OT Security for Facilities Systems

Ensuring Their Safety, Accessibility and Availability

Understanding OT Security Risk

This eBook will focus on operational technology (OT) in facilities systems.

OT is defined as all non-IT devices connected to the network. Examples of facilities systems include network-connected smart buildings, food preparation and storage equipment, manufacturing, warehousing, and production equipment and devices.

Network connectivity gives hackers an opportunity to compromise devices and disrupt operations. The primary sources of OT security risk and vulnerabilities are caused by default passwords, unpatched software, misconfigurations, or non-authorized access leading to successful exploits.

Unmanaged or improperly managed OT devices can result in:

- Reduced device availability
- Decreased safety
- Financial exposure
- Reputational and public relations risk
- Loss of revenue
- Compliance and regulatory issues

According to the 2019 Ponemon Security in Operational Technology Report[1], over 60% of respondents mention concern about an attack against OT. Fortinet's 2020 State of Operational Technology and security report [2] shared that 65% of organizations surveyed experienced at least three OT intrusions, up from 18% in 2019. As OT tech becomes more advanced, so do the security concerns surrounding it.

There is a growing realization that addressing device threats and vulnerabilities means a commitment and collaboration on people, processes, and technology from both the teams overseeing and maintaining OT devices, and the IT team.

This eBook provides an understanding of how modern OT security works and why it is important to select, deploy, and operationalize these capabilities to protect devices—and your reputation—on a sustainable and cost-effective basis.

Closing the Gap in OT and IT Security

IT security has been in place for decades, and the tools to protect IT devices often work well. Securing traditional IT devices is generally a high priority for an organization. In contrast, the teams overseeing OT devices have focused less on security and more on resiliency, performance, and safety.

Now, there is an increasing awareness that addressing OT security requires an organizational and financial commitment. A new era of collaboration between line-of-business device owners and IT is essential to meet growing threats to OT. Process improvements and modern, cloud-based service management technology are also essential to address a complicated set of challenges. IT security teams have the benefit of mature active monitoring capabilities, vulnerability management tools, and nearly universal remote remediation capabilities for IT devices.

Most of these tools and resources are not available or cannot be used for OT security.

- Active monitoring cannot be performed on most OT devices because the installed operating system is often not configured to withstand active monitoring tools. In many cases, active monitoring may cause these OT devices to crash or become unresponsive.
- Passive monitoring is the standard and can provide needed data without interacting directly with the device. Specialized passive monitoring tools sniff the network and can identify and classify operational device or OT signatures.
- security remediation for OT devices can only be executed by authorized, trained, and certified technicians and engineers, not IT security teams
- Specialized skills, training, tools, and experience are required for OT security remediation
- In some cases, OEM or third-party service providers must be utilized to perform OT security corrective maintenance activities versus internal device technicians or IT security teams.

These issues can be complicated by the historical gaps, culturally and organizationally, between IT and device support teams. Closing the gap is critical as more sophisticated and determined attackers are actively exploiting network-connected devices as new and highly vulnerable entry points into your enterprise. The threat is real and growing, and a new era of cooperation is essential

> Closing the gap is critical as more sophisticated and determined attackers are actively exploiting network-connected devices as new and highly vulnerable entry points into your enterprise.

People, Process & Technology

OT security requires more than just ensuring compliance with best practices. Because it directly impacts the safety, accessibility, and availability of business-critical devices, fundamental questions must be answered as part of maintaining a strong security posture.

- When do you know critical OT devices are safe to use?
- How can you confirm the availability of your OT devices?
- How do you make sure your OT devices are accessible when you need them?

People

Your device support teams need a trusted OT inventory resident in a single database, available wherever they work on a mobile device, tablet, or laptop. Team leaders need accurate reporting on OT inventory with information reflecting condition, disposition, and location of all OT devices. The security operations center (SOC) needs OT device monitoring information that empowers them to monitor OT device security and activity on the network.

Process

You need a way to accurately capture the OT device lifecycle, as part of a standard onboarding process Without this, it's difficult to determine details about device disposition, maintenance, and security. When an OT device security threat, vulnerability, or exploit occurs, timely remediation can be difficult or impossible to achieve with the absence of a common data model for matching, contextualization, and OT security event correlation. The process of creating a standard data model enables the technology to perform to expectations. Without this process commitment, the technology will not meet expectations and risk will remain persistent.

Technology

Having multiple CMMS, EAM, IWMS, or other service management technologies will prevent an organization from achieving a successful OT security posture. This is because these technologies operate in isolation to each other, so making informed decisions about OT security is complex and time-consuming. Consolidating legacy maintenance software onto a single, modern, inventory and service management platform is a key first step for an enterprise. Without this commitment, the organization will struggle and accrue security risk over time.

Disparate technologies for managing OT devices add enormous complexity, cost, and risk when a security event takes place. How can your devices be matched to security threats if there is no standard data model? How can your device support team understand what other devices are potentially at risk? It is essentially impossible at scale to manage OT security across multiple inventory and service management technologies with disparate data. Consolidation and a common, standard data model are the only options.

Connected Device Discovery – The Intersection of OT and IT

How do you discover and monitor OT devices that live on your network? The two most common options are to acquire new OT discovery technology or use a third-party service provider. With either option, the key to success is then pairing your selection with a single, modern service management platform for OT that you own and operate. The service management platform is where the security discovery data is ingested, contextualized, and acted upon in a way that mitigates threats and drives remediation work activities. The platform must be authoritative in nature and contain the trusted OT inventory.

A single, trusted OT inventory system helps your organization manage the full network-connected device lifecycle. Regular, ongoing updates to inventory data take place when the device support team performs routine preventive maintenance (PM) or corrective maintenance (CM), provisions new devices, or installs or updates OT device firmware or software.

The OT inventory system includes—but is not limited to—data such as

Owner	Location	Serial number
Device make	Department	Latest software version
Model	Usage	Maintenance history

When a security event happens, the discovery payload is received by Nuvolo and enriched by the service management and inventory data. This enrichment process enables the data security, IT, and device support teams to all be operating with the same data for the first time. Having everyone on the same page is essential for visibility and rapid remediation of OT security events.

.

Trusted Device Data with Monitoring and Remediation

An essential part of safeguarding network-connected OT devices is ensuring persistent visibility using OT discovery tools to prevent blind spots. Monitoring and discovery of OT should be a standard activity for security professionals, with an appreciation and understanding of the growing importance of these devices as part of business operations.

The resources mentioned above help analyze vulnerabilities and provide security event assessment and remediation recommendations. It is critical that only trained, certified, and authorized resources are utilized or dispatched to remediate affected OT devices. A key driver here is regulatory mandates. For example, a device manufacturer may require only certified, authorized personnel to work on an OT device for warranty or compliance reasons.

When a security event takes place, the IT security team will be able to see the full context of the OT device. They'll know who the device owner is and what remediation process must be followed so a work order can be dispatched to a qualified OT device technician. Using a single, modern platform, all activities are tracked, time stamped, date stamped and available as data for reporting and compliance purposes. In this model, information security, IT, and the device support teams have full visibility and reporting on all activities for remediation.

This combination of device expertise, modern technology, and well-documented and operationalized processes helps keep the connected device fleet safe and resilient in the face of rapidly growing OT security threats.

OT and IT Teams - Using the Same Data Means Faster Remediation

When there are thousands of connected OT devices in use in your organization, it's critical to have a scalable, orchestrated, and automated response process to security events. A best-practice automated response process is outlined below.

Intelligence Hub

- Supports All OT Discovery Tools
- Device Profiles in Common Data Model
- IT and OT Teams Can See the Same Threat Data

Automation

- Correlation
- Orchestration
- Automates Intake of OT Security Events

Workflow

- Collaboration
- Gain Context

Response

- Work Dispatching
- Work Order Management

This approach to OT security is where Nuvolo OT Security provides:

- The ability to receive data when authorized OT devices are added to the network
- Single system of inventory
- Common OT data model workflow and orchestration
- Matching capability for "like" affected devices
- Dispatch
- Tracking and reporting

Bringing It All Together

Nuvolo provides a single, trusted inventory system for OT that helps enterprises manage the entire connected device lifecycle. Regular, ongoing updates take place when the device support team performs tasks such as routine planned or corrective maintenance, provisioning new devices, or installing OT device firmware or software updates.

When an OT device is connected to the network or an OT security event takes place, Nuvolo receives that information from device discovery and monitoring tools, creating an intelligence hub of device and event information. This allows Nuvolo to leverage an existing discovery tool, natively embedded as part of the solution. Alternatively, if the enterprise has already purchased and operationalized an OT discovery tool, the intelligence hub allows for easy integration.

These features enable the information security and device support teams to see the full context of the device. The intelligence hub also helps facilitate full knowledge and visibility of a device affected by a security event, including theater of operation, device owner, designation, and many other attributes, as well as the remediation process to be followed.

Nuvolo enables this seamless approach, accelerating remediation and improving quality and safety when OT security events occur.

[1] https://lookbook.tenable.com/ponemonotreport/ponemon-OT-report

[2] https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-state-of-operational-technology.pdf