SKYBOX™ SECURITY
Total Visibility. Focused Protection.™

# Why a Unified Approach to IT and OT Network Security is Critical

## THE EVOLVING IT–OT LANDSCAPE

Operational technology (OT) encompasses hardware and software that monitors and manages physical equipment and processes. It includes a variety of industrial control systems (ICS) such as distributed control systems, supervisory control and data acquisition (SCADA) systems and industrial internet–connected devices (smart devices/IIoT). As the use of OT increases, the need to secure it to support continuous uptime and safety has never been more critical. That's because OT runs some of the most essential systems across multiple industries around the world. This technology monitors and controls critical infrastructure such as oil and gas drilling and distribution; energy generation and distribution; chemical, pharmaceutical and consumer goods manufacturing; and many health, building management, transportation and telecommunications applications, among others.

Because they run essential systems in critical infrastructure and deliver responsive capabilities in real time (such as meeting surge demand/usage), OT networks need to be kept up and running at all times. To secure OT networks in the past, they were air gapped or physically separated from IT networks, essentially isolating them from cybersecurity risks. OT networks were presumed to have a reduced risk profile with respect to cyberattacks due to the difficulty of developing attacks for proprietary protocols and arcane technology.

But in this digitally connected age, these safeguards have all but disappeared. In the last 20 years, OT has been exposed directly to outside risks via remote sensors to retrieve data, Wi–Fi–enabled controllers and USB devices to update software, for example. In addition, many producers are starting to market cloud–based "SCADA–as–a–service" platforms. Considering this exposure and the criticality of services OT supports, OT networks have become a more attractive objective to hack and breach. This interest is visible in the growing availability of productized exploit kits, easily searchable sites on legacy technology and new monetization options such as ransomware. With the increasing convergence of corporate IT and production OT networks, these threats present a greater danger than ever before, as vulnerabilities and security issues in both environments can give an attacker a foothold, as well as opportunities for lateral movement.

To combat these risks, organizations are now looking to improve and unify security management in OT networks, bringing it up to par with their IT security management program.

This whitepaper will examine the challenges, implications and benefits of a unified approach to managing security in converged IT and OT networks.

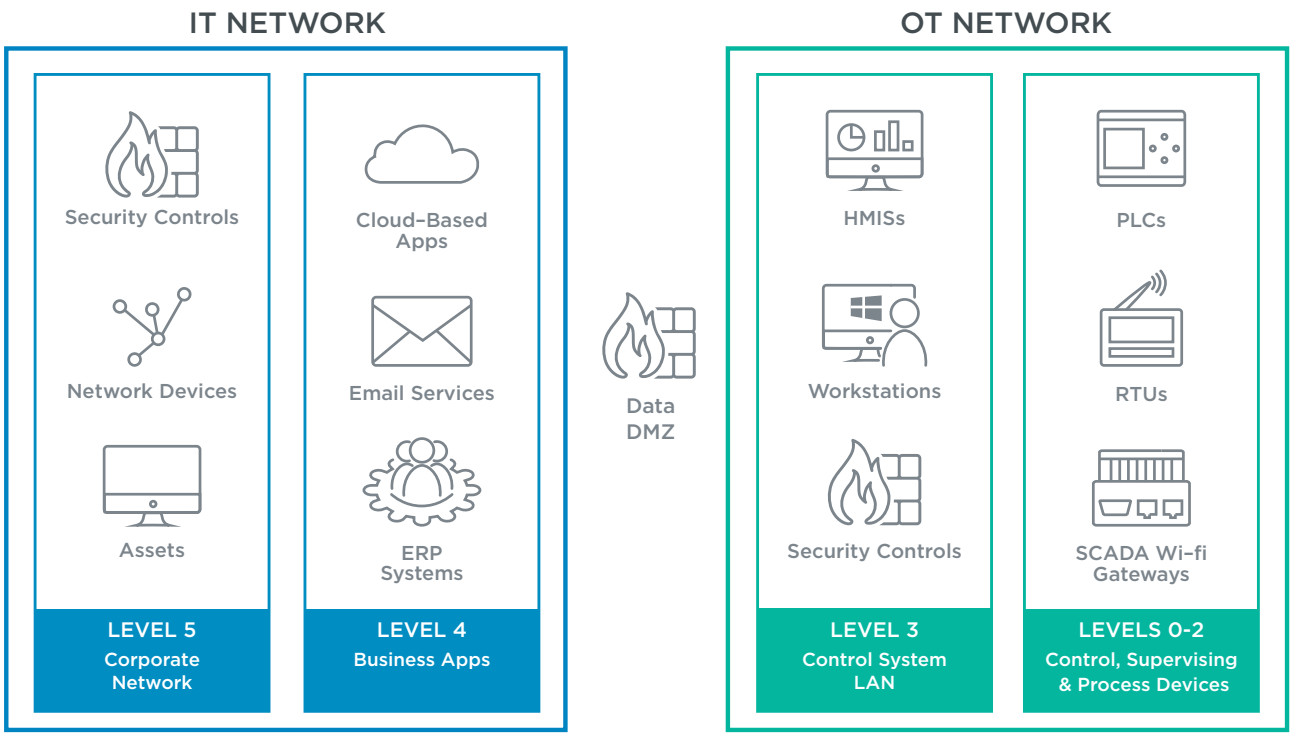


Figure 1: Typical technology stacks across IT and OT networks.

## MASSIVE CHALLENGES COMPLICATE SECURING OT

OT is meant to perform routine but important tasks, such as monitoring temperature, pressure and flow. The technology's first and foremost purpose is continuous uptime. When most OT systems were designed, they were designed with very little consideration for security, as there were no actual or perceived business value to adding security features — or because it was extremely expensive. This has changed. Today, OT manufacturers — and buyers — are recognizing the business value of built-in security for the role it plays in maintaining uptime. Unfortunately, OT networks contain decades-old devices and systems designed long before modern cybersecurity measures, or when implementing such measures was cost-prohibitive. This issue creates challenges to imposing and maintaining fundamental security measures on OT:

- **Legacy technology:** OT is rife with decades-old technology that was designed long before security measures common today, such as encryption or password protection. Even though it's not secure, as long as it can do its job, OT systems are kept up and running — and there may be no better option on the market. Poor security, including weak passwords (for example, "password") can also be embedded at the firmware level and unchangeable.
- **Outdated systems:** The firmware itself can also be outdated, such as in PLCs, with no update process in place, leaving them vulnerable. And, when security measures are installed on IT assets within the OT network, these IT assets are often outdated systems with known vulnerabilities in the software stack that may or may not have vendor support to fix them; for example, old Windows machines that are no longer supported by Microsoft.
- **Unsecure connections:** To easily transfer control data or use new applications, OT devices communicate with the IT network or laptops, or use USBs. Sometimes this communication is performed over unencrypted Wi-Fi connections, leaving them vulnerable to man-in-the-middle attacks.

- **Convergence with IT:** As OT connects with the corporate network, it also becomes vulnerable to malware and vulnerabilities as well as malicious insiders. In addition, as OT systems become smarter and more IT-enabled, OT engineers are tasked with adding IT knowledge and security expertise to their already full and distinct workloads. Conversely, IT teams aren't typically well-versed in OT systems, concerns and protocols.
- **Organizational challenges:** Because IT and OT each have different teams, technologies, processes and objectives, it is difficult to create and maintain security architectures that meet the needs of both groups. This security management disconnect also creates the cracks in which attackers can slip in and move throughout the organization.
- **Limited visibility and insight:** Finally, propriety protocols in OT make it difficult, if not impossible, for IT solutions to map the attack surface. IT security solutions, for the most part, have not been adapted to work in OT environments. For example, permissive scanning of the OT network is generally not allowed, leaving these areas in the dark for vulnerability management practices, risk awareness and proactive threat protection.

> The biggest challenge organizations are struggling with is limited — but vital — visibility of the IT-OT attack surface.

While the convergence of IT and OT technologies is creating tremendous productivity benefits, it is also introducing new security risks. In fact, nation-state cyber warfare, led by bad actors in search of political power and financial gain, has already carried out multiple successful attacks. For example, ransomware infections in 2017, such as WannaCry and NotPetya, showed the threat to converged networks. IT systems connected through poorly configured networks to OT systems running unpatched operating systems can massively disrupt OT systems, bringing production lines to a halt and general business operations to a standstill. Given their criticality, disrupting OT systems and assets can have disastrous outcomes: loss of life, accidents and injuries, environmental disasters, interruption in vital services and the associated economic losses.

Threats to OT are difficult to fight because of all of the challenges cited above and because standard security measures in IT networks often don't work with OT environments. For example, patching vulnerabilities on OT devices requires downtime that isn't always possible and can actually crash devices as well as void their vendor support.

But the biggest challenge organizations are struggling with is limited — but vital — visibility of the IT-OT attack surface. Visibility is essential in security in terms of understanding the environment and its connections, designing security architectures, identifying attack vectors and locating blind spots, among other things. Without visibility, unknown and unchecked security issues abound: vulnerabilities, misconfigurations, access policy violations, faulty design in the form of weak security controls as well as unplanned or unauthorized changes. While there may be visibility solutions for IT and OT networks individually, they rarely intersect. Manually piecing together information from such solutions is likely imprecise, and gaining contextual intelligence from them is an even bigger task. With teams already overloaded, this becomes an impossible situation.

## Defining the Attack Surface

The attack surface is the combined exposure — including the reachable and exploitable vulnerabilities — in IT and OT networks. In order to establish a comprehensive strategy to understand and manage the attack surface, three perspectives should be considered:

**Network attack surface** — the attack is delivered via the network

**Software attack surface** — the attack is delivered via applications, particularly, web applications

**Human attack surface** — the attack is delivered via social engineering or a trusted insider, or is the result of human error or the absence of employees

**Source:** Stephen Northcutt, "The Attack Surface Problem," SANS Technology Institute, https://www.sans.edu/cyber-research/security-laboratory/article/did-attack-surface

## A BETTER APPROACH IS A UNIFIED ONE

To manage security across IT and OT environments, you must be able to see and understand the entire attack surface of your organization, including physical IT and OT, virtual and multi-cloud networks. Illuminating the entire context of the network provides a better, more complete foundation to understand risks anywhere in the organization.

### See and Understand the Attack Surface

The SANS Technology Institute defines the network attack surface as an organization's exposure, reachable and exploitable vulnerabilities. In other words, the sum total of all the ways in which a network is vulnerable to cyberattack. It is made up of the network topology, security controls and assets in the IT and OT environments, as well as the security issues, vulnerabilities and threats that put them at risk.

OT attack vectors include:

- Lateral movement through corporate networks, made possible by IT–OT convergence
- Infiltration via remote access and/or spearphishing (advanced persistent threats)
- Direct access from disgruntled employees as well as external contractors and other third parties such as suppliers and support vendors
- Malware injected through internet connections or direct access
- Targets such as HMI interfaces, DCSs, PLCs, and RTUs
- Malfunctioning units, unmapped networks and configuration mistakes

Building optimal attack surface visibility typically involves an automated four-step method of 1) discovery, 2) modeling, 3) analytics and 4) visualization.

**DISCOVERY:**

On the IT side, the discovery phase should identify:

- Security controls (firewalls, IPSs, VPNs)
- Network topology (routers, load balancers, switches)
- Assets (servers, workstations, networks — including cloud and virtual networks as well as traditional IT)

On the OT side, discovery should be accomplished by passively collecting information about OT network assets and network topology to identify:

- Devices of the DMZ (firewalls and any other security controls)
- Level 3 control system LAN, with assets such as manufacturing systems, inventory control and any routing equipment
- Level 0–2 assets, including information about the type and location of field devices, PLCs and other machines

It is of outstanding importance to underline that the approach of this information collection is completely passive, as OT networks are very susceptible to active actions in terms of time requirements and certification issues.

> To manage security across IT and OT environments, you must be able to see and understand the entire attack surface of your organization, including physical IT and OT, virtual and multi-cloud networks.

**Vulnerability Occurrence on OT Device**

Asset: Supervisory Server [10.100.10.211]

Purdue Level: 3

Status: Up

Exposure: Direct

Vulnerability: CVE-2003-1418 Apache HTTP Server allows remote attacker to obtain sensitive information

OS: Linux

Risk Level: Medium

## MODELING

Mounds of discovery data do not equal actionable intelligence. The data collected should be automatically built into a comprehensive network model encompassing both IT and OT networks, including vulnerabilities and threats. Such a model also provides an offline environment to perform a variety of security management tasks without disruption to the live network — especially beneficial to OT networks requiring constant uptime.

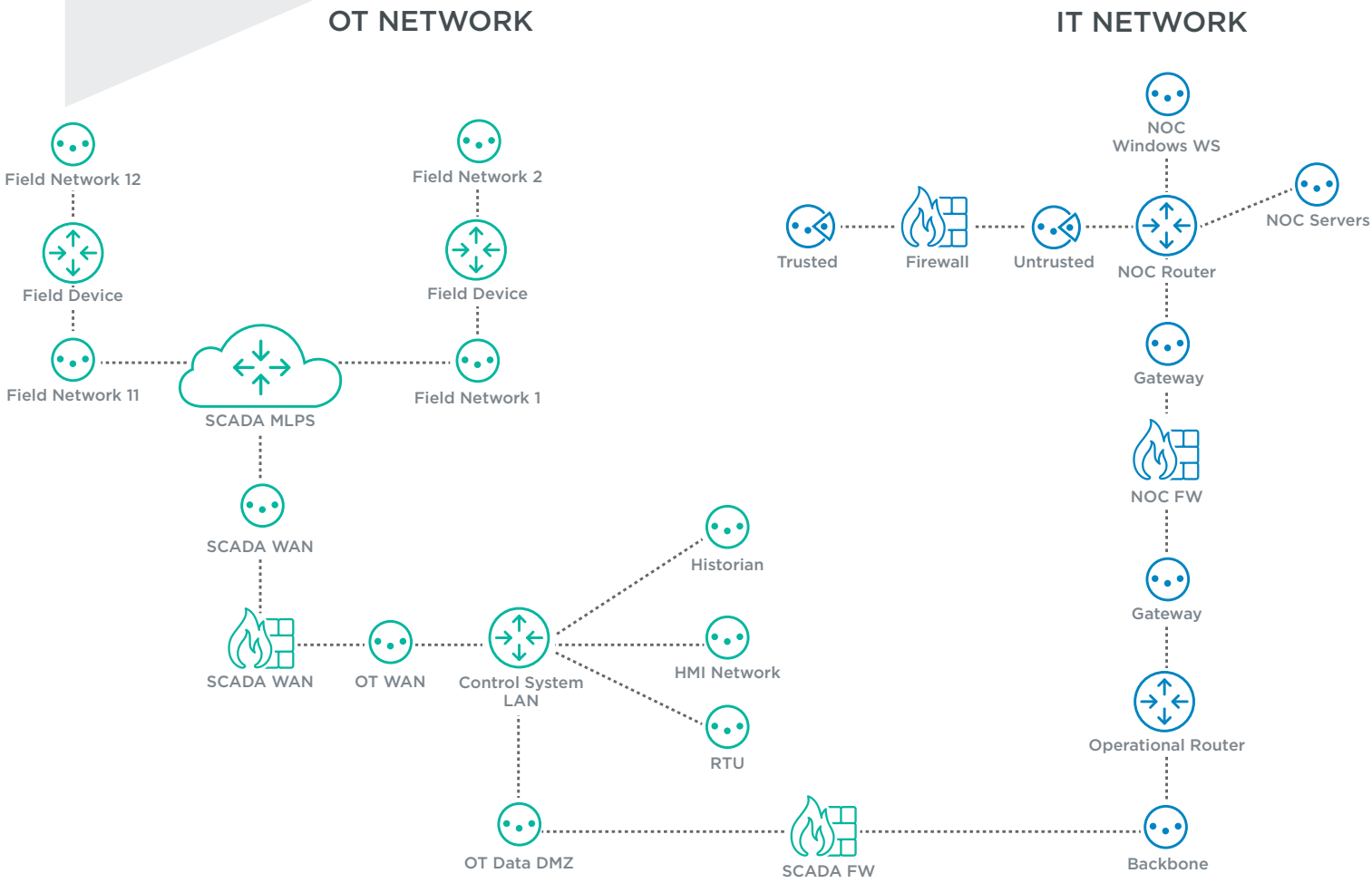


Figure 2: Modeling IT and OT networks illuminates the attack surface.

## ANALYSIS & VISUALIZATION

With an interactive, visual model of your attack surface, you can easily identify risky and needed connectivity within IT networks, OT networks and across both; verify policies are being followed throughout the organization; and evaluate potential threats.

Paths between the corporate and production network can be analyzed in the network model. Firewalls along the path are identified and their rules examined to determine if access is blocked or allowed. For instance, access from the corporate network to mission-critical HMI systems should be blocked, while limited access should be granted to allow config files to be downloaded to production machines.

> **When evaluating IT–OT security management solutions, look for those that offer the ability to passively collect information and completely model all networked environments.**

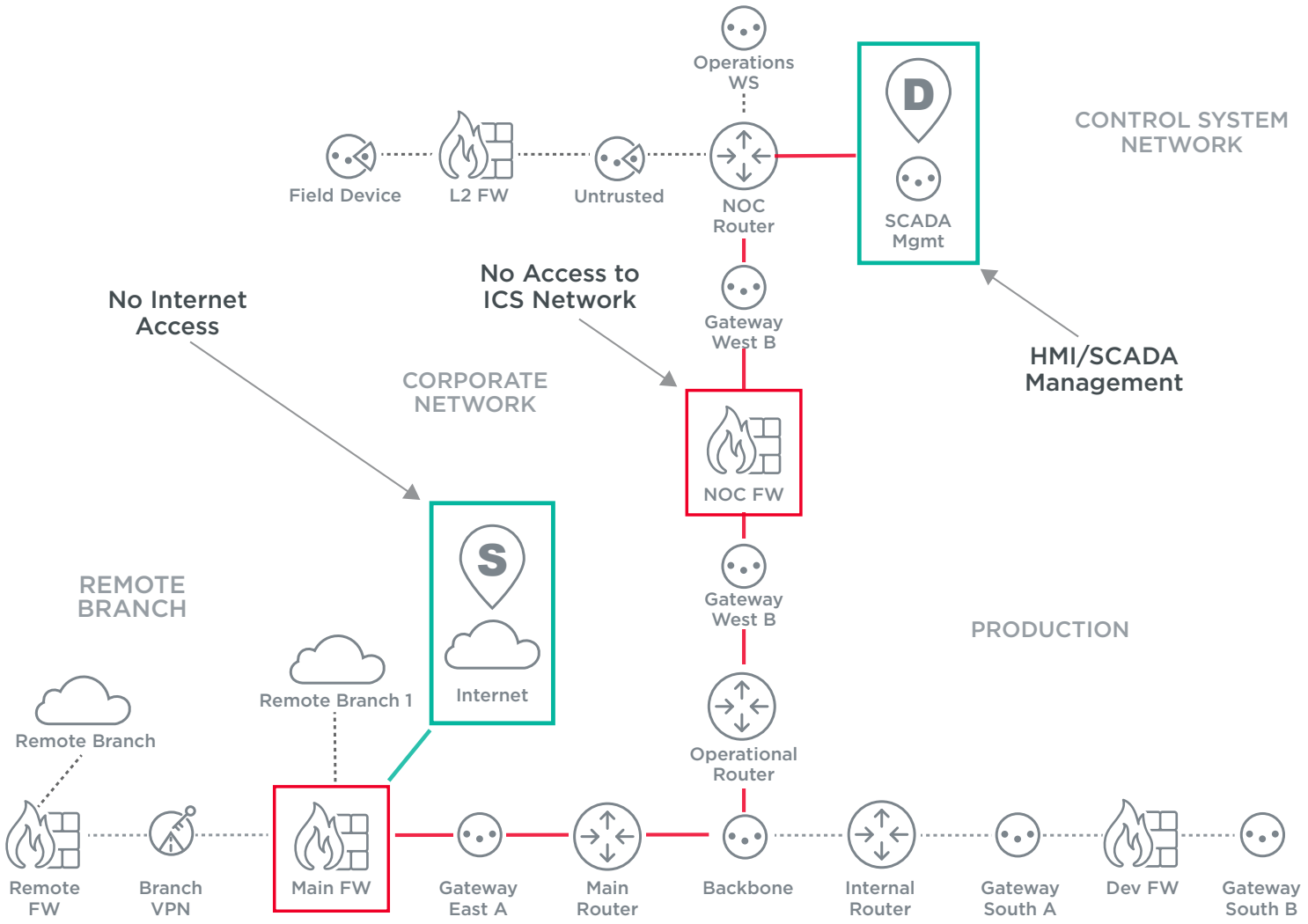


Figure 3: Path analysis from the corporate to production network showing the path to the HMI system is blocked.

## The Importance of Threat–Centric Vulnerability Management

In a converged IT–OT environment, it's critical to understand how vulnerabilities affect risk levels of the entire organization to accurately set remediation priorities. To do so requires threat–centric vulnerability management (TCVM). The TCVM approach takes into account all an organization's vulnerabilities, correlating them with the network model and real–time threat intelligence to determine which vulnerabilities are most likely to be used in an attack. With this information, TCVM can accurately prioritize remediation to ensure critical patches are applied during scheduled OT downtime or compensating controls can be put in place until such time.

TCVM considers:

- The criticality of vulnerabilities
  - CVSS score
  - Potential exploitation impact
- The context of vulnerabilities, including asset criticality and exposure
  - Internet or third–party access
  - Business value and data sensitivity
  - Surrounding network topology and security controls
- The assessment of the threat
  - Active exploitation in the wild
  - Availability of sample exploit code
  - Used in malware, exploit kits, etc.

## Benefits of a Unified View

A unified view of the attack surface across the entire environment helps you:

**1. Understand network context with full network modeling and mapping:**

- All routing paths on the networks
- Device and configuration checks (hardening)
- Dynamic access analysis (processing LAN/corporate LAN/engineering P2P network)
- Communication discovery between OT assets (ISA99/IEC62443 level)

**2. Confirm effective controls through firewall and access control analysis:**

- Policy compliance (e.g., for NERC, FISMA, NIST, ISA99/IEC62443 level)
- Platform security
- IPS analysis
- Ruleset cleanup and optimization
- Secure change management

**3. Identify vulnerabilities and prioritize patching with complete context:**

- Scanless assessment for passive, non–intrusive vulnerability discovery
- Intelligent remediation prioritization identifying exposed vulnerabilities and those exploited in the wild
- Prioritized patching process
- OS and protocol–based risk assessment
- Identification of compensating controls when patching isn't an option

So, how do you know what is exposed in your networks, which risks are the highest priorities and what assets are most likely to be compromised in an attack? How can you get better visibility into what is happening across your entire environment in order to ensure security?

## WHAT TO LOOK FOR IN A UNIFIED IT–OT NETWORK SECURITY SOLUTION

To achieve the kind of comprehensive visibility needed to secure converged networks, look for solutions that offer the ability to passively collect information and completely model all networked environments — including your entire OT network.

Passive collection of OT network assets can be achieved by connecting monitoring sensors to the SPAN/mirroring port of network switches, so that they can forward asset flows and real–time threat information to a command center. Look for solutions that natively interface with enterprise systems such as SIEM solutions, authentication servers and third–party platforms, as this makes it easier to correlate information and security actions. Capabilities to look for include:

- Deep packet inspection (DPI) engine–powered device to collect OT data passively from monitoring sensors, including:
  - IP/MAC address
  - Vendor and model
  - Device role
  - Protocols/services, commands
  - Number of links and data flows to other devices
  - Sent/received bytes
  - OS version and host name
  - Network topology
  - ISA99/IEC62443 level Network Level (0–5)
- Asset inventory and management including dynamic business asset classification
- Vulnerability management of OT and IT vulnerabilities, including those with and without CVE identifiers
- Security anomaly detection engine
- API integration with IT security management tools
- Broad ICS protocol support

Integrated security management solutions enable visibility of both the IT and OT network by receiving all the asset information that the sensors see, combining that information with other data sources (e.g., controls configuration and asset management) and building it into a comprehensive, visual and interactive model.

An effective solution will be able to:

- Highlight an organization's full attack surface, including vulnerabilities in both the OT and IT network to determine potential attack path exposures.
- Analyze network paths end to end — between and within IT and OT networks — to assist in configuring access policy and running analysis for access compliance reporting, among other purposes.
- Alert users to issues requiring immediate response (e.g., zero–day ICS vulnerabilities based on the PLC firmware version or a critical pivot point such as an OPC workstation that has a WannaCry vulnerability).
- Identify key compliance issues (e.g., a dual–homing engineering station with interfaces to both the OT and IT networks has created a bypass, a new communication exists from a PLC to an unknown host or a violation of Critical Control #10 of the NERC CIP standard has occurred).

In this way, a unified solution brings unparalleled visibility into the IT–OT attack surface so you can literally see what's going on, understand the interconnectedness of your environment, pinpoint your biggest risks and plan for how to deal with them.

## SUMMARY

Businesses will continue to expand the connectedness of OT systems. Being able to read, reach, update, adjust or control OT systems from anywhere has significant business value. But these advantages come at a cost, and those responsible for security in IT–OT networks need to have the right security tools to fit the unique needs of the security challenge at hand. A unified approach to IT–OT security management based on model–driven, comprehensive visibility gives organizations:

- Non–intrusive security oversight of production networks to minimize downtime
- Contextual understanding of risk throughout the entire IT–OT environment
- Improved communication between IT and OT security stakeholders via a common and complete view of the attack surface

An effective unified approach dissolves the traditional organizational challenges between IT–OT teams, so that OT engineers can focus on maintaining services without becoming security experts, and IT security has the insight they need to effectively understand and manage risk.

### NEXT STEPS:

Read more about how Skybox Security unifies IT, SCADA and ICS network security.

Read the technology brief on securing OT networks with Skybox Security.

## ABOUT SKYBOX SECURITY

Skybox™ Security provides the industry's broadest cybersecurity management platform to address security challenges within large, complex networks. By integrating with 120 networking and security technologies, the Skybox™ Security Suite gives comprehensive attack surface visibility and the context needed for informed action. Our analytics, automation and intelligence improve the efficiency and performance of security operations in vulnerability and threat management and firewall and security policy management for the world's largest organizations.

## ABOUT SKYBOX FOR OT

Skybox for OT™ gives organizations with hybrid IT–OT environments the comprehensive visibility they need to ensure security and compliance standards are met throughout their networks, risks are systematically reduced and operations run smoothly.

Skybox for OT offers passive network monitoring and situational awareness that provides instant visibility and cyber resilience for OT networks. It discovers all IT and OT devices, building them into one unified model to give insight to networks, assets and vulnerabilities with full context. The Skybox solution delivers a complete risk, compliance and exposure posture, empowering organizations to take preventive actions such as improving security control configurations, prioritizing patching or using IPS shielding to block access to known exposures in the network.

Benefits of Skybox for OT include:

- Visibility of your entire attack surface to better defend and protect critical assets
- End–to–end path analysis from any source to any destination, including between and within networks, to identify potential attack vectors and ensure policy compliance
- Insight into vulnerabilities, their exposure and use in the wild
- Automated processes and orchestration to maintain uptime and avoid costly or dangerous disruptions

SKYBOX SECURITY

www.skyboxsecurity.com | info@skyboxsecurity.com | +1 408 441 8060