

Crucial Considerations When Enabling Secure Industrial Digital Transformation

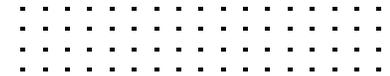


Table of Contents

Executive Summary	3
When OT Met IT: A Network Convergence Story	3
The Attack Surface Expands	6
Security Incidents Are on the Rise	8
Key Problem Areas in OT Security	10
The Path Toward Comprehensive Network Protection	12
Crucial Considerations When Enabling Secure Digital Transformation	13
Fabric Solutions: Operational Technology	14
Critical Capabilities for Secure Digital Transformation	15
Conclusion	15



Executive Summary

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 threats previously avoided within these environments. The result is that traditional security approaches are insufficient to protect connected OT environments.

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.¹ OT includes industrial control systems (ICS) that run equipment and machinery and the supervisory control and data acquisition (SCADA) subset systems that provide a graphical user interface for ICS.

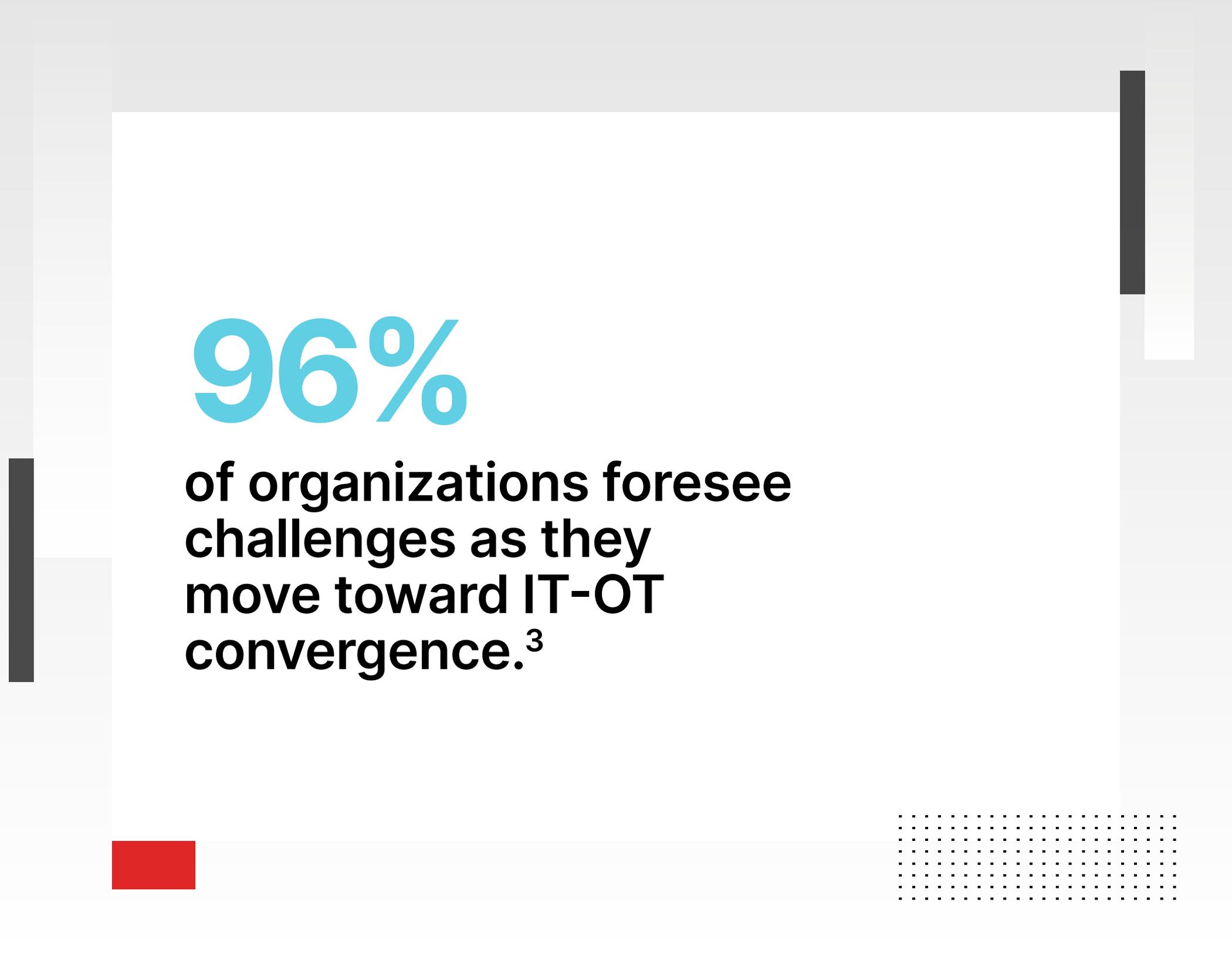


The value of OT assets can range into the billions of dollars, and their safe operation is often critical to public safety and global economic health. A system crash on a manufacturing floor can stall production for days and potentially ruin millions of dollars in materials. Having to reset a 10,000-gallon 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 maintain security, operational uptime, and safety simultaneously.

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 for 20+ 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.

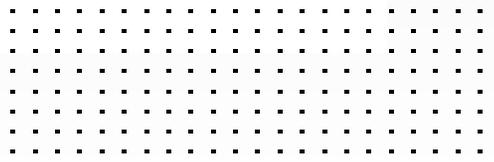
But increasingly, IT and OT are being integrated for greater business efficiency, increased innovation, and competitive advantage. The benefits of convergence include more effective and efficient monitoring of processes, the ability to leverage data from Internet-of-Things (IoT) devices to inform decision-making, and significant cost savings in power consumption, reduced raw materials waste, and employee efficiency. Convergence is the clear trend. But the process brings with it several security challenges because it eliminates the de facto security of the air gap against common internet-borne attacks.²





96%

of organizations foresee challenges as they move toward IT-OT convergence.³



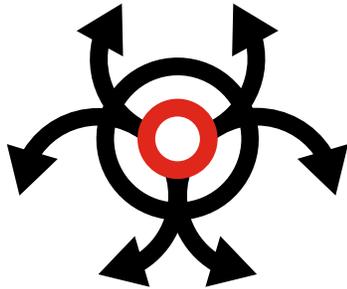
The Attack Surface Expands

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.

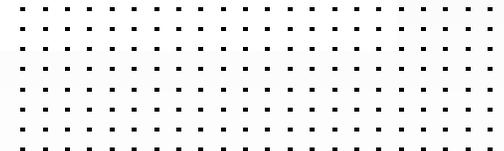
When it comes to cybersecurity, existing OT defenses are much less evolved than their analogous security counterparts in the IT realm due to a prior lack of investment and knowledge. So, OT decision-makers must modernize their security controls. And as the attack surface continues to grow and evolve 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. OT leaders continue to struggle to keep pace with change and the lack of skilled labor.

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.





9 out of 10 OT organizations experienced at least one intrusion in the past year and 78% had three or more intrusions. The most common intrusions were malware at 57% and phishing at 58%. 61% of intrusions impacted OT systems.⁴



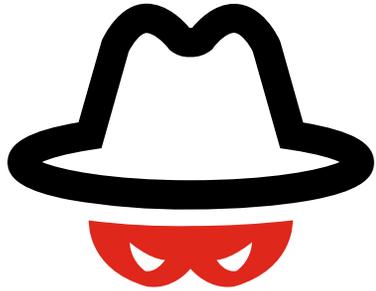
Security Incidents Are on the Rise

Where there is opportunity, there is exploitation. Threats targeting OT systems are on the rise. The current lack of effective OT security contributes to these risks. Two high-profile examples are:

- **SolarWinds:** This U.S. information technology firm was the victim of a cyberattack that spread to 33,000 of its customers and went undetected for months. When SolarWinds sent out software updates to its customers, it included hacked code that created a backdoor to the customers' IT systems, which the attackers used to install more malware so they could spy on companies and organizations.⁵
- **Colonial Pipeline:** One of the largest oil pipelines in the U.S. was the victim of a ransomware attack in May 2021 that infected some of the company's digital systems. Colonial Pipeline shut down more than 5,500 miles of pipeline for several days to prevent the ransomware from spreading.⁶

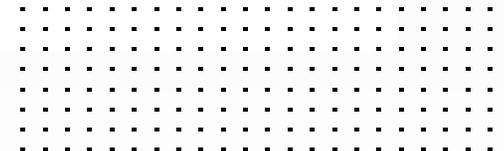
Politically motivated cyberattacks against critical infrastructure have the potential to do more than just grab headlines. They can be weaponized to cripple civil defenses, shut down the production of vital resources, and even cause widespread harm to human lives. The current lack of effective OT security contributes to these risks.





Successful intrusions resulted in the following damages at OT companies:

- **Productivity, 51%**
- **Revenue, 42%**
- **Brand reputation, 43%**
- **Business-critical data, 29%**
- **Physical safety, 40%⁷**



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 IT and OT convergence. New digital technologies in OT require internet interconnections—and with the good comes the bad.
- 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 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 hypersensitive. Legacy OT systems can operate for 30 to 40 years and may depend on dated configurations that remain unpatched. Because updating devices may 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, OT security may seem a daunting task to take on.

“In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network. On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network.”⁸

-Sean McGurk, Former Director, NCCIC, the Department of Homeland Security



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 IT and OT 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 IT and OT 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 threat detection across the entirety of our IT and OT environments?

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



Crucial Considerations When Enabling Secure Digital Transformation

The following questions will be helpful when considering technology vendors to secure your industrial digital transformation:

1. How completely does this platform address the entire edge-to-cloud data pathway? Can this vendor provide everything from rugged firewalls and switches deep in the Purdue model all the way up to cloud-security capabilities?
2. Is SD-WAN part of the solution? SD-WAN enables considerable connectivity cost savings that can dramatically improve the digital transformation initiative's return on investment (ROI). When you can get security benefits from the same devices that enable SD-WAN, you combine security posture improvements with cost reductions for a compelling security-up-costs-down business case synergy.
3. Can this vendor secure north-south communications with security policies that fit the OT environment? How extensive is their list of OT protocols? And most importantly, does this vendor support the protocols in *my* industrial controls environment?
4. Can this vendor's security solution also help me discover what's on my network? Do they have asset discovery and topology capabilities built into the firewall itself?
5. Does this vendor have an extensive ecosystem of partners? And most importantly, do they partner with the vendors I've already selected?
6. How committed is OT to this vendor's corporate strategy? Are they cloud-*capable* or cloud-*only*? And will that vendor's cloud posture work for me in my OT environment?
7. Does this vendor's product enable federated management and air-gapped licensing?



Fabric Solutions: Operational Technology

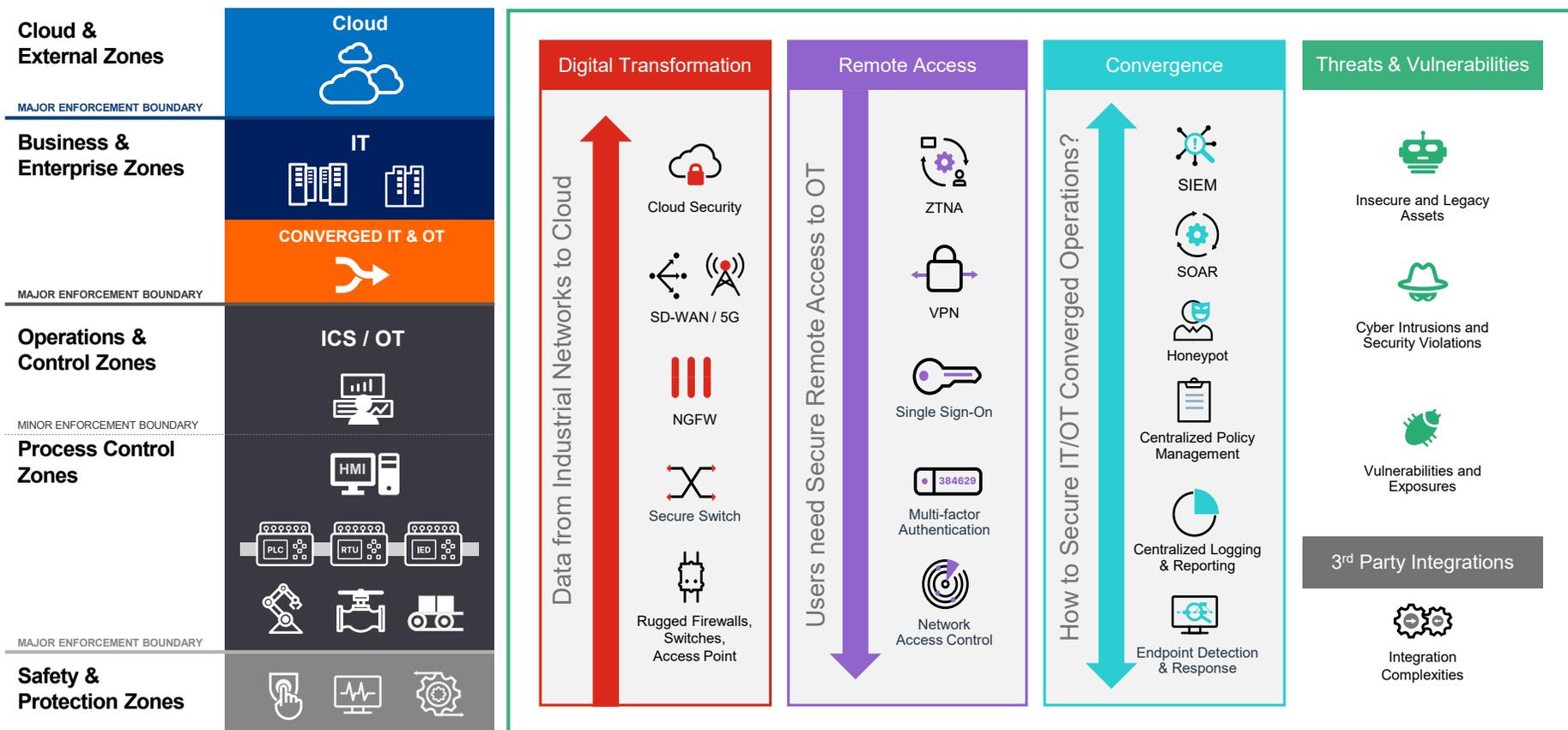


Figure 1: The red digital transformation rectangle in the chart above shows the most important technologies to apply when securely empowering digital transformation.



Critical Capabilities for Secure Digital Transformation

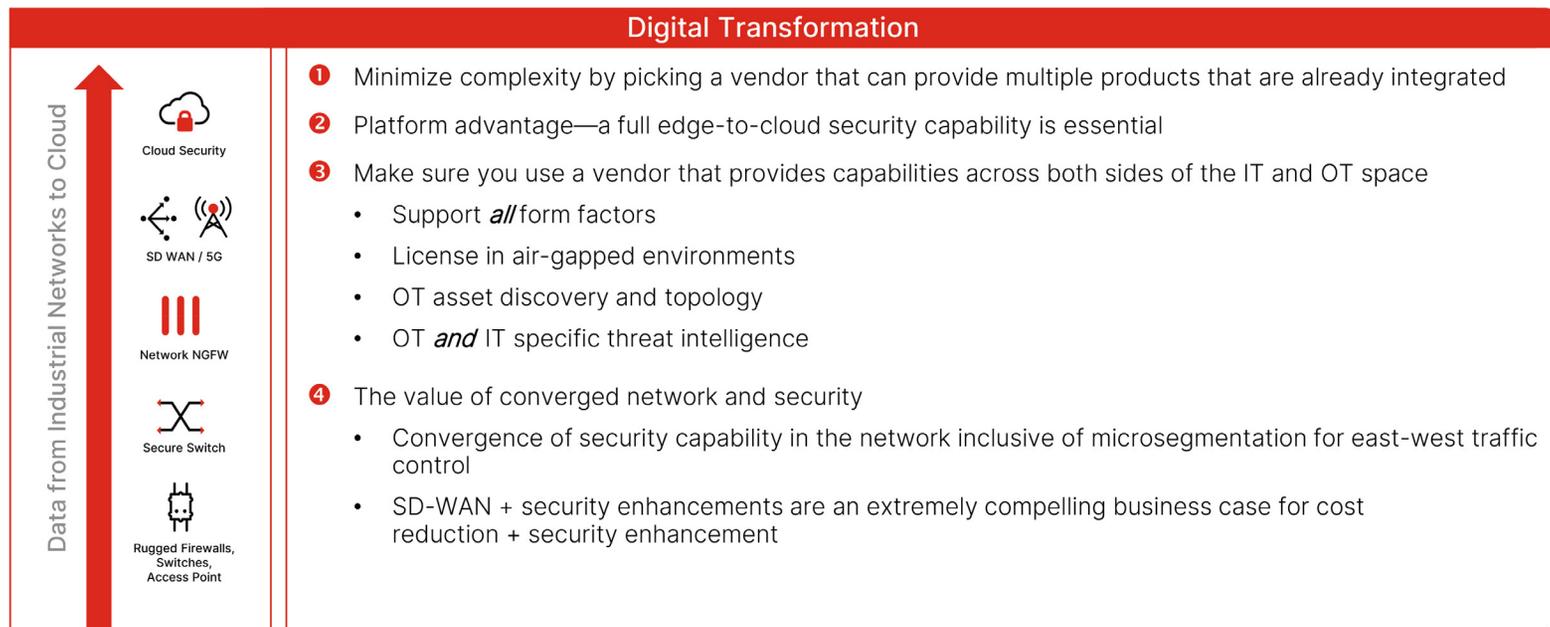


Figure 2: Above are the critical capabilities for secure digital transformation.

Conclusion

Digital transformation initiatives offer tremendous opportunities to reduce costs and improve profitability for industrial operators. However, these benefits require connecting previously air-gapped environments and risk increasing the security exposure of industrial assets unless important security technologies are deployed alongside. The Fortinet Security Fabric includes everything asset owners need to securely empower their digital transformation.



In the [Westland Advisory the IT/OT Security Platform Navigator 2022 Report](#), Fortinet is a leader. There is only one other IT-OT security platform vendor that is designated a leader out of the 103 considered. Why does Westland Advisory see Fortinet as a leader? It's our ability to enable secure digital transformation along with the full breadth of the Fortinet Security Fabric portfolio. Additionally, Fortinet's strong growth of 75% year-over-year growth in 2021 showcases that the Fortinet solution is finding traction in the space. Finally, a large number of the other vendors in the Westlands Advisory report are existing Fortinet ecosystem partners, validating that the Fortinet IT-OT Security Fabric is recognized by all players in the market.

To learn more about how Fortinet can assist your organization's industrial digital transformation, please visit fortinet.com/ot.

¹ ["2021 State of Operational Technology and Cybersecurity Report,"](#) Fortinet, May 26, 2021.

² ["Independent Study Finds That Security Risks Are Slowing IT-OT Convergence,"](#) Fortinet, May 23, 2021.

³ Ibid.

⁴ ["2022 State of Operational Technology and Cybersecurity Report,"](#) Fortinet, June 21, 2022.

⁵ Isabella Jibilian and Katie Canales, ["SolarWinds Hack Explained,"](#) Business Insider, April 15, 2021.

⁶ Sean Michael Kerner, ["Colonial Pipeline hack explained: Everything you need to know,"](#) TechTarget, July 7, 2021.

⁷ ["2021 State of Operational Technology and Cybersecurity Report,"](#) Fortinet, May 26, 2021.

⁸ ["Fortinet Q2 2022 Earnings Prepared Remarks,"](#) Fortinet, August 2022.



www.fortinet.com

Copyright © 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.