SOLUTION BRIEF

Fortinet and CyberX

Accelerating IoT and OT Threat Detection and Prevention

Executive Overview

Companies looking to take advantage of the operational efficiencies that Internet-of-Things (IoT)/operating technology (OT) devices and networks bring to their operations face a dilemma. As the number of networked devices grow, an organization's attack surface also expands and becomes more vulnerable to cyberattack. These sorts of cyberattacks carry the same potential damage risks that any company would face (e.g., downtime, revenue loss, brand damage, loss of intellectual property). But successful attacks against critical infrastructure can also result in large-scale power blackouts, environmental catastrophe, or even loss of human life. To address these risk exposures, CyberX and Fortinet have developed joint integrations through the Fortinet Fabric-Ready Program, which enables joint customers to decrease the time to detect and stop attacks against information technology (IT) and OT networks.

Digital Innovations Introduce New Threats to Critical Infrastructure

Traditionally, industrial networks were kept secure by isolating them from internet-connected IT networks. This practice (known as "air gapping") ensured that sensitive control systems for manufacturing and critical infrastructure operations (e.g., electrical grids, hydroelectric dams, nuclear power plants, water supplies) were kept safe from outside tampering and disruption. But digital innovations like the adoption of IoT/OT devices that enable new business capabilities are also creating many new potential connections to IT networks. As businesses adopt these operational efficiencies by converging the environments, previously isolated OT devices can inadvertently be exposed to internet-based cyberattacks.

A Joint Solution for Reducing OT/IT Risk Exposure

A combination of CyberX and Fortinet solutions addresses these new risks to OT/ IoT devices with technologies that support advanced threat detection and prevention

capabilities. The CyberX cybersecurity platform detects anomalous behavior in IT and OT networks and then delivers local threat intelligence to a FortiGate next-generation firewall (NGFW) and FortiSIEM security information and event management.

The information provided by CyberX gives FortiSIEM administrators visibility into previously "dark" (or invisible) IT and OT networks. Meanwhile, FortiGate administrators use the information discovered by CyberX and collected in FortiSIEM to create rules for automatically blocking the identified anomaly before it causes damage to production, profits, or people. This includes potential threat behaviors caused by chaotic actors as well as those caused by misconfigured devices.

Joint Solution Components

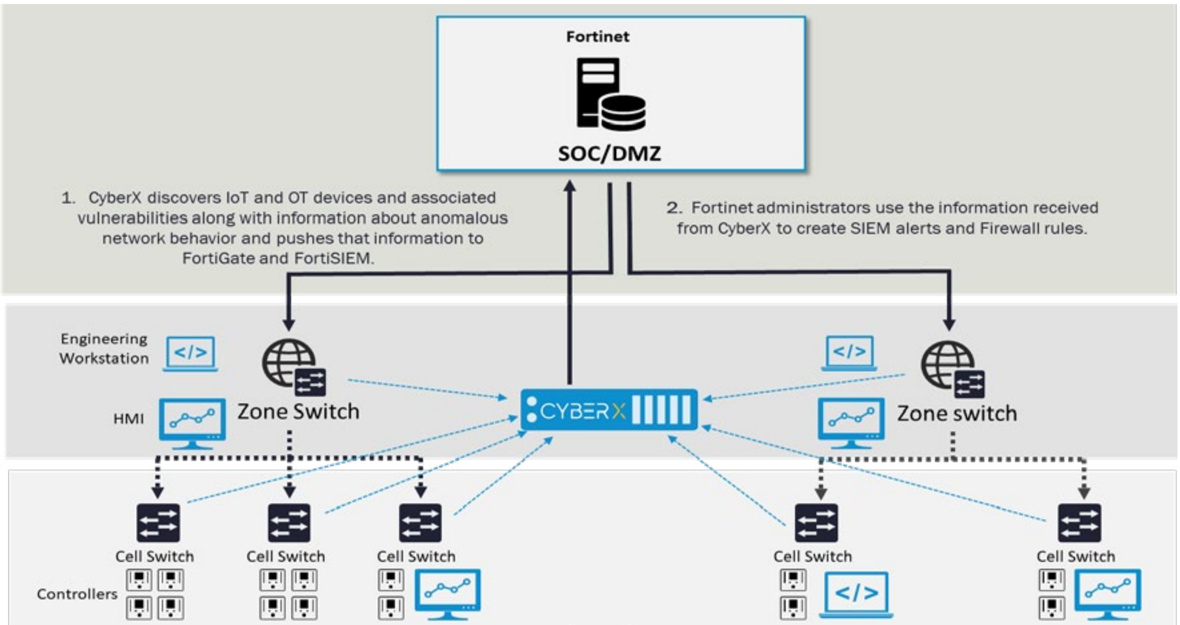
- Fortinet FortiGate Next-generation Firewalls, FortiSIEM
- CyberX Cybersecurity Platform

Fortinet and CyberX prevent:

- Unauthorized changes to programmable logic controllers (PLCs)
- Malware that manipulates industrial control systems (ICS) and/or IoT devices via their native protocols
- Reconnaissance tools from collecting data
- Protocol violations caused by misconfigurations or malicious attackers

IoT/OT networks continue to be soft targets for attack—up to 71% of existing sites will have outdated Windows systems that no longer receive security patches from Microsoft as of January 2020.[1]

FORTINET FABRIC-READY



1. CyberX discovers IoT and OT devices and associated vulnerabilities along with information about anomalous network behavior and pushes that information to FortiGate and FortiSIEM.

2. Fortinet administrators use the information received from CyberX to create SIEM alerts and Firewall rules.

Figure 1: Fortinet FortiGate architecture diagram.

The CyberX Platform

The CyberX platform auto-discovers and fingerprints unmanaged IoT and OT devices while continuously monitoring for targeted attacks and malware. Risk and vulnerability management capabilities include automated threat modeling, comprehensive reporting of endpoint and network vulnerabilities, and risk-prioritized mitigation recommendations. The CyberX platform is agentless, nonintrusive, and easy to deploy—delivering actionable insights minutes after being connected to the network.

CyberX is the most widely deployed platform for continuously reducing IoT/OT risk and preventing costly production outages, safety and environmental incidents, and theft of sensitive intellectual property.

About three-fourths (77%) of organizations running operational technology networks (such as for OT devices) have experienced a malware intrusion in the past 12 months, causing damages to productivity, revenue, brand awareness, data loss, and physical safety.[2]

A majority (82%) of organizations report having only partial cybersecurity visibility into operational technology.[3]

Fortinet FortiGate NGFWs

FortiGate NGFWs utilize purpose-built security processors and threat-intelligence security services from FortiGuard Labs to deliver top-rated protection, as well as high-performance inspection of clear-texted and encrypted traffic. FortiGate NGFWs reduce cost and complexity by providing full visibility into applications, users, and networks.

As a core part of the Fortinet Security Fabric framework, FortiGate NGFWs share threat- intelligence information across the entire integrated security ecosystem—including Fabric-Ready third-party solutions in a multivendor environment. This improves an organization's holistic security posture. The Security Fabric also lays a foundation for unified visibility and control at the device level, helping network operations teams to understand their organization's overall security posture. It includes automated workflows for compliance auditing and reporting that reduce the burden on limited staff resources. Most importantly, Fortinet offers security that is purpose-built for industrial and critical-infrastructure environments. This enables organizations to repel advanced threats without disturbing sensitive systems.

[1] "2020 Global IoT/ICS Risk Report," CyberX, October 24, 2019.

[2] "Fortinet 2019 Operational Technology Security Trends Report," Fortinet, May 8, 2019.

[3] Ibid.

Fortinet FortiSIEM

Effective security requires visibility of all deployed devices across the entire infrastructure in real time. It also requires context—namely, which devices represent a potential problem and the associated level of risk—in order to manage actual threats rather than the noise created by multiple point security tools working in isolation.

FortiSIEM brings visibility, correlation, automated responses, and remediation together in a single, scalable solution. Using a business services view, the complexity of managing network and security operations is reduced—which helps unburden staff resources while improving the effectiveness of breach detection. Additionally, FortiSIEM applies cross-correlation, machine learning, and user and entity behavior analytics (UEBA) capabilities to stop breaches before they occur.

Use Case: Preventing Unauthorized Changes to PLCs

Organizations use programmable logic controllers (PLCs) to manage physical processes such as robotic arms in factories, spinning turbines in wind farms, and centrifuges in nuclear power plants. An update to a PLC's ladder logic or firmware may often come from legitimate authorized activity—but it can also represent an attempt to compromise the device by inserting malicious code. CyberX can detect unauthorized changes to PLCs and then immediately deliver information about that change to both FortiSIEM and FortiGate. Armed with that information, FortiSIEM administrators then decide how to best mitigate the solution. One mitigation option would be to create a policy rule in the FortiGate console that stops further communication to the affected device.

Use Case: Stopping Ransomware Before It Causes OT/IoT Damage

CyberX continuously monitors OT/IT networks for behaviors caused by ransomware (e.g, LockerGoga, WannaCry, NotPetya). When integrated with FortiSIEM and FortiGate, CyberX can deliver contextual information about the presence of these types of threats. FortiSIEM operators can immediately spot where the malware is located, enabling FortiGate administrators to quickly contain the ransomware and stop it from causing damage to the organization.

End-to-end Visibility and Control for Critical Environments

The combination of CyberX and FortiGate and FortiSIEM provides transparent visibility and purpose-built control features for OT/IT connected networks. This joint solution offers a foundation for securing delicate systems without disruption, maximizing operational uptime while maintaining safety within critical infrastructure.

FORTINET.

www.fortinet.com

September 24, 2021 2:26 PM

Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 3:sb-FA-fortinet-and-cyberX_092021:sb-FA-fortinet-and-cyberX_092021

598909-A-0-EN