FORTINET

Simplifying OT Security Complexity

Architectural Recommendations for the Network Operations Analyst

Table of Contents

FORTINET

Executive Overview

In response to the disappearance of the air gap between information technology (IT) and operational technology (OT) environments and an evolution in regulatory and security standards, organizations are adding point security products. But these make cybersecurity more complex to manage. This diminishes operational efficiencies, which is particularly problematic in the face of a cybersecurity skills shortage. It also ratchets up risks with complexity slowing an organization's response to threats and intrusions. Instead, an integrated security architecture offers network operations analysts a foundation for greater visibility, control, and automated capabilities to improve protection and reduce the burden on limited staff resources.

Increasing OT Complexity Introduces Risks

The challenges of greater security complexity and naturally fragmented infrastructures continue to enable a rise in cyber events and data breaches. Adding to the problem, the assortment of point security products deployed by most enterprises normally operate in isolated siloes. In most circumstances, these disparate products cannot share threat intelligence or coordinate responses across a progressively dispersed organizational infrastructure. This extends response times to security events and increases the chances that critical OT systems are compromised and disrupted, and critical data is stolen. Subsequently, network operations analysts need to find ways to simplify their security infrastructure to protect their OT environments.

Nearly three-quarters of organizations report at least basic connections between their IT and OT systems.[1]

With nearly 3 million unfilled security positions worldwide today—a number that is expected to grow in coming years—hiring skilled cybersecurity professionals has never been more difficult.[2]

Security Integration Provides Visibility and Control

Integrating these various security solutions into a unified security architecture converts a fragmented deployment of disparate products into a cohesive risk management system. It lays the foundation for comprehensive visibility across the organization, sharing threat intelligence in real time to help shrink analyst response times. At the same time, it enables manual workflows to be automated, which helps to alleviate the burden on constrained staff resources.

An integrated architecture also lays a foundation for comprehensive visibility and control. Maintaining security in any modern, complex environment requires broad visibility across all the silos and systems deployed to fully observe an organization's complete security posture. At the same time, the delicate nature of OT environments requires that this be done via passive (rather than active) scanning so as not to disrupt sensitive devices or systems.

The solutions should provide **centralized management** in the form of a single-pane-of-glass console that unifies controls of all deployed security solutions across the architecture. Specific security capabilities should include **network access control (NAC)** for both visibility of all devices connecting to the network along with dynamic and granular control of those devices. **Intent-based segmentation** limits access to OT systems in both east-west and north-south directions based on defined business needs (who, what, where). Establishing greater transparency and controls across the security infrastructure offers immediate benefits to protection, but there are additional ways that the foundation of an integrated security architecture can simplify and solidify OT defenses.

Streamlining Compliance, Auditing, and Reporting Workflows

Security integration also unlocks automation capabilities, including compliance audits, tracking, and ongoing reporting. Compliance management for international data privacy laws and industry regulations often involves multiple full-time staff and can require months of work each year. 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 often ineffective.

Reporting automation saves network operations analysts the countless hours of manual log aggregation and correlation associated with disaggregated security architectures that lack transparent visibility and centralized controls. As part of the integrated security architecture, advanced **security management and analytics** tools provide powerful and simplified network orchestration, automation, and response capabilities. These solutions can feature audit tracking capabilities and prebuilt reporting tools for easy-to-schedule delivery of reports based on business role—CEO, CIO, CFO, board of directors, and others.

For a majority of organizations, compliance technology is a top spending priority over the next 12 months (57%) and within the next three years (51%).[3]

Expanding Access Management Capabilities

Current OT complexity also goes beyond the infrastructure itself. It also includes the difficult job network operations analysts face in managing a growing number of users who include third-party partners, and vendors who have access to the OT environment in order to perform services. This includes both on-premises (wired/wireless) and remote connections.

In response to this expanded attack surface, cyber criminals have adapted their attack methods to target third-party suppliers and contractors with authorized access to OT systems. As many network services are delivered via third parties, network operations analysts must be able to control access to third-party vendors. Indeed, some of the most damaging breaches in history have been accomplished by compromising third-party access to a network. For example, the GreyEnergy malware family utilizes stolen credentials obtained via spear phishing to compromise public-facing web servers and then move laterally to attack ICS workstations, plant backdoors, and communicate with command and control servers.[4]

About two-thirds (65%) of OT companies also lack role-based access control, which gives attackers greater freedom to move within their OT environments.[5]

A starting point in addressing these risks is multi-factor authentication. Multi-factor authentication makes the successful use of stolen credentials more difficult—and more than half (56%) report they do not have this critical feature in place.[6] It offers OT organizations the ability to transparently identify and verify network users to then enforce identity-driven policy based on the user's role.

But guests and partners are not the only potential risks to OT systems. In a recent survey, "employees" topped the list of actors who companies are most concerned about exposing their organization to risk—through both errors and malicious intent.[7] In addition to authentication tools to help validate network users, a user and entity behavior analytics (UEBA) solution can help organizations protect against insider threats by detecting behavioral anomalies that correlate to a problem with the organization.

In a study on cyber risk in the electric power industry, Deloitte found that internal threats attributed to disgruntled employees are among the most common threats.[8]

Do Not Disturb—Maintaining OT Uptime

Because many of these systems were designed long ago to operate in isolation for decades at a time, OT environments were not created with the expectation of probing. Even processes as benign as active device scanning can cause them to fail. Therefore, security for OT must be purpose-built—providing protection for uniquely sensitive systems that may need to operate around the clock.

The result is that the required visibility of all devices across the organization must use passive means so as not to disturb the critical nature of the operation. In addition, potential security issues require instantaneous notification with detailed contextual data so that network operations analysts can quickly investigate and determine the best course of action for maintaining both security and uptime.

A Security Architecture That Simplifies OT Complexity

Piecemeal OT security creates additional complexity—which can expose organizations to greater risks rather than fewer. Implementation of a security architecture that connects the disparate solutions into a cohesive system simplifies this growing problem while protecting organizations from sophisticated attacks.

An integrated security architecture can provide the foundation for establishing end-to-end visibility and control of all devices and users. It also enables automated workflows to help unburden limited staffs, as well as compliance management through built-in tracking, auditing, and reporting capabilities. Assembling the security architecture with OT-friendly solutions that are purpose-built for these environments can help further ensure availability and uptime of operations.

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

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

[3] Steve Culp, "How The Compliance Function Is Evolving In 2018—Five Key Findings," Forbes, March 27, 2018.

[4] JD Sherry, "8 Tips for Preventing Credential Theft Attacks on Critical Infrastructure," Dark Reading, November 27, 2018.

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

[6] Ibid.

[7] "Mobile Security Index 2019," Verizon, March 2019.

[8] Steve Livingston, et al., "Managing cyber risk in the electric power sector," Deloitte, January 31, 2019.

www.fortinet.com

391249-0-0-EN

August 2, 2019 9:24 PM

eb-simplifying-ot-security-complexity