Building Proactive Defenses Against Advanced OT Threats
# Table of Contents

- Executive Overview ................................................................. 3
- Advanced Attacks Against OT Are Increasing ......................... 4
- Modern OT Security Requires Visibility, Control, and Awareness .. 6
- A Comprehensive Solution for Securing Industrial Operations .... 9
  - Prevention ............................................................................... 9
  - Detection ............................................................................. 12
  - Response ............................................................................. 13
- Putting a Strategic Security Plan Into Action .......................... 14
Executive Overview

Industries that utilize operational technology (OT) are under pressure to maintain the highest levels of uptime, availability, and safety. This includes critical infrastructure (e.g., hydroelectric dams, nuclear power plants, oil and gas pipelines)—where a system failure can directly impact human lives or the environment. But as OT systems evolve to increasingly interact with information technology (IT) systems, this convergence is creating new pathways for bad actors to disrupt these sensitive environments. Plant managers and operations leaders are seeing an onslaught of attacks targeting OT systems. Some even use sophisticated techniques (e.g., agile development, polymorphism) that make it more difficult to identify, detect, and remediate attacks. To address these sorts of advanced threats, organizations need purpose-built OT security solutions to help them instantly prevent, detect, and respond to these threats—before downtime or critical damage can occur.
**Advanced Attacks Against OT Are Increasing**

Traditional OT systems are widely regarded as the most vulnerable assets inside an organization. At the same time, sophistication of attacks against OT systems is growing. Older threats are reinventing themselves and coming back stronger than ever. And as OT environments increasingly converge with IT technologies, cyber criminals are maximizing their opportunities by simultaneously targeting both older vulnerabilities as well as new ones that appear on an expanding attack surface.¹ For example, malware attacks are now specifically being designed to target vulnerable industrial control (ICS), supervisory control and data acquisition (SCADA), and safety systems.²

Unfortunately, many threat attempts become successful breaches with significant consequences—impacting the organization’s operational efficiency and/or revenue. As a 2020 survey revealed, 90% of organizations experienced at least one OT system intrusion in the past year—and 65% had three or more (an increase of 18% since 2019).³

The main reason behind this rise in OT-based cyberattacks is the convergence between IT and OT networks. Increased digitization of OT technology increases the need for connectivity, often across IT networks. This connectivity renders the traditional air-gap protection of OT environments a thing of the past. In response to these new exposures, many organizations have tried deploying an array of individual point security solutions to block security gaps one at a time. Those who manage OT operations find themselves stuck in a reactive stance while trying to protect environments with uniquely sensitive requirements.⁴

As air gaps are removed around the world, OT systems are increasingly barraged with both recycled IT-based attacks and purpose-built OT exploits.⁵
Only 8% of respondents to a 2020 OT security survey reported zero intrusions over the past 12 months, a decline of 18% compared with the previous year’s report.\textsuperscript{6}
Modern OT Security Requires Visibility, Control, and Awareness

Improving OT security is not easy, as planned downtime is required for testing, installation, and maintenance. But with increasing IT-based exposures and higher numbers of attacks, point security approaches cannot keep OT systems safe from disruptions. Disaggregated security architectures lack the ability to share threat information across the organization and provide coordinated responses to sophisticated attacks. Effective protection requires a platform-based approach—purpose-built security solutions that are connected and fully capable of sharing threat intelligence in real time.

Digitization of industrial environments is opening doors for adversaries to maneuver both north-south (from outside to inside OT environments) and east-west (laterally across the entire organization). Without the ability to immediately spot threats early in the attack cycle, damages tend to compound. The time from an attacker’s first action in an event chain to the initial compromise of an asset is typically measured in minutes—while the time to discovery is more likely to be months. An integrated security platform also enables automated responses that can contain threats from spreading without disrupting specific OT systems or broader operations.
Operations managers need purpose-built OT security that covers three essential needs for protecting their environments:

- **Visibility.** A majority (78%) of organizations have only partial centralized visibility of their OT environments.\(^8\) This is a foundational problem in that they cannot protect any parts of their infrastructure that they cannot see.

- **Control.** Extensive points of enforcement, dependent on each OT system and subsystem doing its job—and only its job.

- **Awareness.** Continuous security monitoring to detect anomalies. This includes ongoing analysis of user and device behaviors (learning what, where, when, who, and how) to provide actionable intelligence about any potential known or unknown threats.

\_[The current time it takes to identify and contain a single breach is an average of 280 days.\(^9\)](\)
IT/OT convergence may be the root of today’s security challenges, but it is also the foundation for a durable solution in enabling delivery of accurate, actionable information.
A Comprehensive Solution for Securing Industrial Operations

Time is a critical multiplier in any breach situation, but especially so with OT systems. Manufacturing and plant operations managers need to close any and all windows of exposure. When preparing a defense against advanced threats, organizations should evaluate integrated solutions that provide real-time threat prevention, detection, and response capabilities.

**Prevention**

Preventing threats from entering the organization starts with implementing role-based controls. All devices and users need to be authenticated before they can access the OT environment or any of its segmented assets. Applications used within the OT environment can be limited to only those on a preapproved list.

**Intent-based segmentation** capabilities can limit lateral movement of malicious exploits across the organization. Network segmentation provides defense by design by instituting checkpoints for transparent visibility and detection of threats.
A majority (78%) of organizations plan to increase budgets for securing industrial control systems this year.

Patching sensitive OT systems can also present issues. To avoid production disruptions, operations teams are often forced to follow the mandated change process that only allows mitigation within a scheduled maintenance window. In the meantime, the systems are vulnerable to attacks. Security with **virtual patching** capabilities can help proactively mitigate these risks without taking systems offline between scheduled maintenance windows.

A **next-generation firewall** (NGFW) with third-party validated performance for blocking advanced threats is a central component of any platform-based security infrastructure. The NGFW should be able to share threat intelligence with all other integrated security solutions deployed across the organization to help prevent coordinated attacks.
Top-tier OT organizations are 51% more likely to use network segmentation than bottom-tier organizations.¹²
Detection

Detection of unknown threats requires the ability to filter, inspect, and analyze threats in virtual environments—safely isolated from sensitive systems. **Sandboxing** has shown proven effectiveness in detecting emerging and zero-day threats. A sandbox solution isolates suspicious objects from general traffic and observes it in a simulated environment. If analysis confirms it is malicious, the solution then automatically initiates mitigation. But in order to effectively protect industrial environments, the sandbox must specifically support the types of operating systems found in OT environments.

**Endpoint detection and response (EDR)** solutions are not only able to identify sophisticated attacks but also prevent any unknown application (such as ransomware or other malware) from executing until it has been analyzed. Ransomware in particular has been an increasing problem for OT managers.\(^{13}\)

OT security architectures also benefit from **deception decoys** (also known as “honeypots”) that emulate OT-specific equipment. These solutions lure attackers away from an organization’s valuable assets and then trick them into revealing themselves.

Insiders account for a significant percentage of intrusions, usually through negligence, but sometimes with malicious intent. An advanced threat detection and mitigation strategy should incorporate **user and entity behavior analytics (UEBA)** to track any potential inside threats to the organization.

*Regulations can provide an excellent starting point for basic security controls. But even regulated organizations can find themselves without a clear direction forward as they try to establish advanced security controls around the OT side of their environment.*\(^{14}\)
Any and all detection solutions will not be fully effective if they operate in silos. In addition to an integrated security architecture, OT environments also need **centralized security information and event management (SIEM)**. SIEM collects logs and analyzes security events along with other data to speed threat detection and support security incident and event management, as well as compliance with industry regulations. This helps reduce threat risks as well as the workflow burden on under-resourced security teams.

**Response**

Integration across the security infrastructure is essential to enable the aggregation of data from prevention and detection solutions. This, in turn, can provide contextual awareness of a threat so that **automated security responses** can be taken. Once an advanced threat is detected, security solutions that are integrated as part of a connected architecture can instantly block similar threats across the OT attack surface. Coordinated threat-intelligence sharing across IT and OT systems can extend these benefits across all parts of the business.

An effective solution should also offer the ability to **quarantine devices or allow them to run infected** after alerting admins, depending on the context of the system. Some OT equipment cannot automatically be taken offline without operational repercussions.

In addition, an effective OT solution is one that offers the ability to create **“automatable” playbooks** for faster responses. This minimizes human analysis and decisions, which impede fast remediation. At the same time, it should keep human intelligence in the response loop in order to prevent overreactions.

In early 2020, a ransomware attack against a natural gas facility in the U.S. resulted in a two-day pipeline shutdown while systems were brought back online from backups.15
Additional **recovery capabilities** should be addressed for:

- Observing network traffic and imitating threats
- Continuous learning of threat behaviors
- Rolling back compromised (e.g., ransomware-infected) systems to a previously known good state. For example, some EDR solutions can defuse threats post-infection to prevent data exfiltration, lateral movement, file tampering, and ransomware interference with system operations.

**Putting a Strategic Security Plan Into Action**

Without question, most OT environments urgently need more effective security measures in place to address the growing volume and variety of advanced threats. When evaluating solutions to evolve their security architecture, operations managers should ask:

- Can the security infrastructure be integrated so that threat intelligence is shared in real time across all security elements to block concurrent attacks?
- Does it include segmentation capabilities to control the flow of threats on both north-south and east-west vectors?
- Does the solution offer automated incident response and event management workflows to mitigate successful intrusions before they propagate and have an impact?
- Does it include advanced threat- and breach-detection capabilities such as sandboxing and decoys?
- Does it offer automated responses to help shrink attack windows and control access to network assets post-intrusion?


