FORTINET

How to Manage the Complexities of Operational Technology

Strategic Recommendations for the CISO

Table of Contents

FORTINET

Executive Overview

Securing operational technology (OT) networks is increasingly complex. Driving this complexity are numerous manual cybersecurity processes, the convergence of OT and information technology (IT) networks, and the lack of security transparency and centralized controls. A security skills shortage and gaps in specific skill areas exacerbate the situation, ratcheting up the complexities of security management. To address these complexities, CISOs in OT environments need to look for solutions that 1) automate manual intrusion prevention, detection, and incident response processes, 2) implement systems to achieve integrated IT and OT security transparency using centralized controls, and 3) automate manual compliance and audit tracking and reporting. These initiatives enable CISOs to scale their overstretched teams through improved efficiencies, while allowing them to manage threats faster and more effectively.

01 Security Complexity Creates Risk and Inefficiencies

The complexity of security has never been greater. Digital transformation (DX) is expanding the attack surface through cloud adoption, growth in Internet of Things (IoT), increases in mobility, and more. In response, organizations—both those with OT systems and devices, which are often designated as industrial control systems (ICS) that are accessed through supervisory control and data acquisition (SCADA) graphical user interfaces, and those without—are adding more point security solutions. This fragmentation creates greater complexity.

Removal of the air gap between IT and OT environments—whereby OT systems and devices were previously not connected to the IT network—presents new risks and complexities. Introduction of new government and industry regulations, along with adoption of cybersecurity frameworks, only adds to the complexity.

While CISOs are responsible for security in only 9% of OT organizations today, this is going to change very soon, with 70% of OT organizations indicating they plan to roll security underneath the CISO this year.[1]

02 Minimizing Cybersecurity Complexity: Recommended Practices for OT CISOs

CISOs in OT organizations can reverse trends toward greater complexity by implementing solutions that adhere to several basic principles. These focus on integrating fragmented security architectures and automating manual processes. The three principles, covered in the pages that follow, include:

- Achieving integrated IT and OT security transparency and centralized controls
- Automating manual intrusion prevention, detection, and incident response
- Automating manual compliance and audit tracking and reporting

Achieving Integrated IT and OT Security Transparency and Centralized Controls

The ability to achieve transparency and centralized controls involves two key challenges: 1) use of point security approaches versus integrated solutions and 2) the limited visibility that results from siloed architecture.

The downside of point product approaches

It is common to deploy best-of-breed, point product security solutions to solve different security challenges. However, point security solutions are not integrated and work in silos. As a result of this fragmented approach, security becomes complex and difficult to manage (see Figure 1).

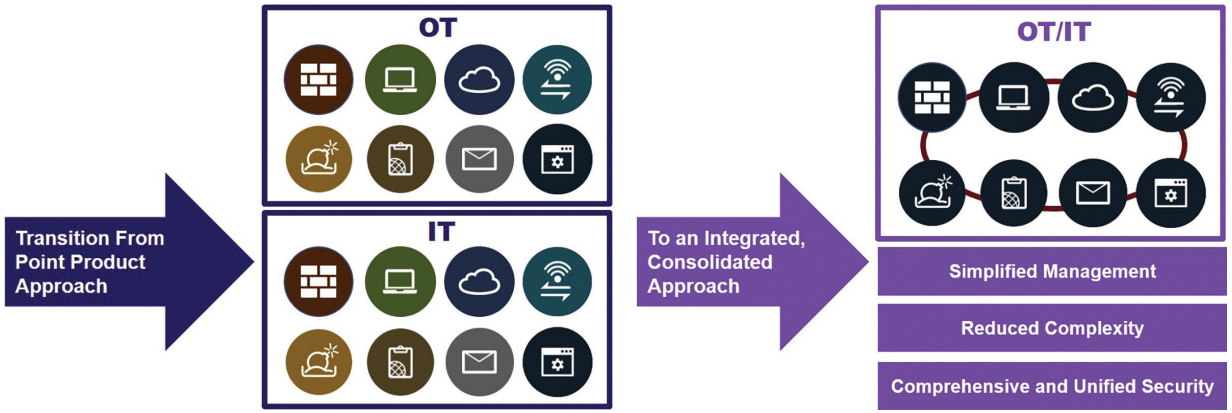

Figure 1: The Need to Bring OT and IT Security Together. A point product security approach—with different security products in IT and OT environments—adds complexity, is difficult to manage, and introduces security gaps. A unified solution simplifies management and reduces complexity.[2]

Limited visibility

A siloed security architecture not only increases complexity but also degrades an organization's security posture. Part of the reason for this is siloed visibility, which makes it easier to miss an attack to one silo before it impacts others. Regarding this lack of security transparency, the adage "you do not know what you cannot see" may be apropos.

78%

of OT leaders indicate they have only partial centralized visibility on the cybersecurity of their OT environment.[3]

Recommendations: Achieving Integrated IT and OT Security Transparency and Centralized Controls

To address these challenges, an OT cybersecurity approach must include:

- **Broad visibility** of the entire digital attack surface, spanning OT and IT environments
- **Integrated protection** across all devices, networks, and applications, sharing global intelligence on advanced threats
- **Automated operations and response**, driven by machine learning
- **Simplified management** from a single pane of glass

The security architecture should continuously provide a trust assessment of devices and workloads, dynamically adapting as network configurations change. Further, the different security elements need to operate as a unified whole, offering optimal total cost of ownership (TCO) for overstretched cybersecurity teams in OT organizations.

Automating Manual Intrusion Prevention, Detection, and Incident Response

The need for automation stems from the rapidly evolving threat landscape and the need for rapid detection and response. Each of these is addressed below:

Rapidly evolving threat landscape

The threat landscape is rapidly evolving, and detecting and preventing malicious attacks is becoming increasingly difficult. For example, 97% of malware infections are polymorphic today, meaning the virus changes its signature each time it replicates itself.[4] According to a recent survey, nearly two-thirds (64%) of OT leaders say that keeping pace with change is their biggest challenge.[5] Manual processes for intrusion prevention, intrusion detection, and incident response are an inefficient way to keep up with evolving threats.

Rapid detection and response needed

Threats now move at machine speed. Malicious intrusions execute their payloads faster and quickly move across and between IT and OT networks and devices. As a result, the windows for incident detection and response are quickly shrinking.

The amount of time spent remediating intrusions is a growing issue for most organizations and consumes valuable resources. As an example, the time legal and cybersecurity teams spent responding to intrusions increased 20% over the past year—to an average of 19.4 days annually.[6]

But with the right detection, prevention, and response solutions in place, organizations can drive down their costs. One study finds that organizations that identify breaches in less than 100 days save more than $1 million as compared to those that take more than 100 days to do so. Similarly, companies that contain breaches in less than 30 days save over $1 million as compared to those that take more than 30 days to resolve them.[7]

The damages that successful intrusions and breaches incur can be dramatic. In many cases, even a brief OT system disruption (e.g., an assembly line interruption) can cause an organization to incur very high reset costs, damaged material costs, lost revenue, and other costs. With manual detection, prevention, and response processes in place, OT organizations simply cannot keep up with the pace of many advanced threats. The solution is to employ automation, which only comes through an integrated security platform.[8]

Recommendations: Automating Manual Intrusion Prevention, Detection, and Incident Response

Organizations should *automate* manual prevention, detection, and incident response by integrating siloed security tools into a unified security architecture. Automation should adhere to the following principles:

- Automation of network operations:
  - Helps DevOps teams to focus on time to market
  - Improves operational efficiencies through zero-touch provisioning
  - Generates real-time insights around branch network performance involving issues such as spikes, scaling, and priority routing of traffic
- Automation of security operations reduces risk through proactive threat detection, threat correlation, intelligence-sharing alerts, and threat research and analysis.
- Integration of IT service management (ITSM) tools unlocks automation of event analysis and response. This reduces response times from days to minutes or even seconds.

By following these principles, CISOs in OT organizations can protect their environments from advanced threats designed to exploit ICS and SCADA.

Automating Manual Compliance and Audit Tracking and Reporting

In addition to security compliance issues, CISOs also face regulatory and industry compliance requirements. Compliance is a critical part of an OT cybersecurity strategy and presents different challenges than purely security-related issues. While a compliant OT environment is not necessarily a secure one, it is an important starting point for getting the right security architecture in place. Compliance initiatives also differ by sector (see figure 2 for examples).

Sector	Region	Regulatory Initiative
Manufacturing	U.S.	NIST Cybersecurity Framework
	EU	NIS Directive
Energy and Utilities	U.S.	NERC Cybersecurity Standards
	EU	NIS Directive Tool for Energy
Transportation	U.S.	TSA Cybersecurity Roadmap
	EU	NIS Directive Tool for Transport

Figure 2: Sample Cybersecurity Initiatives by OT Sector.[9]

Just as organizations must shrink their detection, prevention, and incident response timelines, they also need to reduce their windows for reporting data breaches. For example, rather than having weeks to report discovery of intrusions, organizations have 72 hours under the European Union's General Data Protection Regulation (GDPR).[10] Noncompliance with these notification requirements can quickly lead to millions of dollars in fines and penalties.

CISOs can no longer rely on manual compliance and audit tracking and reporting, which consumes valuable IT and OT staff time that is in short supply while also slowing compliance audit responses. In response, CISOs require a security platform that uses automation to transform manual processes into automated ones. The result must include dashboards for the CISO, CIO, CEO, and even the board of directors. Automation of these processes can save security teams myriad hours in manual log aggregation and correlation—tasks that are particularly onerous with a disaggregated security architecture lacking transparent visibility and centralized controls.

Recommendations: Automating Manual Compliance and Audit Tracking and Reporting

Any solution that addresses compliance must also *address and automate* security standards and frameworks such as those from the Center of Internet Security (CIS) and the National Institute of Standards and Technology (NIST). This also includes the top 20 critical security controls from the SANS Institute.[11] Following are some examples:

- **Visibility.** Single-pane-of-glass transparency enables organizations to monitor all aspects of OT and IT, including security, performance, availability, and change management. This visibility must include whether an organization is in compliance with relevant security regulations.
- **Access control.** User activities need to be tracked to ensure compliance with security policies. They also must leverage multiple authentication technologies for restricting user access, including two-factor authentication, identity management, and network access control.
- **Secure configuration.** Organizations need to be able to define security policies based on business requirements to ensure consistency and enhance compliance. Definable business logic needs to extend to log management.
- **Auditability.** Tracking of security and compliance factors needs to identify instances of noncompliance and enable automated incident response. This includes the use of a security score that provides a comparison against peer and industry groups. Regulations supported should include Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), North American Electric Reliability Corporation (NERC), Federal Information Security Modernization Act (FISMA), International Organization for Standardization (ISO), Gramm-Leach-Bliley Act (GLBA), Good Practice Guide (GPG13), and SANS Critical Controls.

The above enables CISOs in OT organizations to maintain and demonstrate compliance with regulations and security standards without taking down OT systems that impact operational uptime requirements.

03 Integrate Fragmented Security Architectures and Automate Manual Processes to Maximize OT Cybersecurity

When evaluating different security options, CISOs in OT organizations need to consider the following questions:

- Does it address the entire attack surface and all of the different security elements by providing broad visibility?
- How well do the different security pieces integrate? Are these built into a holistic security platform?
- Does it simplify tracking and reporting of security and compliance issues and use integration to unlock automation of those processes?
- Does it dynamically adapt to network configuration changes and employ continuous trust assessments of devices and workloads?

[1] "State of Operational Technology and Cybersecurity Report," Fortinet, March 15, 2019.

[2] "A Solution Guide to Operational Technology Cybersecurity," Fortinet, April 15, 2019.

[3] "State of Operational Technology and Cybersecurity Report," Fortinet, March 15, 2019.

[4] Milena Dimitrova, "97% of Malware Infections Are Polymorphic, Researchers Say," Sensors Tech Forum, March 8, 2016.

[5] "State of Operational Technology and Cybersecurity Report," Fortinet, March 15, 2019.

[6] Patrick Spencer, "Cyber Resilience Rises to the Forefront in 2019, According to New Scalar Security Study," Scalar, February 20, 2019.

[7] "2018 Cost of a Data Breach Study: Global Overview," Ponemon Institute, July 2018.

[8] Patrick Spencer, "Cyber Resilience Rises to the Forefront in 2019, According to New Scalar Security Study," Scalar, February 20, 2019.

[9] "A Solution Guide to Operational Technology Cybersecurity," Fortinet, April 15, 2019.

[10] Mahmood Sher-Jan, "From incident to discovery to breach notification: Average time frames," International Association of Privacy Professionals, September 26, 2017.

[11] Tim Greene, "SANS: 20 critical security controls you need to add," Network World, October 13, 2015.

www.fortinet.com

430073-0-0-EN

June 15, 2019 1:00 AM

eb-ot-security-complexity