Operational technology (OT) networks, including ICS and SCADA systems common in critical infrastructure and manufacturing organizations, have become increasingly connected to IT networks. While this has improved operational efficiency, it has also made OT a more prevalent attack vector and target for today’s threat actors.

Unlike attacks on IT that generally focus on data theft and monetary gain, a successful attack on OT can alter physical processes. Cyberattacks on OT could damage infrastructure, disrupt services, and endanger the health and safety of workers and the communities they serve.

As such, it has increasingly become the responsibility of IT security teams to inform OT engineers of their cyber risks and potential impacts. In order to do this, organizations need to have unified visibility of the hybrid network, its assets and vulnerabilities at all times.

**Challenges in Securing OT Environments**

• Standard IT security controls and technologies either don’t translate or are prohibited in OT due to the disruption they may cause to operational processes

• OT devices are often plugged in straight out of the box with default passwords and easily discoverable/exploitable default settings

• Software and firmware may contain vulnerabilities or were designed without modern security methodologies (encryption, data validation)

• Patching can be disruptive to uptime, can void warranties or is impossible for legacy technology no longer supported by the vendor
The Solution

The Skybox® Security Suite provides the most comprehensive set of cyber risk management solutions to secure IT and OT networks from a single platform. With seamless visibility, contextual intelligence and analytics-driven automation, Skybox eases the resource requirements to understand and manage risks in hybrid IT–OT environments.

Skybox integrates data from more than 130 networking and security technologies, including OT cybersecurity platforms. It merges and normalizes this data in central repositories to establish a single source of truth, so your entire security program has a common reference for infrastructure, asset and vulnerability data.

Skybox then builds this information into a comprehensive model of on-prem, multi-cloud and OT networks, providing total visibility across hybrid environments and enabling detailed analysis to:

- Compare the aggregate access of your network to the access designed in your security policies, analyzing by Purdue level, device type, etc.
- Analyze access end to end to troubleshoot connectivity issues and protect critical assets
- Identify critical-risk exposed and exploited vulnerabilities to effectively plan patches or mitigation
- Automate and orchestrate processes to maintain uptime and avoid costly or dangerous disruptions

FIG 1: A representation of the Skybox model encompassing on-prem, public and private cloud and OT environments — their topology, security controls and assets
BENEFITS OF SKYBOX FOR OT

- Bring on-prem, multi-cloud and OT environments into a single and complete model of your attack surface
- Analyze paths from any source to any destination within and between hybrid networks
- Find exposed and exploitable vulnerabilities anywhere in your organization, and prioritize remediation based on risk
- Strengthen security to maintain uptime and avoid disruption

Unify your hybrid IT-OT environment into central repositories, a common reference model and centralized management platform. By harnessing the power of Skybox for OT, you'll gain unparalleled insight to your hybrid environment — and its risks — to inform action with better context, increase process efficiency and improve collaboration between teams.

Learn more about the Skybox approach by downloading our whitepaper or schedule a demo today.