FORTINET

Empower Digital Transformation by Protecting Converged IT and OT

Table of Contents

Executive Summary

Operational technology (OT)* networks, which control equipment in critical infrastructures such as utilities and manufacturing assembly lines, have traditionally been kept separate from information technology (IT) networks, which control data in organizations. However, in recent years, compelling innovations in IT such as artificial intelligence (AI) and big data analytics have improved outcomes that could benefit OT networks as well. As a result, the convergence of OT and IT networks is accelerating. One of the drawbacks of this new convergence is the expansion of the digital attack surface and exposure of OT networks to the same type of attacks that IT networks experience. Therefore, OT breaches are becoming more common.

This ebook identifies and discusses the drivers of IT and OT network convergence. It also highlights the technologies that asset owners should deploy to address the challenges posed by connecting industrial environments to the data center and the cloud. To maintain a security posture consistent with the risks posed by connecting industrial environments, asset owners must deploy solutions that keep the environment secured in the process.

*OT is a synonym for industrial control systems (ICS). OT was established as a term to contrast with IT, because OT protocols, vendors, and use cases are distinct. Supervisory control and data acquisition (SCADA) systems are an element of OT. SCADA systems use graphical user interfaces for high-level supervisory management of OT/ICS processes.

Why IT and OT Networks Are Converging

From machine learning (ML) to augmented reality (AR) to the Internet of Things (IoT), digital transformation (DX), and new developments in IT are remaking processes and improving outcomes in many business sectors.

In many OT networks, which control critical infrastructures such as pipelines, electric grids, transportation systems, and manufacturing plants, change is coming. OT environments are vital to public safety and global economic well-being. They were developed decades before IT networks and have different vendors and proprietary protocols. In the past, there was little reason to connect OT and IT networks, especially because doing so increases the risk of cyberattacks.

What's behind digital transformation?

Gartner reports that "OT environments that were traditionally separated are no longer completely isolated. They now have direct connections for business, OEMs, and other third parties."[1] Digital transformation is driving greater connectivity to industrial environments. What's behind DX? Three things:

1. Anticipating asset failure
2. Maintenance strategy upgrade, from calendar-based to condition-based maintenance
3. Secure remote access

Asset owners want to reduce costs and increase profitability by anticipating when their expensive industrial assets are going to break. By foreseeing failure, they can optimize the asset utilization and increase profitability. But anticipating failures requires building a digital twin. A digital twin marries a physics model of the underlying industrial asset with operating data that can reveal characteristics of how the machines are actually performing. But that operating data can only come from one place: the OT system. So, to build a digital twin to anticipate failure requires taking data out of that asset and delivering it to the cloud or data center. Thus, the air gap (the separation of the OT network from the IT network) must be removed.

The second facet of DX is upgrading the maintenance strategy from calendar-based maintenance to condition-based maintenance. When an industrial original equipment manufacturer (OEM) supplies that equipment to the asset owner, they provide a maintenance manual that includes specific tasks that must be done on a regular calendar interval. For example, a wind turbine manufacturer may require their customer to tighten the bolts connecting the tower sections every six months or change the oil every 18 months.

These manuals and instructions are based on the worst-case scenario for that asset, so the asset owner knows that the instructions may be overly cautious. They would much rather do that maintenance when the asset actually requires the work—for example, when the nuts and bolts are starting to be too loose or when the oil contains too much iron particulate. Understanding the actual condition of the asset, again, requires taking data out of it and processing that data in cloud analytics. This is another case for connecting OT and IT networks.

An underlying truth in industrial control systems is that most programmable logic controllers (PLCs) are insecure by design. PLCs typically follow orders without testing for authorization or authenticity and rarely use encryption. Newer PLCs have improved security practices, but industrial systems are designed with long lifetimes and are often expected to last several decades. "The automation hardware in a process automation system is often capable of running 20 to 30 years."[2] The only conclusion is that the technology brain behind most critical infrastructure remains insecure due to the inherently insecure PLCs that are still in the industrial installed base.

In the past, asset owners could rely on the air gap as a natural defense, but DX is removing it and exposing PLCs to more and more risks. We're seeing more frequent and impactful attacks on OT environments as a result.

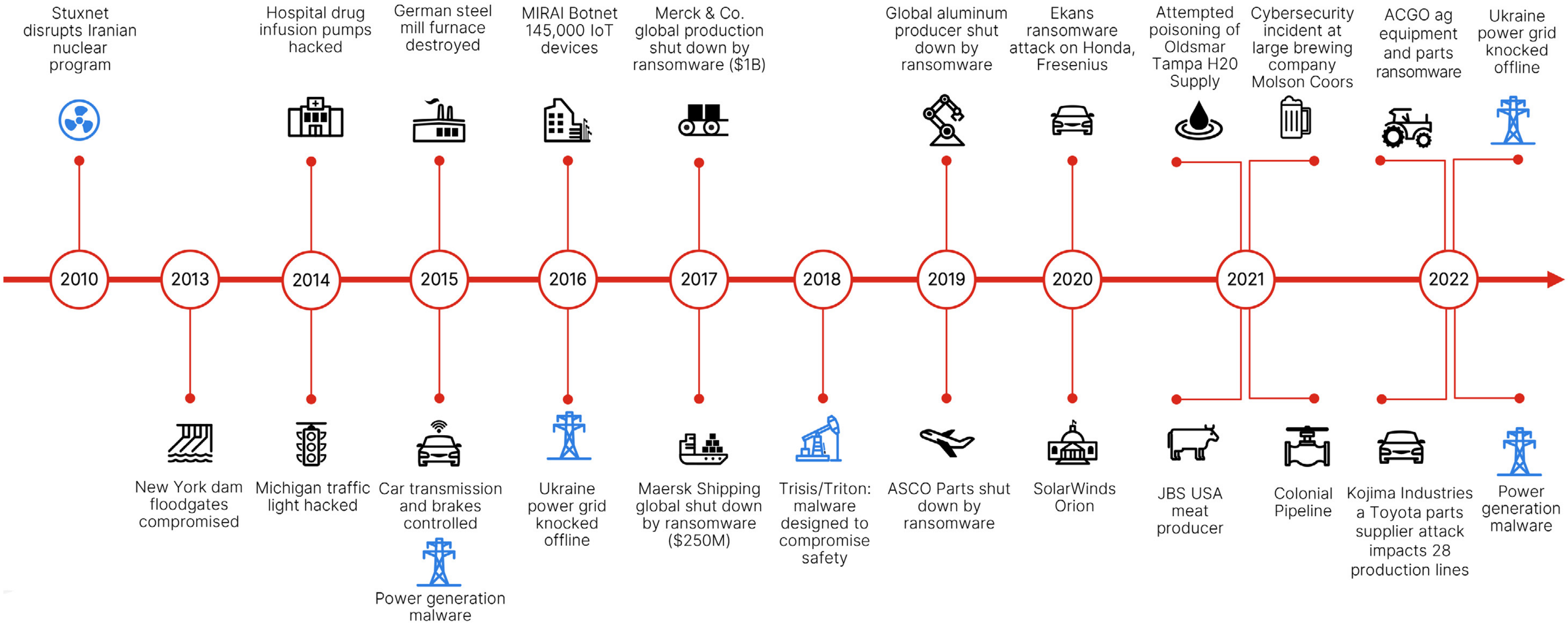

Stuxnet disrupts Iranian nuclear program
Hospital drug infusion pumps hacked
German steel mill furnace destroyed
MIRAI Botnet 145,000 IoT devices
Merck & Co. global production shut down by ransomware ($1B)
Global aluminum producer shut down by ransomware
Ekans ransomware attack on Honda, Fresenius
Attempted poisoning of Oldsmar Tampa H20 Supply
Cybersecurity incident at large brewing company Molson Coors
ACGO ag equipment and parts ransomware
Ukraine power grid knocked offline
2010
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
New York dam floodgates compromised
Michigan traffic light hacked
Car transmission and brakes controlled
Power generation malware
Ukraine power grid knocked offline
Maersk Shipping global shut down by ransomware ($250M)
Trisis/Triton: malware designed to compromise safety
ASCO Parts shut down by ransomware
SolarWinds Orion
JBS USA meat producer
Colonial Pipeline
Kojima Industries a Toyota parts supplier attack impacts 28 production lines
Power generation malware

Figure 1: Attacks on OT infrastructure are increasing in frequency and impact (2010–2022)

How remote access can create more risk

Many organizations have industrial assets that are spread far and wide. They are geographically dispersed. For example, an oil and gas company may own hundreds or thousands of pump jacks. It is not cost-effective to have a person on-site at each pump jack to do maintenance. This is also true on the renewable energy side. It is simply not cost-effective or efficient to run a wind energy business with a human operator inside each wind turbine. Even food and beverage manufacturers that own dozens of plants globally don't have the expertise inside each plant to care for and maintain the OT systems that control the manufacturing of products in their factories.

Therefore, asset owners need a secure way to enable their employees and their trusted third parties (like original equipment manufacturers or system integrators) to access the system. They need a way for people to get into these environments to do remote monitoring and diagnostics or SCADA upgrades or to reset something that's gone offline. However, all that remote access creates additional risk.

An example of that risk is the Oldsmar attack. In 2021, in the town of Oldsmar (near Tampa, Florida), a water treatment facility had put their SCADA system on TeamViewer—not a secure way of creating remote access. An attacker hacked into it and changed the setpoint, which could have put too much sodium hydroxide in the water supply if it had not been observed by a human and corrected.[3] This is why remote access needs to be created in a secure way.

Aside from just remote access, the relationship between asset owners, system integrators, and the OEMs also creates an element of risk. There's additional risk because asset owners often need the OEM or the system integrator to do technical maintenance. When these individuals come on-site physically, they may bring phones, laptops, and USB sticks that asset owners don't have control over if they're plugged into the network.

9 out of 10 organizations experienced at least one intrusion in the past year, and 78% had three or more intrusions.[4]

What Solutions Can Help Address These Challenges?

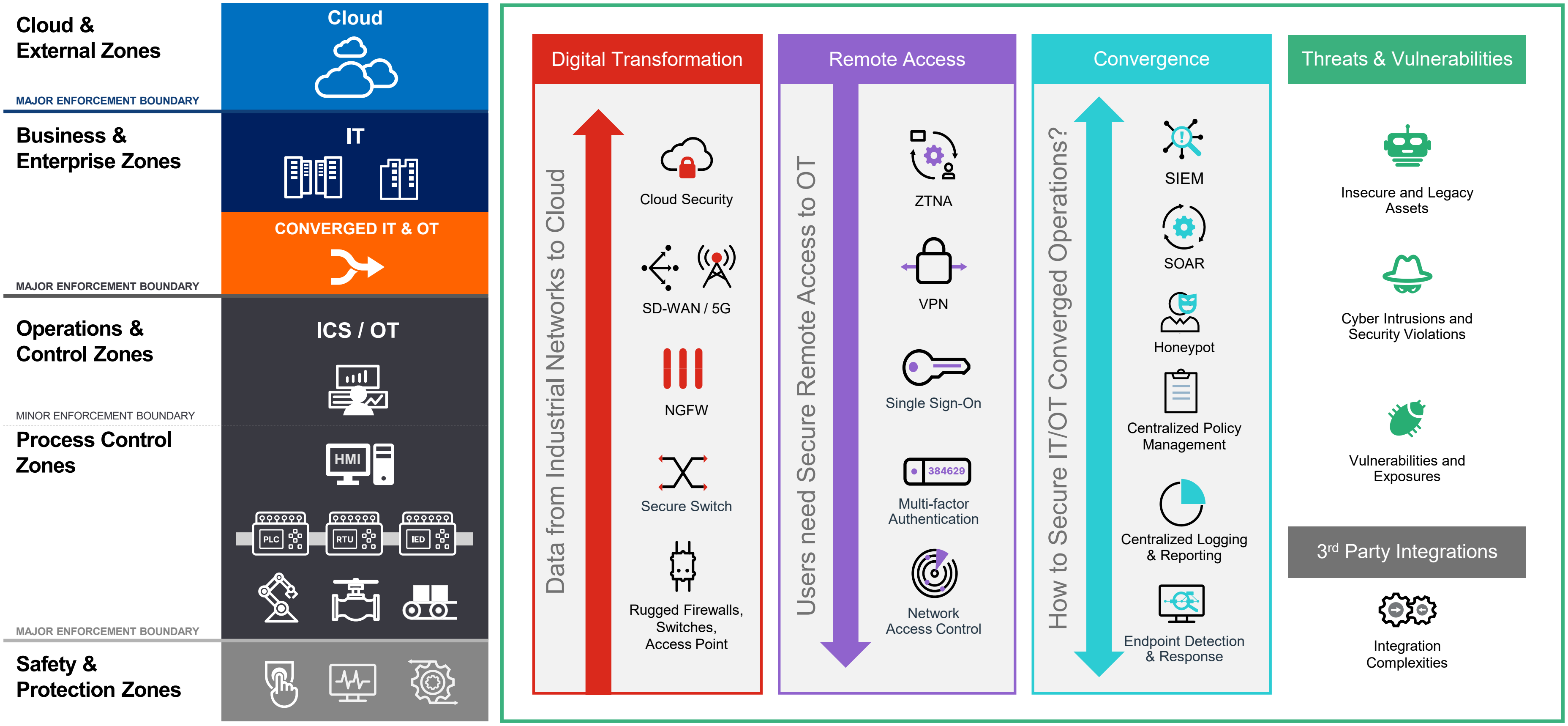

Cloud &
External Zones
MAJOR ENFORCEMENT BOUNDARY
Business &
Enterprise Zones
MAJOR ENFORCEMENT BOUNDARY
Operations &
Control Zones
MINOR ENFORCEMENT BOUNDARY
Process Control
Zones
MAJOR ENFORCEMENT BOUNDARY
Safety &
Protection Zones
Cloud
IT
CONVERGED IT & OT
ICS / OT
HMI
PLC
RTU
IED
Digital Transformation
Data from Industrial Networks to Cloud
Cloud Security
SD-WAN / 5G
NGFW
Secure Switch
Rugged Firewalls, Switches, Access Point
Remote Access
Users need Secure Remote Access to OT
ZTNA
VPN
Single Sign-On
384629
Multi-factor Authentication
Network Access Control
Convergence
How to Secure IT/OT Converged Operations?
SIEM
SOAR
Honeypot
Centralized Policy Management
Centralized Logging & Reporting
Endpoint Detection & Response
Threats & Vulnerabilities
Insecure and Legacy Assets
Cyber Intrusions and Security Violations
Vulnerabilities and Exposures
3rd Party Integrations
Integration Complexities

Figure 2: Fabric Solutions for OT. Different technology solutions help asset owners meet the trends and challenges of OT. The left side of the diagram represents the Purdue model, and the columns on the right side represent the technologies that can address different challenges posed by IT and OT network convergence.

Let’s overlay the Purdue model above across these domains of IT, IT/OT convergence, and OT. This is the left side of the diagram.

The Purdue model is a well-recognized logical architecture around all the different systems in an OT environment. It is common to different verticals. Therefore, whether it’s a manufacturing facility or an oil and gas facility or a wind farm or a gas turbine, or even a hospital, typically, OT workers understand this architecture and can talk about it. It’s a common language for them.

At the very bottom, we have the Safety Zone, which is paramount in OT. At the top is the cloud or data center, where we find different layers of technology, including the enterprise network on the IT side, and PLCs, SCADA, and field devices down below.

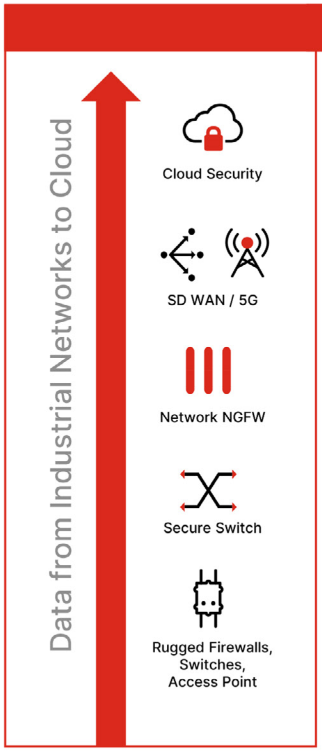
Digital Transformation

When asset owners connect their industrial control systems to the cloud, it is imperative that they protect those environments with next-generation firewalls and ruggedized switches and access points that enable secure connectivity down to the level of those PLCs.

SD-WAN lowers connectivity costs and provides enhanced network reliability. Recalling how these networks are brittle to change one way, Fortinet can enhance the security via our convergence of network and security. Also, our rugged switches and access points enable security directly in the network infrastructure.

Although the digital transformation arrow is pointing up, we should remember that another use case for DX is delivering edge analytics from the cloud to the edge of the industrial network. Fortinet can also play an important role with our edge-to-cloud security capabilities.

Digital Transformation


Data from Industrial Networks to Cloud
Cloud Security
SD WAN / 5G
Network NGFW
Secure Switch
Rugged Firewalls, Switches, Access Point

1. Minimize complexity by picking a vendor that can provide multiple products that are already integrated
2. Platform advantage—a full edge-to-cloud security capability is essential
3. Make sure you use a vendor that provides capabilities across both sides of the IT and OT space
    - Support *all* form factors
    - License in air-gapped environments
    - OT asset discovery and topology
    - OT *and* IT specific threat intelligence
4. The value of converged network and security
    - Convergence of security capability in the network inclusive of microsegmentation for east-west traffic control
    - SD-WAN + security enhancements are an extremely compelling business case for cost reduction + security enhancement

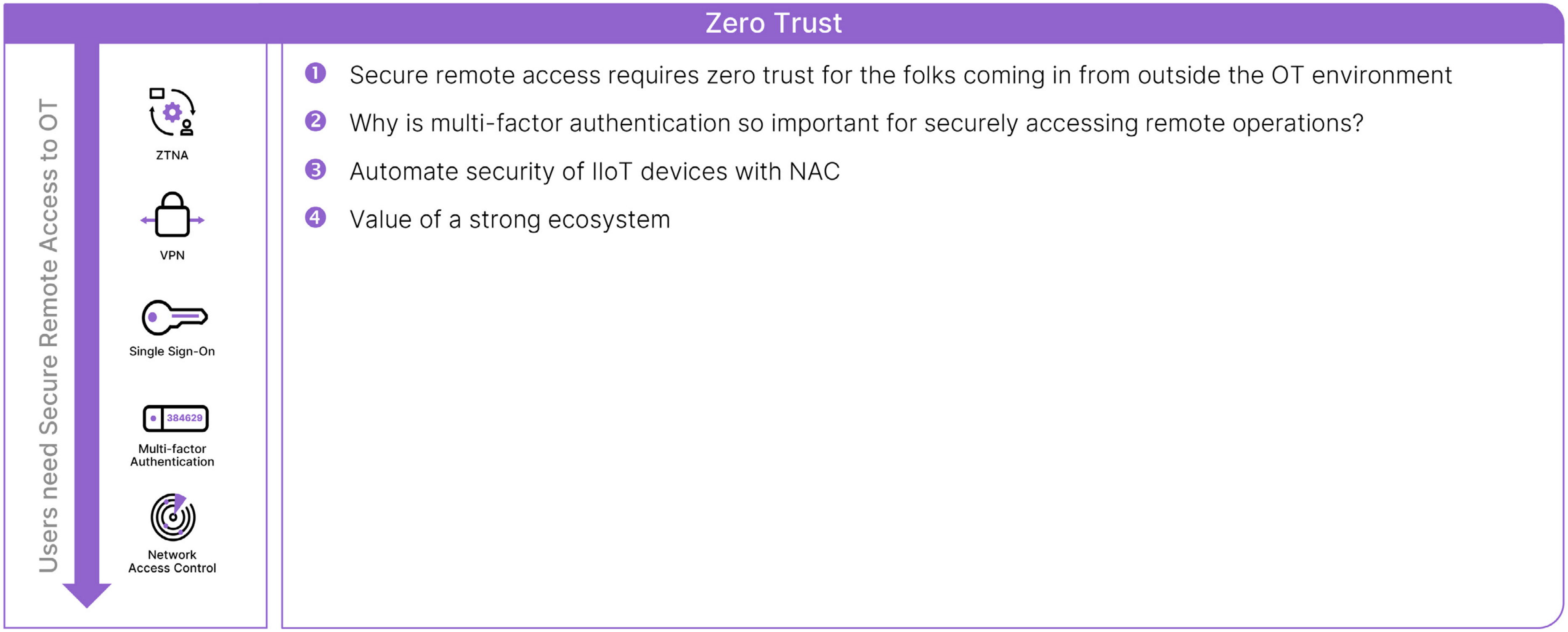
Figure 3: Best practices when selecting technologies to securely enable digital transformation

Secure Remote Access

Another use case driving connectivity is secure remote access to distributed industrial assets. In this case, asset owners want to enable their employees and trusted third parties, such as OEMs, to remotely access their systems to perform SCADA maintenance and enable remote monitoring and diagnostics of their industrial investments.

This section is much more about remote access for employees AND the supply chain accessing the industrial environment network from far away. In this use case, it's critical to provide protected communications leveraging zero-trust capabilities such as VPN, single sign-on (SSO), and multi-factor authentication (MFA).

Fortinet has a major differentiator with our zero-trust proxy, which can be deployed in FortiOS—and thus in Software-as-a-Service (SaaS), in FortiGate hardware (ruggedized or standard), in the virtual machine (VM), and in the container. Therefore, our proxy can be served anywhere, unlike other vendors that are forcing a cloud-based proxy, which is rarely easy to do in OT environments.



Zero Trust

Users need Secure Remote Access to OT

ZTNA

VPN

Single Sign-On

384629

Multi-factor Authentication

Network Access Control

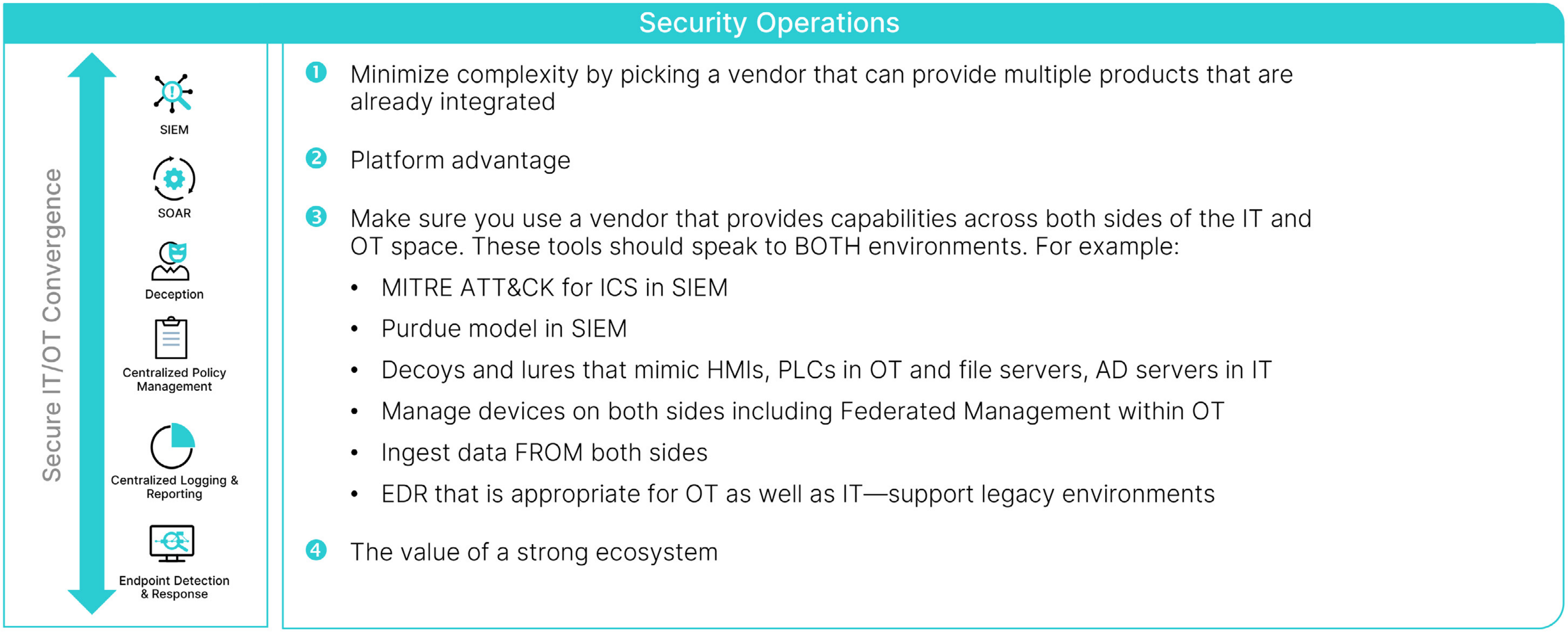
1. Secure remote access requires zero trust for the folks coming in from outside the OT environment
2. Why is multi-factor authentication so important for securely accessing remote operations?
3. Automate security of IIoT devices with NAC
4. Value of a strong ecosystem

Figure 4: Considerations when selecting technology to enable secure remote access

Converged Security Operations

A key Fortinet differentiator is the network security products deployed on both the IT and OT sides that can be managed from a common security operations center (SOC). With centralized management, logging, and security information and event management (SIEM) and security orchestration, automation, and response (SOAR) capabilities deployed in the SOC, organizations can effectively manage, monitor, and hunt threats and orchestrate responses from a common SOC.

Fortinet is trailblazing by developing OT-specific features into our SIEM and deception solutions. Additionally, our endpoint detection and response (EDR) solutions help protect SCADA engineering workstations, historians, and jump boxes found in Level 3. Our sandboxing product is also relevant and can be deployed to protect IT and OT with OT-specific capability.



Secure IT/OT Convergence
SIEM
SOAR
Deception
Centralized Policy Management
Centralized Logging & Reporting
Endpoint Detection & Response

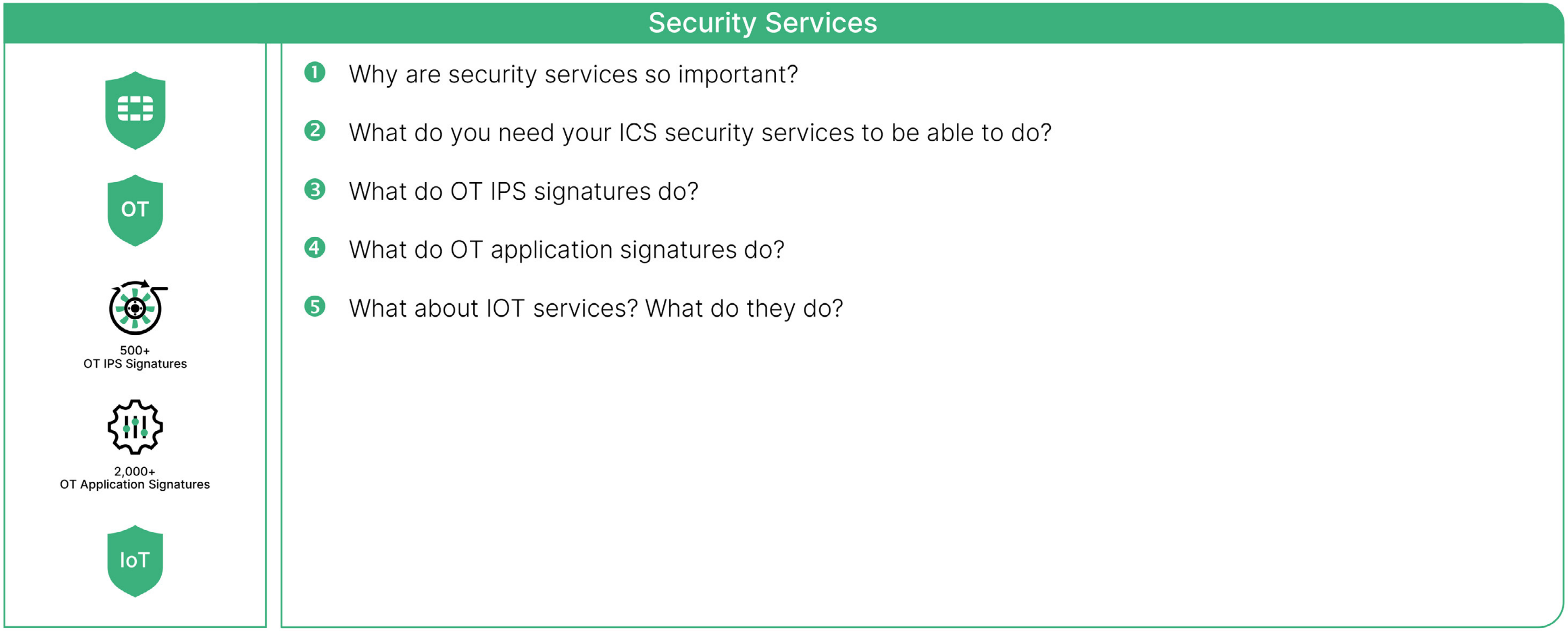
Security Operations

1. Minimize complexity by picking a vendor that can provide multiple products that are already integrated
2. Platform advantage
3. Make sure you use a vendor that provides capabilities across both sides of the IT and OT space. These tools should speak to BOTH environments. For example:
   - MITRE ATT&CK for ICS in SIEM
   - Purdue model in SIEM
   - Decoys and lures that mimic HMIs, PLCs in OT and file servers, AD servers in IT
   - Manage devices on both sides including Federated Management within OT
   - Ingest data FROM both sides
   - EDR that is appropriate for OT as well as IT—support legacy environments
4. The value of a strong ecosystem

Figure 5: Critical capabilities for converged security operations

Security Services

FortiGuard Labs has rich OT security services and industrial security services with 500+ OT intrusion prevention signatures that can limit known vulnerabilities from being exploited in the OT environment. These security services also have 2,000+ OT application signatures to set policy on industrial protocols such as Modbus or other protocols that are unique to those industrial control systems (and otherwise very hard to protect because they are so insecure). All these systems need to be kept current as the threat landscape evolves.



Security Services

1. Why are security services so important?
2. What do you need your ICS security services to be able to do?
3. What do OT IPS signatures do?
4. What do OT application signatures do?
5. What about IOT services? What do they do?

Figure 6: Five questions to answer when converging security services

Conclusion: Proactively Limit Risk in OT Networks

To stay competitive, organizations are connecting OT environments to their IT networks. In most instances, IT and OT convergence is planned and strategic. Although IT and OT integration is often a strategic initiative, it also increases the likelihood of OT breaches. Experience suggests that a cybersecurity breach is less a matter of “if” than “when.”

Even though breaches cannot be stopped 100% of the time, they can be limited via network segmentation, detected faster by traffic analysis, and minimized in frequency through identity and access management and wired and wireless access control. Deploying these solutions can greatly reduce costs and potential downtime if an attacker gets a foothold into the OT network.

[1] Wam Voster, “Reduce Risk to Human Life by Implementing This OT Security Control Framework,” Gartner, June 17, 2021.

[2] Dennis Hummel, “Life cycle management of process automation control systems,” iAutomation Industrial Information Technology, April 8, 2021

[3] Andy Greenberg, “A Hacker Tried to Poison a Florida City’s Water Supply, Officials Say,” Wired Magazine, February 8, 2021.

[4] “2022 State of Operational Technology and Cybersecurity Report,” Fortinet, June 21, 2022.

FORTINET®

www.fortinet.com

September 29, 2022 3:26 AM

1716666-0-0-EN