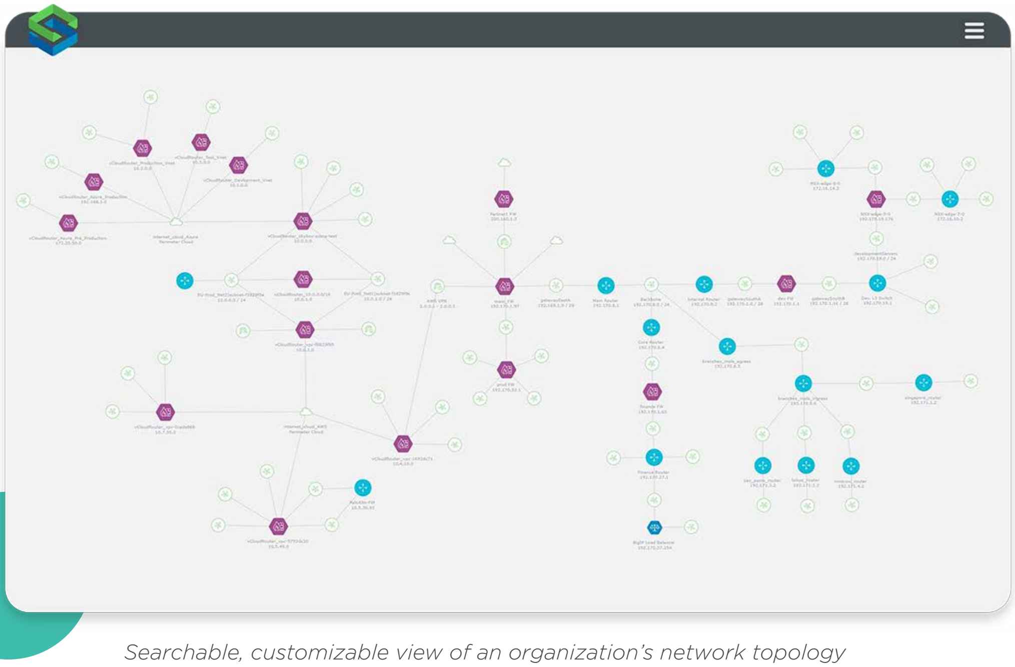
The Skybox **Security Posture Management Platform** ingests:

- Configurations and routing tables from Purdue Enterprise Reference Architecture Layer 3 devices
- Security groups, security tags, and assets from virtual domains
- Asset information from configuration management databases (CMDBs) and management systems
- Vulnerabilities from scanners and vulnerability definitions from Skybox threat intelligence

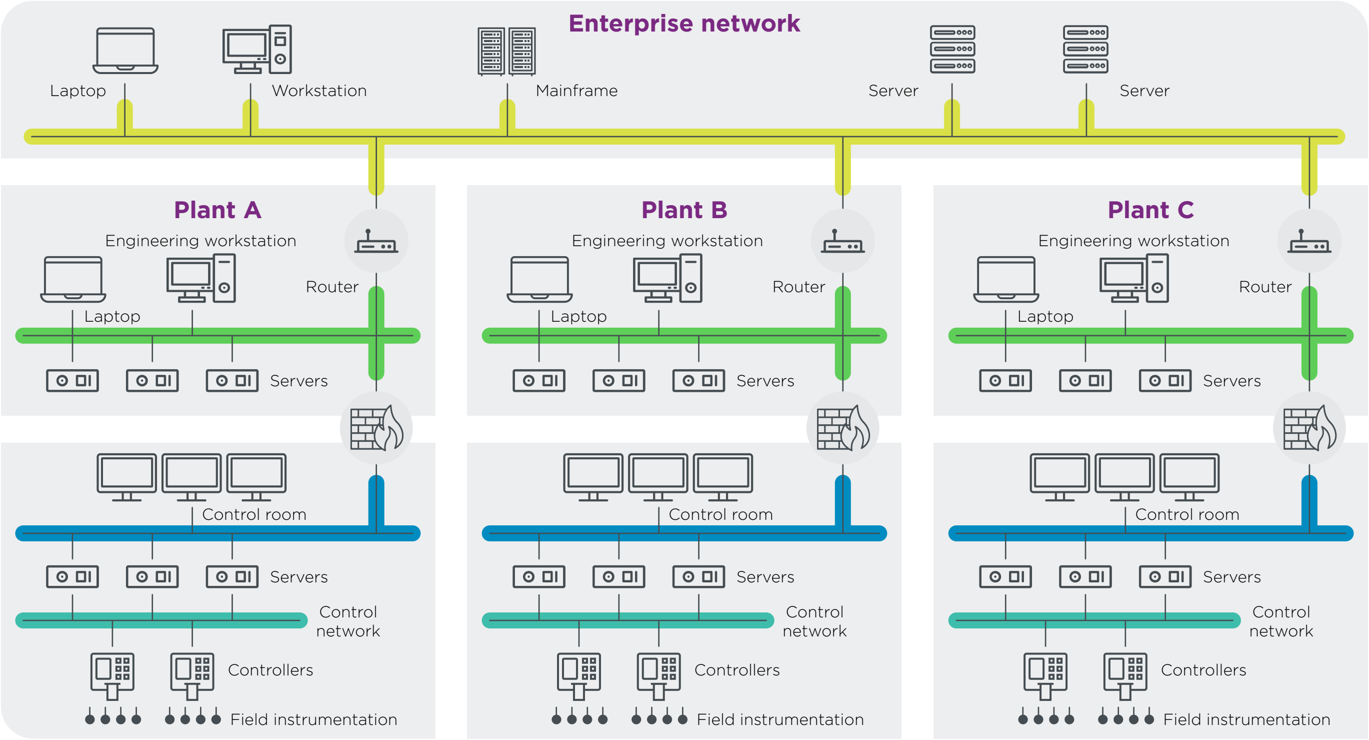
The information is parsed and normalized to create a network model, which is an abstraction of the IT, OT, and hybrid cloud infrastructures. The entities represented in the model include assets, network devices, networks, locations, and clouds. The model can include both industrial and general-purpose infrastructure. It supports specialized devices that are custom-built for industrial applications and hazardous environments, such as the Siemens 1400 and 1500 families of intelligent edge routers.

Map networks to zones and define access policies

Map networks in the model to zones and easily customize out-of-the-box templates to create flexible policies aligned with industrial standards such as ISA/IEC 62443. Encode the standards' requirements in the policies created in the Skybox platform – such as segmenting the network into zones (grouping cyber assets with the same cybersecurity requirements) and conduits (used for communication within/between zones).



Searchable, customizable view of an organization's network topology



Set up zones and conduits in a manufacturing environment[1]

Analyze access compliance and update violating rules

The Skybox Access Analyzer is a powerful simulation tool that analyzes the actual – as opposed to theoretical – access across network zones and considers access rules, routing rules, and network topology. The model identifies violating rules for easy updates. Include industrial firewalls in the network model to test, demonstrate, and ultimately ensure compliance with the regulations governing network separation across the entire attack surface.

Maintain firewall hygiene

Skybox ensures that industrial firewalls, in addition to other firewalls in the network, are correctly configured to align with industry best practices. Rule compliance policies are used to inspect specific rules to identify violations in the configured source, destination, port, or application. Access compliance policies are used to identify firewall rules that allow violating traffic to move between network zones. To help maintain good firewall hygiene, Skybox identifies shadowed or redundant rules and objects for elimination, which significantly reduces the organization's attack surface.

Track changes

Skybox provides the ability to track any changes made to firewall access rules. This includes recording new, deleted, and modified rules to create a comprehensive audit trail for the purposes of troubleshooting, forensic analysis, and compliance. Change records include details of the change made, the time and date stamp, and the user who made the change. These change records make it easy to reconcile every detected change to the firewall with an existing change request in the organization's chosen change management platform.

[1] Diagram inspired by ISA Global Cybersecurity Alliance, How to define zones and conduits

Generate audit-friendly reports

Skybox delivers a single model of the IT and OT estates for reporting and auditing purposes. Tailor dashboards and reports to suit the needs of different audiences and stakeholders across the organization. The highly configurable Web-based interface makes it easy to report on the entire estate or specific areas such as device configuration, network separation, access, and firewall rule compliance. Generate reports in a range of the most popular file formats.

Detect infrastructure vulnerabilities without scanning

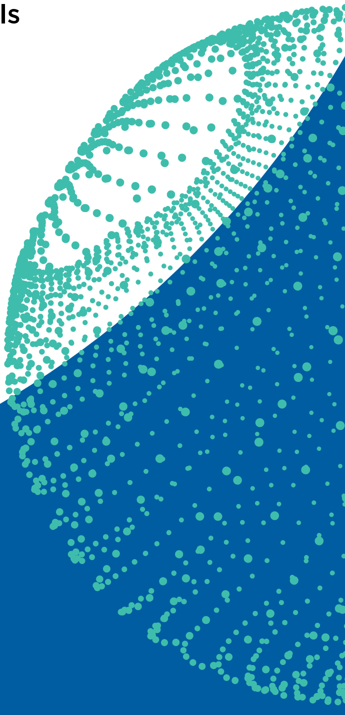
Active scan-based vulnerability assessment tools unlock point-in-time visibility at best. Gaps between scan events on a device can result in undetected vulnerability occurrences. Scanless detection, powered by the Skybox platform, addresses such blind spots by combining outputs from generic CMDB parsers and patch management systems with the Skybox vulnerability dictionary to continuously detect vulnerabilities on networking and firewall infrastructures.

Benefits

- **Easily demonstrate compliance with automated operational workflows**
- **Avoid costly audit preparation fees and non-compliance penalties**
- **Reduce the need for hands-on expertise in every technology with network abstraction**
- **Allow lean teams to manage complex converged estates using simulation tools**

Want to learn more? Get a demo or talk to an expert:

skyboxsecurity.com/request-demo



ABOUT SKYBOX SECURITY

Over 500 of the largest and most security-conscious enterprises in the world rely on Skybox for the insights and assurance required to stay ahead of their dynamically changing attack surface. Our Security Posture Management Platform delivers complete visibility, analytics, and automation to quickly map, prioritize, and remediate vulnerabilities across your organization.