FORTINET

Understanding the Complexities of Digital OT Security

Four Challenges Facing Network Operations Analysts

Table of Contents

FORTINET

Executive Overview

Vulnerabilities in operational technology (OT) as a result of a growing number of connections with information technology (IT) have become a major concern for OT organizations. To address these security challenges, many organizations have added a broad selection of point security products to cover each new risk exposure. But this increases OT infrastructure complexity and introduces additional problems in terms of manual workflows, compliance requirements, and access control that the network operations analyst is charged to resolve.

The Convergence of OT and IT

OT business sectors include energy, utilities, manufacturing, and transportation. Their safe operation is often critical to public safety or even national and global economic health. Network operations analysts, as a result, are under pressure to simultaneously maintain security, operational uptime, and safety of these OT systems. With significant changes to how these systems are now being operated, however, network operations analysts must adopt new techniques for secure and efficient environments.

Traditionally, security was maintained by keeping IT and OT completely separate from one another—a process known as "air gapping." Isolation of vulnerable and delicate OT technologies protected them from most outside disturbances. But IT and OT are converging to achieve greater efficiency and business advantages. Indeed, nearly three-quarters of organizations now report at least basic connections between IT and OT.[1] Thus, for the majority of organizations with OT, the air gap is broken, exposing them to a growing number of internet-based attacks.

OT environments may include industrial control systems (ICS) that run equipment or machinery as well as the supervisory control and data acquisition (SCADA) subset systems that provide a graphical user interface for ICS. A SCADA or ICS system crash in manufacturing could stall productive operations for hours at a time, ruin sensitive materials mid-process at a cost of millions of dollars, and expose organizations to potential compliance penalties. Cyberattacks against critical infrastructure have the potential to do more than just grab headlines—they could be weaponized to cripple national defenses, obstruct access to resources, and even cause harm to innocent civilians.

Nearly three-quarters of OT organizations have experienced a malware intrusion in the past 12 months that caused damages to productivity, revenue, brand trust, intellectual property, and physical safety.[2]

Complex Security Causes Problems

As OT and IT increasingly intersect, many organizations have added point security solutions to compensate for the loss of air-gap protection. This increasingly complex and fragmented security infrastructure exposes new vulnerabilities that expand the opportunities for breaches. Point security products almost always operate in isolation—covering a single vulnerability or compliance requirement as an add-on measure. This approach inhibits visibility and intelligence sharing across the security infrastructure. Subsequently, network operations analysts rarely have clear and real-time insight into what is happening across their OT environment in terms of security.

The average enterprise uses 75 different security solutions, many of which address a single vulnerability or compliance requirement.[3] And while this number may not be as high in the case of OT environments, proliferation of point security solutions is a growing problem in OT. 31% of OT professionals in a recent webinar indicated their current OT security architectural approach is to employ fragmented point security solutions, and another 24% admitted they have no OT security architectural strategy.[4] These disparate products typically cannot share threat intelligence or coordinate responses across an increasingly dispersed organizational infrastructure. This increases response times to security events and raises the chances that critical OT systems are compromised and disrupted.

64% of OT organizations report a struggle to keep up with change.[5]

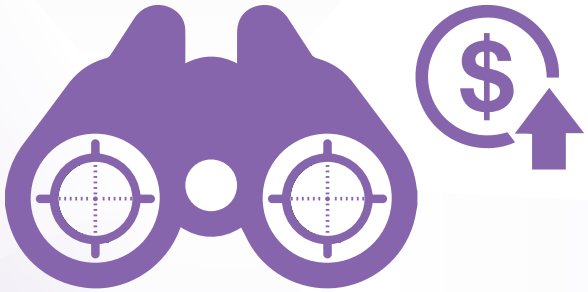
But the current problems of security complexity in OT are many—touching on compliance, auditing, staffing, costs, and efficiency. These complexity issues can be grouped into four key challenge areas:

1. Compliance management responsibilities

Many industry regulations—such as North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) or National Institute of Standards and Technology (NIST)—and data privacy laws—such as the EU's General Data Protection Regulation (GDPR)—require detailed auditing and reporting. In some circumstances, organizations can face fines that can reach millions of dollars per compliance violation—both for documented violations or even the inability to demonstrate compliance.

Compliance management is typically a very manual process. It often involves multiple full-time staff and can require months of work to get right. Data must be aggregated from multiple point security products and then normalized to ensure that regulatory controls are reported accurately. To do this, network and security staff must monitor security controls using each individual vendor's audit tools and then correlate that information to prove compliance. This complex and unwieldy auditing process is inefficient and can leave gaps in coverage or yield mismatched data.

The complexities presented by fragmented security solutions are further exacerbated by changes from regulatory bodies on compliance issues—either new regulations and standards or evolution in existing ones. Without an effective solution in place that offers automated tracking/auditing/reporting capabilities, organizations must expend substantial staff time to manually aggregate and reconcile data. Not only that, real-time compliance management helps organizations proactively manage security, identify vulnerabilities, and address risks before problems occur.



Compliance technologies that help better visualize risk are a top spending priority for enterprises—both over the next 12 months (57%) and within the next three years (51%).[6]

2. Maintaining uptime on sensitive, unpatched systems

It is very common for OT systems that may operate for 30 to 40 years to depend on outdated and unpatched firmware or software. But even newer systems are often consciously left unpatched. Because updating devices can require shutting down entire systems, many managers follow the "if it isn't broken, don't fix it" rule—or they only have time to patch the most critical systems in the small maintenance windows they get. Without regular patching and maintenance, OT systems can be very susceptible to common IT-based threats such as known malware attacks. To make matters more complicated, OT systems can be surprisingly fragile due to their age and lack of patching. Even security practices as benign as active device scanning can cause them to fail.

3. The manual burden on limited staff resources

Nearly two-thirds of OT leaders report that keeping pace with changes is their biggest challenge, and at the same time almost half (45%) are limited by a shortage of skilled labor.[7] The worldwide shortage of cybersecurity professionals has grown to nearly 3 million unfilled positions.[8] However, despite a shortage of staff resources, OT organizations are determined to improve their security posture.[9]

Fragmented security architectures inhibit automation capabilities that can alleviate the demands of expanding manual workflows on constrained staffs. This complexity also compounds security management due to a lack of visibility. A majority (78%) of organizations report having only partial cybersecurity visibility into OT.[10] This makes it difficult for teams to detect unusual behavior, quickly respond to potential threats, and perform threat analysis. Managing many siloed security solutions puts further pressure on short-handed OT organizations.

4. Access management controls

Network operations analysts also face complexity due to outsourcing pieces of OT management. Third-party vendors and partners are given greater access to OT environments, both remote and onsite—and more access from those outside the company means expanded exposure to the organization. But many organizations lack fine-grained controls that can define different roles for these sorts of users and limit what they can access. Complex and fractured security inhibits visibility of users and the ability to enforce uniform, policy-based controls across all parts of the security infrastructure.

But security complexity and lack of visibility can also contribute to access management problems for insiders as well. Verizon reports that 81% of breaches begin with lost or stolen credentials.[11] Many breaches in OT environments depend on spear phishing to obtain stolen credentials from users who have some form of access to the environment. This is a serious concern: an estimated two dozen U.S. energy grid companies were breached using spear phishing and stolen credentials within the past two years per *The Wall Street Journal*.[12] In these sorts of instances, attackers can even plant malware inside OT environments to be used for future sabotage.

Security challenges in OT are compounded by a lack of security expertise within in-house staff (40%), and even with the third-party vendors to which organizations outsource their security services (41%).[13]

The Path Toward Simplified OT Security

Complexity is the enemy of security. To ensure operational integrity of OT systems, network operations analysts must reevaluate their existing security architecture. Reducing the complexity and fragmentation of isolated point security deployments can improve compliance management, operational uptime, manual workflow burdens, and access management issues—as well as overall visibility and protection across the organization.

[1] "Independent Study Pinpoints Significant SCADA/ICS Security Risks," Fortinet, June 28, 2019.

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

[3] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating," CSO, March 14, 2016.

[4] "Securing the Future of Industrial Control Systems," Fortinet Webinar, June 26, 2019.

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

[6] Samantha Regan, et al., "Comply & Demand: 2018 Compliance Risk Study," Accenture, March 2018.

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

[8] "Cybersecurity Skills Shortage Soars, Nearing 3 Million," (ISC)², October 18, 2018.

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

[10] Ibid.

[11] 2017 Data Breach Investigations Report, Verizon, accessed November 30, 2018.

[12] Rebecca Smith and Rob Barry, "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It," The Wall Street Journal, January 10, 2019.

[13] John Maddison, "Is Converging Your IT and OT Networks Putting Your Organization at Risk?," CSO, May 09, 2018.

www.fortinet.com

391249-0-0-EN

July 31, 2019 7:51 PM

eb-complexities-digital-ot-security