FORTINET

CHECKLIST

How To Secure Operational Technology

Protecting Against Advanced Threats Requires Automation and Integration Across Security Solutions

The consequences of a successful intrusion into operational technology (OT) are serious. In businesses that rely on operational and industrial production systems, the chief information security officer (CISO) must ensure that security teams have the right architecture and solutions in place.

7 Considerations for the CISO Charged With Securing Operational Technology

Fortinet helps CISOs reduce network security complexity and the costs of continuously adding on more isolated products to cover new threats or risk exposures.

☑ Integrate OT and IT Security

Securing both IT and OT networks against advanced threats requires the CISO to take a multifaceted approach. That does not mean security solutions should operate independently. Instead, all the solutions protecting OT and IT networks should be tightly integrated and be able to share information in real time. This enables detection of a threat in one area to trigger a coordinated response across the company's entire security infrastructure.

The Fortinet Security Fabric provides just such an infrastructure. Together, tightly integrated Security Fabric solutions provide well-orchestrated protection that reaches every edge of corporate OT and IT networks. They also offer broad visibility across the entire digital attack surface, while facilitating automated workflows to increase efficiency and speed of operations and response.

☑ Effectively Control Access to OT Resources

Companies are increasingly undertaking outsourcing or other process changes that require network connectivity for guests, contractors, and vendors. In many cases, wireless and remote access capabilities are necessary, both for employees and for any visitors who need to use the network. Such environments demand careful attention to access control, to prevent unauthorized connections to network resources.

Organizations can leverage the Fortinet Security Fabric to deliver sophisticated user identity awareness and management solutions. For example, FortiAuthenticator facilitates role-based access policies and multi-factor authentication for all users of OT and IT systems.

FortiAP and FortiSwitch provide secure wireless access and network switching, respectively. Both are designed for operational and industrial production environments; they come in a ruggedized form factor that enables deployment in the extreme conditions of OT field sites and manufacturing and warehouse environments.

☑ Use Network Segmentation To Control Lateral Movement Between IT and OT

Placed between OT and IT network segments, next-generation firewalls (NGFWs) can control traffic flows and artificially re-create the “air gap” that used to keep many businesses' OT resources separate from IT systems. FortiGate NGFWs are especially capable in this environment. Their OT application-aware whitelisting can be configured to allow only specific OT protocols into the corporate OT network and to turn away all other traffic.

Another critical consideration in selecting FortiGate NGFWs for network segmentation or edge security is throughput. With some firewalls, activating advanced security features dramatically reduces the firewall's throughput. By contrast, FortiGate NGFWs are specifically designed to minimize latency, even with intrusion prevention system (IPS) and other advanced capabilities enabled.

☑ Make Sure Threat Intelligence Is Integrated

Protection against new and emerging strains of malware requires nearly real-time dissemination of local and global threat intelligence across the network. Solutions in the Fortinet Security Fabric integrate artificial intelligence (AI)-driven data feeds from FortiGuard Labs threat-intelligence services. With one of the industry's largest teams of security experts, FortiGuard Labs is continuously studying the threat landscape to identify zero-day threats—not only to IT systems but also to the most common OT protocols and OT application vulnerabilities.

☑ Look for OT-aware Sandboxing and Deception Technologies

No threat-intelligence service can identify every threat before it reaches the corporate network. Organizations must also deploy solutions designed to prevent unknown threats from reaching their OT systems. In the Fortinet Security Fabric, FortiSandbox receives suspicious packets from other Security Fabric elements and tests the code in a quarantined environment. In operational environments, FortiSandbox can emulate OT platforms, opening files that are unique to particular OT operating systems.

Deception technologies are also an important part of a comprehensive security infrastructure. FortiDeceptor deploys OT-specific decoy virtual machines (VMs) or applications, with the goal of luring attackers to reveal themselves. Because advanced threats are constantly evolving, CISOs need to come at the problem of zero-day threats from a number of directions simultaneously.

☑ Deploy Protection Against Insider Threats

Malicious and intentional attacks by insiders are a threat to both OT and IT environments. In addition, well-intentioned insiders may unintentionally offer attackers entry to the network or access to data. The FortiInsight user and entity behavior analytics (UEBA) solution continuously monitors users and endpoints. It leverages machine learning (ML) and analytics to automatically identify compromised accounts when behaviors are suspicious, noncompliant, or otherwise anomalous.

☑ Prioritize Effective Oversight of Security Infrastructure

Security teams need to be able to centrally manage policies, based on security standards from organizations such as the National Institute of Standards and Technology (NIST) and Center for Internet Security (CIS), and efficiently roll them out across security solutions. They also must have access to centralized, automated reporting on both threats detected and security solutions' response. The Fortinet Security Fabric Management Center includes single-console management, reporting, and analytics with automated workflows to deliver end-to-end visibility into the security landscape, as well as collecting OT security data that is necessary for industry and government audits.

Conclusion

OT network breaches can have catastrophic consequences. CISOs in sectors that utilize OT must deploy security solutions that incorporate best-of-breed approaches to advanced threat detection, and that tightly integrate for improved visibility and automated threat response.

The Fortinet Security Fabric delivers on these needs, facilitating tight integration among solutions from Fortinet and third parties. Backed by recommendations from leading testing organizations such as NSS Labs, Security Fabric integration makes best-in-class Fortinet solutions the obvious choice for OT organizations.

FORTINET®

www.fortinet.com

June 25, 2021 6:06 AM

448524-A-0-EN