FORTINET

Shortcomings of Traditional Security and Digital OT

Key Takeaways for Network Operations Analysts

Table of Contents

Executive Overview

Organizations across all industries are embracing new digital tools and services to accelerate and grow their businesses. The rapid adoption of these technologies has caused internet-connected information technology (IT) networks to increasingly intersect with previously isolated (and often difficult to update with patches) operations technology (OT) networks. This overlap also means that the ever-expanding IT attack surface now exposes OT systems to previously unknown threats within these environments. The result is that traditional security approaches are insufficient to protect connected OT environments.

63% of OT companies are increasing their cybersecurity budgets this year.[1]

Almost 80% of businesses are adopting new digital innovations faster than their ability to secure them against attack.[2]

01 When OT Met IT … A Network Convergence Story

Securing OT systems has become a crucial concern in industrial and critical infrastructure environments such as energy, utilities, manufacturing, communications, transportation, and defense. OT includes 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.

The value of OT assets can range into the billions of dollars and their safe operation is often critical to public safety or national/global economic health. A system crash on a manufacturing floor can stall production for hours and potentially ruin millions of dollars in materials. Having to reset a 10,000-gallon boiler processing caustic chemicals can have far more devastating consequences than any IT network outage. In other circumstances, a SCADA or ICS breach within critical infrastructure (such as a hydroelectric dam or nuclear power plant controls) could endanger the lives of workers and surrounding citizens. This puts network operations analysts under tremendous pressure to simultaneously maintain security, operational uptime, and safety.

Until recently, the best way to do this was to keep IT and OT completely separate from one another—a process known as "**air gapping**." It is very common to find OT systems that have been running 10-plus years with legacy operating systems that have no available security patches. Isolation of vulnerable and delicate OT technologies protected them from almost all outside disturbances.

But increasingly, IT and OT are being integrated for greater business efficiency, increased innovation, and competitive advantage. Nearly three-quarters of organizations report at least basic connections between IT and OT.[3] And this convergence has eliminated the de facto security of the air gap against common internet-borne attacks.

97% of organizations acknowledge security challenges because of the convergence of traditional IT and OT.[4]

02 The Attack Surface Expands

IT and OT convergence means that the ever-expanding range of threats that target IT networks now have pathways to attack OT as well—which vastly expands an organization's potential attack surface. To complicate matters even further, the delicate nature of OT systems means that traditional security approaches are insufficient to protect these environments.

When it comes to cybersecurity, existing OT defenses are much less evolved than their analogous security counterparts in the IT realm due to prior lack of investment and knowledge. So, OT decision-makers must modernize their security controls. And as the attack surface continues to grow and evolve with greater IT-OT connectivity, improving the OT security posture is also constrained by the need to keep up with rapid change and a lack of staff resources. Nearly two-thirds (64%) of OT leaders say that keeping pace with change is their biggest challenge, and almost half (45%) are limited by a shortage of skilled labor.[5]

All of these factors contribute to a heightened sense of awareness of OT across the enterprise, with the awareness making OT security a top priority.

About 74% of OT organizations have experienced a malware intrusion in the past 12 months, causing damages to productivity, revenue, brand trust, intellectual property, and physical safety.[6]

03 Security Incidents Are on the Rise

Where there is opportunity, there is exploitation. Threats targeting OT systems are on the rise.

The Triton attack on a petrochemical plant in Saudi Arabia[7] and the Ukrainian power grid failure that shut down electrical services for 80,000 customers[8] are just two high-profile examples in recent years. A majority of OT organizations report SCADA/ICS system breaches in the past year, a number that ranges from 56% to 74% depending on the study.[9] Politically motivated cyberattacks against critical infrastructure have the potential to do more than just grab headlines. They can be weaponized to cripple civil defenses, shut down production of vital resources, and even cause widespread harm to human lives.

The current lack of effective OT security contributes to these risks.

Successful intrusions resulted in the following damages at OT companies:[10]

- **Productivity, 43%**
- **Revenue, 36%**
- **Brand Reputation, 30%**
- **Business-Critical Data, 28%**
- **Physical Safety, 23%**

04 Key Problem Areas in OT Security

For network operations analysts, there are a few problem areas of interest that must be understood to approach a comprehensive solution for OT network security.

1. **Adding IT-based innovations brings IT-based vulnerabilities.** Automation and improved operational efficiency are driving forces behind OT and IT convergence. New digital technologies in OT require internet interconnections—and with the good comes the bad. "Industrial organizations have found practical applications for connecting devices to the internet, including cost savings, visibility, and efficiency. One problem that was not fully addressed in this quantum shift is that industrial controllers being opened up to the outside world have no defense mechanisms against cyberattacks."[11]

2. **Traditional security approaches are no longer effective.** The increasingly distributed nature of any modern network (IT or OT) has made traditional perimeter-only defenses an ineffective strategy. Many organizations allow a substantial number of wireless and Internet-of-Things (IoT) or industrial IoT technologies (such as smart environmental controls) to connect to their OT networks for greater efficiency. Most of these technologies are thought to be contained in a closed OT environment without their owners realizing that these devices are connected and therefore adding to the OT attack surface. IoT devices deployed within OT environments can provide backdoors for internet-based threats to reach vulnerable systems like SCADA and ICS. And because IoT devices themselves are typically headless—lacking the ability to support their own sophisticated, built-in defenses—they require holistic security from an outside source.

3. **OT systems can be hyper-sensitive.** Legacy OT systems can operate for 30 to 40 years and may depend on dated configurations that remain unpatched. Because updating devices can require shutting down entire systems, many operations managers follow the "if it isn't broken, don't fix it" rule. As a result, many older OT systems are notoriously vulnerable to malware and other threats that IT networks are naturally protected against. Complicating the problem even further, devices and systems installed in an OT network can be notoriously fragile when it comes to how they are secured. Even processes as benign as active device scanning can cause them to fail. This can become a case of both the disease and the cure potentially causing serious harm.

In light of this somewhat unique set of problems, OT network security must be fully reconsidered at a foundational level. And lacking many of the basic controls that IT networks have already adopted in recent years to address digital evolution and sophisticated threat exposure, this may seem a daunting task to take on.

A reported 78% of OT organizations only have partial centralized visibility of the cybersecurity deployed in their environments. 65% lack role-based access control, and more than half do not use multi-factor authentication or internal network segmentation.[12]

05 The Path Toward Comprehensive Network Protection

To be successful, security must become seamlessly integrated into OT environments without disrupting the often-sensitive nature of the systems in use. With an expanding attack surface, new threat exposures on multiple fronts, and a dearth of advanced threat protection solutions in place, network operations managers need to ask questions such as the following to determine their level of OT risk:

- ☐ How integrated are our IT networks and OT systems and what risks does this pose for the organization?
- ☐ Do we have transparent visibility across our OT environments or do SCADA/ICS reside in silos?
- ☐ Is the security for our OT and IT environments integrated and do we have single-pane-of-glass visibility and unified controls?
- ☐ How many headless OT devices and systems exist and what risk do these present to our broader OT and IT environments?
- ☐ Which OT devices and systems cannot be updated regularly and present a threat risk (and what does that risk look like)?
- ☐ How long does it take for us to respond to a threat detection across the entirety of our OT and IT environments?

There certainly are other questions that network operations analysts can ask, but the above is a good starting point.

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

[2] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon, March 6, 2019.

[3] "Independent Study Pinpoints Significant SCADA/ICS Cybersecurity Risks," Fortinet, May 7, 2018.

[4] Ibid.

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

[6] Ibid.

[7] Kelly Jackson Higgins, "Triton/Trisis Attack Was More Widespread Than Publicly Known," Dark Reading, January 16, 2019.

[8] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," WIRED, March 3, 2016.

[9] "State of Operational Technology and Cybersecurity Report," Fortinet, March 2019; "Independent Study Pinpoints Significant SCADA/ICS Cybersecurity Risks," Fortinet, May 7, 2018.

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

[11] Barak Perelman, "Interconnectivity Has Put ICS Environments in Cyber Risk Crosshairs," SecurityWeek, June 5, 2018.

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

www.fortinet.com

360405-0-0-EN

April 12, 2019 3:47 PM

eb-network-operations-analyst