White paper

A holistic approach to securing operational technologies

verizon business

Cybersecurity challenges for OT

The current industrial landscape demands rapid, secure and resilient services and systems to support the production of goods and services. Organisations must prioritise the security of their operational technology (OT) and establish appropriate monitoring and response mechanisms to address any potential issues that may arise.

Forrester: Offer preventative capabilities in addition to detection. The OT security market has a lot of emphasis on asset identification and threat and vulnerability detection, but don't forget protection.

Source: *The Forrester Wave™: Operational Technology Security Solutions, Q2 2024; Forrester*

IDC: 80% of CIOs to embrace AI and automation for agility and insights-driven businesses by 2028

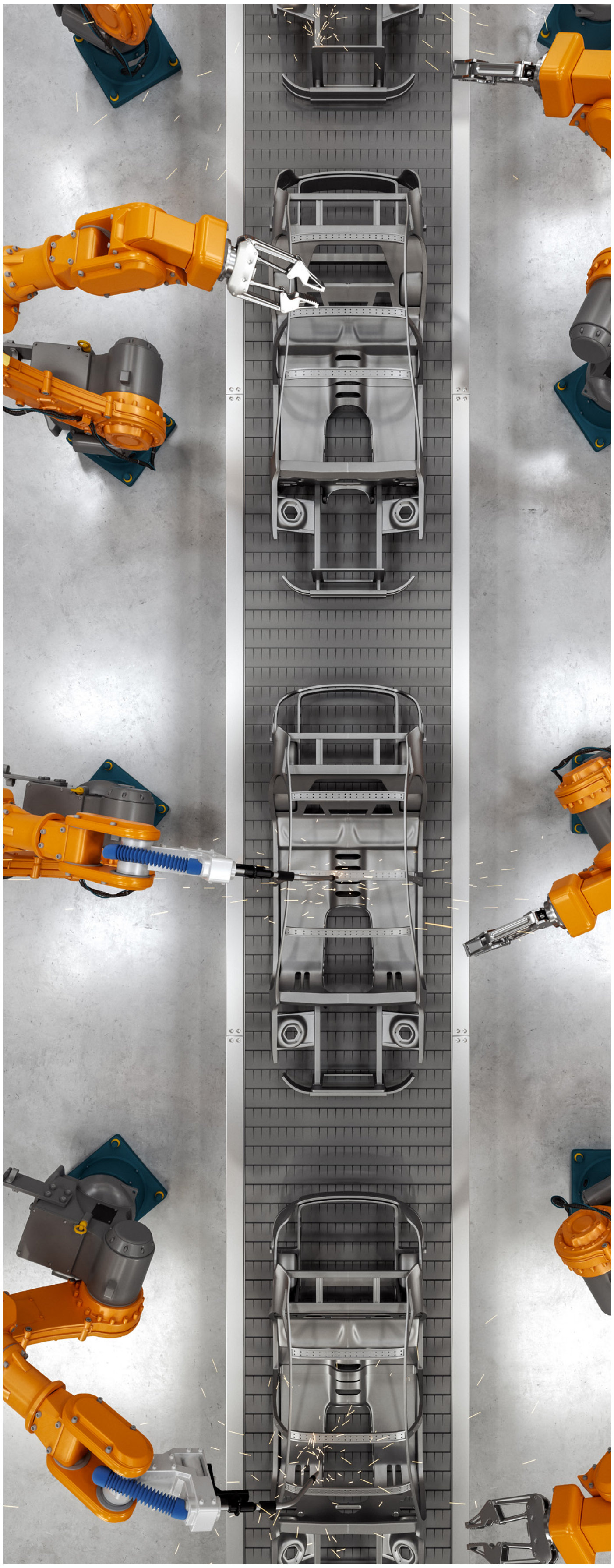
Source: *CIO Predictions in Asia/Pacific* for 2024 and Beyond Revealed by IDC.*

Connecting OT to applications is driving the Fourth Industrial Revolution (4IR), where large amounts of data can be stored and processed for various purposes. The data is hosted in IT data centres or in the cloud.

Providing connectivity between OT applications and OT devices can open routes for malicious users and cyber criminals to gain access to the technology underpinning the organisation's business.

OT networks have traditionally been isolated from IT networks and the internet for the security and reliability of the OT network. This is no longer the case and poses a security challenge outlined in this white paper.

The purpose of this paper is to provide an insight on how to secure integrated OT networks, so that they can become a business enabler and benefit from being integrated into the organisation's broader IT network, without increasing cyber risk.

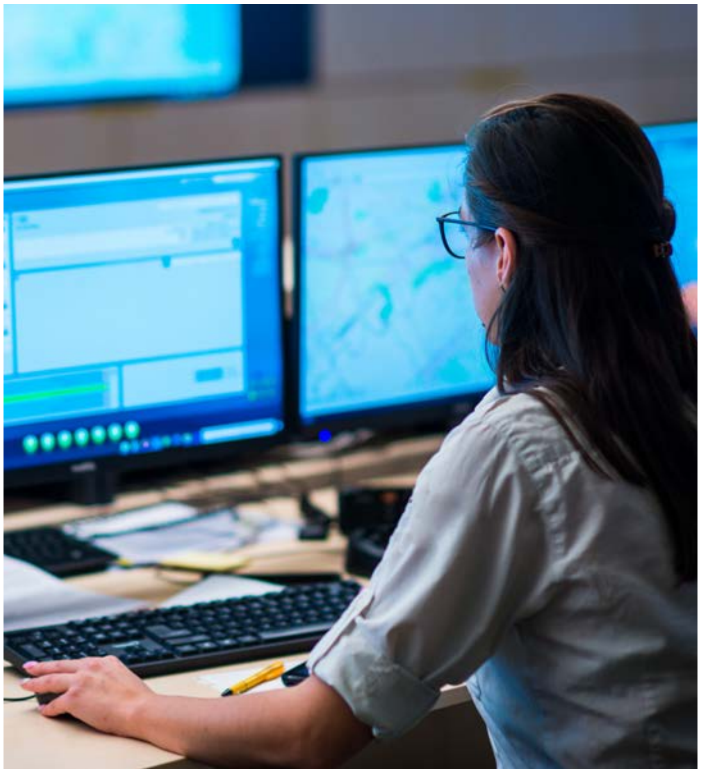


Business drivers and risks: OT evolution

As the push for more efficiencies grows within the organisation's OT, more monitoring and greater flexibility is being sought. This then means the introduction of the IT and OT interconnection as services move to the cloud. That evolution can also include building a more stable production line by leveraging AI for predictive maintenance, a better and more cost effective use of third parties for maintenance, and operational support by allowing secure remote access for third parties.

IT-OT convergence risks

The increased connectivity between IT and OT networks potentially expands the attack surface. Legacy OT systems were typically not designed with security in mind and are now being exposed to cyber threats.



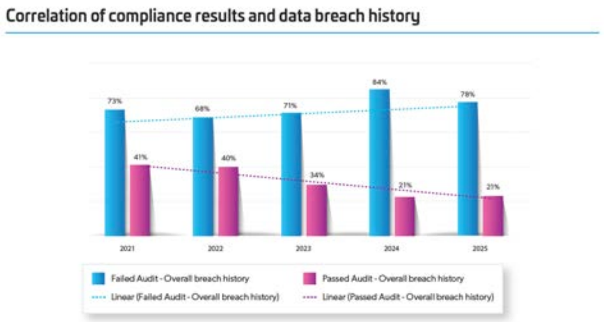

Correlation of compliance results and data breach history
73%
41%
68%
40%
71%
34%
84%
21%
78%
21%
2021
2022
2023
2024
2025
Failed Audit - Overall breach history
Passed Audit - Overall breach history
Linear (Failed Audit - Overall breach history)
Linear (Passed Audit - Overall breach history)

Figure 1: Top patterns over time in Manufacturing industry breaches;

Source: *2025 Verizon DBIR*

The hidden costs of inferior access

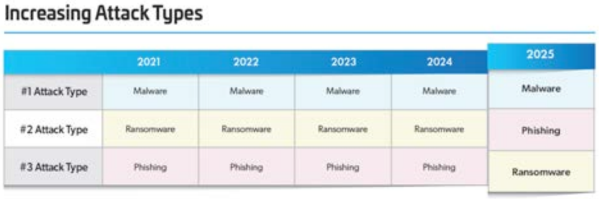
In the Verizon 2025 Data Breach Investigations Report (DBIR), system intrusion has increased since 2020 while the manufacturing industry specifically has seen a significant increase in the past year as Figure 1 indicates.

The DBIR also reports the manufacturing industry has seen a significant increase in data breaches this year, with small- and medium-sized businesses reporting 1,607 confirmed breaches compared to 849 last year. While financially motivated external actors remain the primary threat (87%), it's noteworthy that espionage was the motive in approximately 20% of manufacturing breaches, a substantial rise from 3% the previous year. Although it's plausible to attribute this surge to state-sponsored actors seeking exotic technologies for aerospace and military applications, this increase is more likely due to changes in our contributors' datasets.

Legacy and unpatched systems: Many OT environments still rely on outdated operating systems and software that lack vendor support or have no support at all. Patching and updating OT systems is difficult due to concerns over downtime and lost production.

Lack of visibility and asset management: Organizations often lack a clear inventory of connected OT assets, making risk assessments difficult. Shadow OT devices and undocumented endpoints can introduce additional unknown vulnerabilities.

Ransomware and cyber threats: Ransomware attacks are the top action variety in breaches against the manufacturing industry according to the 2025 DBIR. Threat actors exploit weak segmentation between IT and OT to move laterally and disrupt operations.



Increasing Attack Types

	2021	2022	2023	2024	2025
#1 Attack Type	Malware	Malware	Malware	Malware	Malware
#2 Attack Type	Ransomware	Ransomware	Ransomware	Ransomware	Phishing
#3 Attack Type	Phishing	Phishing	Phishing	Phishing	Ransomware

Figure 2: Ransomware increase over time;

Source: *2025 Verizon DBIR*

Ransomware incidents, with and without encryption, have seen a notable increase, appearing in 44% of all breaches reviewed, up from 32% in the previous year's report–a 37% surge in their presence. Despite this rise, the median ransom paid has decreased to $115,000 from $150,000 previously. This decline may be linked to the growing number of victim organisations refusing to pay ransoms, which has risen to 64% from 50% two years ago. Ransomware disproportionately impacts small- and medium-sized businesses (SMBs), accounting for 88% of their breaches, compared to 39% in larger organisations.

Regulatory and compliance complexity: Organisations must comply with multiple cybersecurity frameworks and industry regulations, for example the National Institute of Standards and Technology (NIST), IEC 62443 and the Cybersecurity & Infrastructure Security Agency (CISA) guidelines. Ensuring compliance across global supply chains adds complexity.

Third party and supply chain risks: Numerous vendors, contractors and suppliers create multiple points of cyber exposure throughout the OT networks. Robust controls around identity and access management following the principles of zero trust are a must for remote access to devices in the network.

Skills and workforce gaps: There is a shortage of cybersecurity professionals with expertise in OT security. Many staff lack cybersecurity awareness, which can result in increasing insider threats and miscellaneous errors.

Architecture that enables Industry 4.0

Industry 4.0 or 4IR is characterised by a fusion of technologies that is blurring the lines between the physical, digital and biological spheres.

In the digital arena, modern robotics with near real-time controls and newer methods of connectivity (including 5G and edge computing) that connect to the cloud, require a rethink of the modern architectures and fit this into the OT Purdue Model, originally developed by Theodore J. Williams and members of the Industry-Purdue University Consortium for Computer Integrated Manufacturing.

At the same time, options like zero trust access require stricter security controls and present new opportunities for simplifying the layers in the architecture.

New architectures are being proposed to better address the needs for Industry 4.0. One such example is the collection of massive datasets for analytics. This increased level of data can also increase the level of incident handling. Verizon can provide such handling on a 24/7 basis along with recommendations for remediation, next actions and mitigation of cybersecurity risks to the customer, all based on industry best practices.

Building an OT security strategy: Frameworks like NIST CSF, NIST 800-53, ISO 27K, IEC 62443, NIST 800-82, and the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) are very helpful in providing a consistent approach toward managing any cybersecurity programme, as well as in building a customised OT security strategy.

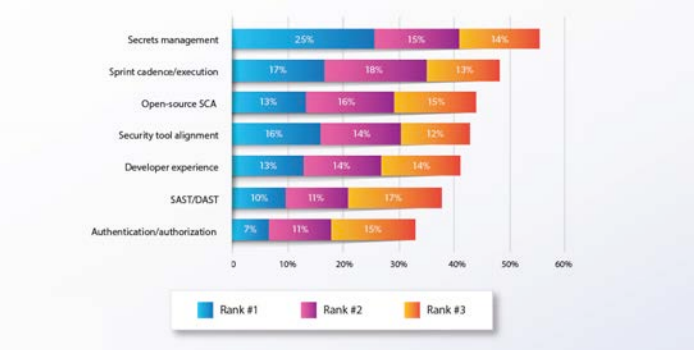


Figure 3: Features of a comprehensive OT security strategy;

Source: *2025 Verizon DBIR*

A simplified strategy for OT security must at least include the following components combined in a governance structure:

Comprehensive asset management framework to keep track of what you have, how old it is, its end-of-life status, and software or firmware versions.

Periodic security assessments of the OT network to identify any security weakness or gaps.

A multilayered network architecture with an IT demilitarized zone (DMZ) providing simplified access to applications hosted in the cloud.

Continuous threat monitoring for improved detection capabilities of anomalous behavior within operational technology networks, encompassing both network and application layers. Also use YARA rules to detect OT-specific malware and integrate learnings into monitoring and visibility programmes.

OT-specific threat intelligence, for early attack detection and prevention. The threat intel should be a combination of Public and government threat intel, industry-specific threat feeds, open-source and community feeds, and vendor and private threat feeds for anomaly detection.

A well designed and tested incident response plan enabling the incident response lifecycle for early detection.

OT security framework transformational phases

The phases above show an example of an OT network security journey. The customer can start in the most relevant phase, depending on their maturity level. In parallel to the technical phase, the following areas around OT governance and organisation are important:

- Focusing on aspects of the organisation that are concerned with innovation and future development
- Executive strategy planning and execution at corporate and business unit level.
- Identify a local champion per factory or group to make the OT planning and execution a bigger success.

PHASE 1: Increase OT visibility

Verizon Security Consulting Services aim to enhance customers' understanding of interconnected IT and OT devices within factories, warehouses and similar environments.

This is achieved through a comprehensive factory asset discovery

and assessment. This can be conducted either onsite or remotely, to ensure complete visibility of the OT devices and their associated risk factors.

PHASE 2: IT and OT Segregation

Segregate the OT network from the IT network by using basic protection controls.

Such segregation can be achieved through the implementation or reuse of physical or virtual firewalls. The following minimum security controls must be activated:

- Threat prevention
- Anti-malware
- Domain Name System (DNS) protection

Our certified consulting services experts facilitate the implementation and configuration of security controls, while Verizon's managed services can oversee their operation from our Security Operations Centres (SOCs).

PHASE 3: Micro-segmentation

the OT Purdue Model. This is achieved through the development of custom blueprints that are repeatable across the company facilities to drive standardisation and simplification. This phase describes the different security zoning and policies. Verizon Security Consulting services can develop and implement these blueprints on existing security controls (Phase 2).

PHASE 4: First automation and life cycle management

Development of specific OT playbooks for seamless creation and updating of OT segment rules, leveraging customer available tools, ticketing systems or via script development.

Life cycle management will be used to keep the devices aligned with required security controls and placed in an extra security zone when no proper maintenance is possible.

PHASE 5: Remote access to the OT environment for suppliers and employees

Activate modern remote access services on a zero-trust need-to-know basis for suppliers. For example, the customer should only have controlled access to their own industrial control systems (ICS), like programmable logic controller (PLC) systems, not to another system that sits in the same segment.

Implement access controls for employees and different suppliers.

Verizon can implement these access control systems, as well as support agent-based and browser-based solutions.

PHASE 6: Activation of advanced – mainly AI-driven – security controls and automation

AI-enhanced security controls such as data loss prevention (DLP), intrusion prevention systems (IPS), and security analytics with user and entity behaviour analytics (UEBA) services, can provide an additional level of visibility in the IT and OT streams. This information can be used to develop new or update the OT playbooks, OT incident response services and enable the development of OT deception-based services.

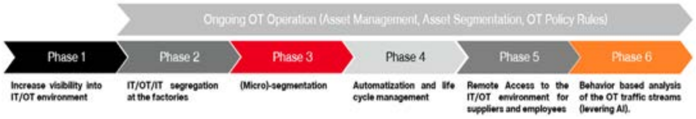
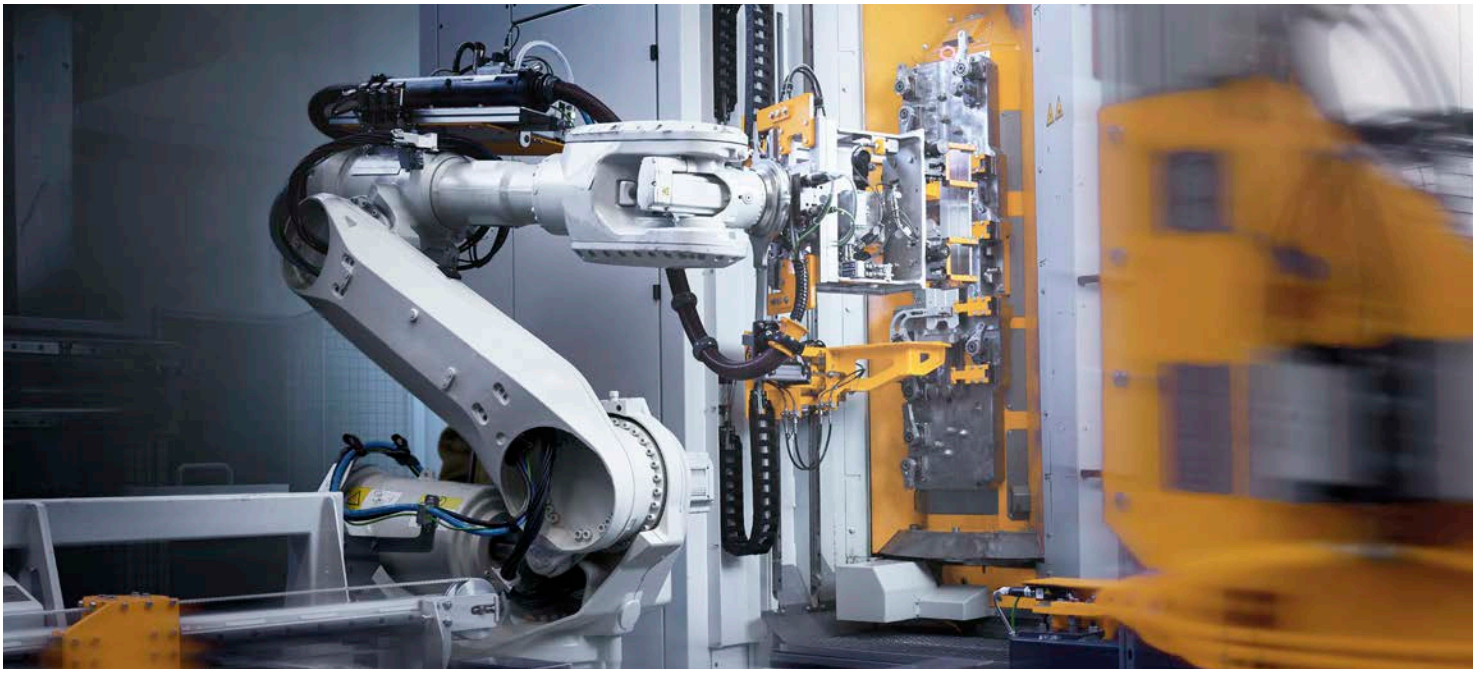

Ongoing OT Operation (Asset Management, Asset Segmentation, OT Policy Rules)
Phase 1
Phase 2
Phase 3
Phase 4
Phase 5
Phase 6
Increase visibility into IT/OT environment
IT/OT/IT segregation at the factories
(Micro)-segmentation
Automatization and life cycle management
Remote Access to the IT/OT environment for suppliers and employees
Behavior based analysis of the OT traffic streams (levering AI).

Figure 4: OT security framework transformational phases;

Source: *Verizon*



Operating model recommendations for OT environments

The recommendations within this section are based on Verizon's experience of the transformation programmes within a similar environment, what worked and what didn't. The near-term goal for the target operating model might mean trying to achieve a matrix structure that better aligns with driving the desired business outcomes. The long-term vision would mean restructuring the organisation and processes.

As a security services provider, Verizon can provide managed takeover and transformation services, as well as other managed security services around these connectivity and security environments. Such an arrangement can enable organisations to focus on their areas of differentiation.

Conclusion

With this holistic approach to OT security, businesses can better achieve the right security setup that meets their needs and their budgets. And they can be better prepared to keep cybercriminals at bay.

Learn More

To find out how Verizon can help you mitigate cyberthreats and protect your business, contact your Verizon Account Manager and visit verizon.com/business/security

The proposed organisational structure has all cross-functional horizontal technologies and relevant resources reporting through the group Chief Information Officer (CIO), with the CIO being accountable for the common services provided to the business unit. Each unit then has a Chief Technology Officer (CTO) or CIO function that is responsible for the differentiated operational technology. The division CIOs report into their division but have matrix reporting into the group CIO while sitting on the CIO board.

The purpose of the CIO board is to provide common alignment and governance on technology. A Chief Information Security Officer (CISO would be accountable for the security functions and also be part of the CIO board.

The diagram below represents a recommended organisational structuring that Verizon has utilised in some IT/OT programmes. This structure represents the common or group technology operating model.

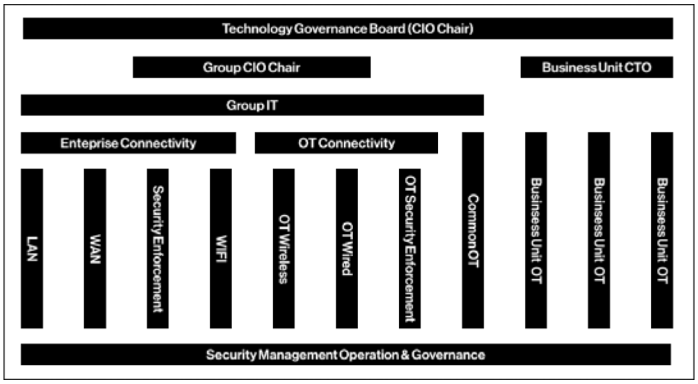


Figure 5: The common/group technology operating model;

Source: *Verizon*

Author and contributors

Author

Marc Borking, OT SME and Principal Security Consultant, Consulting Services , Verizon Business

Contributors

Ashish Khanna, Senior Director and Head of EMEA Security Consulting Services

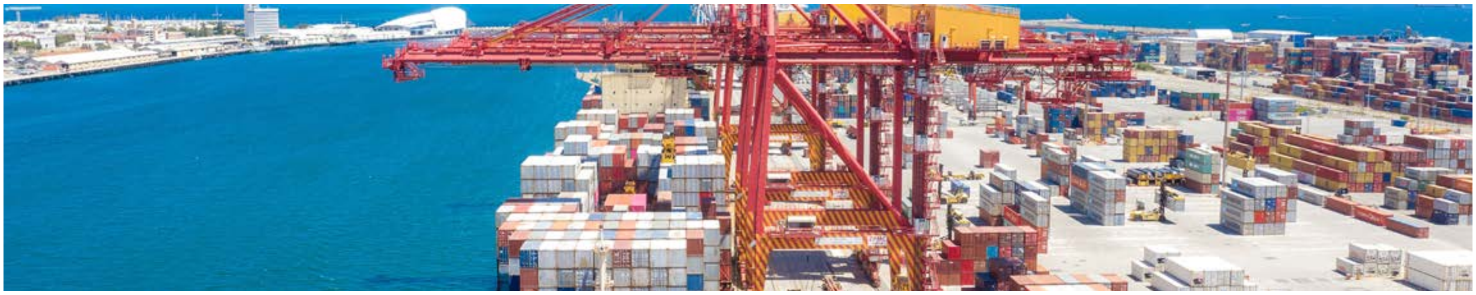
Stephen Young, Director, Security Consulting Services

Beat Kueng, Associate Director, EMEA Security Solutions Architecture

Chris Zijderveld, Associate Director, Security Consulting Services

Ali Akl, Head of Risk and Resilience, EMEA Security Consulting Services

David Samreth, Principal Consultant, Consulting Services



Case study: Global manufacturer

With an increase in automation across the business, a global manufacturing company was encountering a growth in traffic between IT and OT, together with a corresponding increase in security risk and a widening of the attack surface. To meet these challenges, the company took proactive measures, performing a complete security assessment on their existing OT environment and identifying several business and security imperatives.

Business imperatives:

- Update existing security infrastructure which is no longer fit for purpose due to changed requirements and demands driven by the business
- Get a clear view of current implemented architecture, security requirements, segmentation policies, business flows, installed devices, or what the people and processes are
- Ascertain security risks due to a lack of implemented segmentation between OT and IT in factories
- Enable security controls to protect the business assets
- Align security setup and policies, due to history of decentralised IT management
- Mitigate security risks from new global risks and new compliances
- Update the environment ready for future growth and compliance

Solution:

- Run an onsite discovery and OT assessment at the factories; run discovery tools; collect devices information and documents; interview key people; collect traffic flow and logs
- Build a configuration management database (CMDB); create an architecture design; create a security policy template and OT and IT segmentation template
- Reuse or install new on-premises firewalls, configuring new policies, segments and zones and hand over to Verizon Managed Security Services (MSS) management
- Apply local area network (LAN) segmentation (OT and IT) to all (25+) global factories and enable IoT discovery
- Fine-tune security policies in a phased approach, starting with an open learn policy, then adjust during review cycles and finally deny policy after agreement
- Automate playbooks to create and simplify OT segmentation

Benefits and outcomes:

- Help address cyber risk by performing isolation of the IT and OT network, as well between OT and OT segments
- Improve monitoring of security devices with Verizon MSS
- Increase visibility of devices and business flows.
- Enhance compliance in line with new requirements and global threats.

Lessons learned:

What has been agreed in theory always takes more time in practice. That's par for the course for most projects. In this case, the client needed to shift scope before the project could start. Then, when the green light was given, capturing the necessary data: finding the right contact people, discovery of the right switches, and implementing the correct configuration, took longer than anticipated. The business also encountered longer time leads due to competing business priorities.

Align, inform, include and motivate:

Coordination was also crucial. Automation requires alignment between different teams to ensure that playbooks work as designed. Everyone involved needs to know what is expected of them and should be kept fully informed at all times.

It has to be said that equipment vendors generally have broad access to devices. Access can be limited but only by Secure Shell (SSH), Remote Desktop Protocol (RDP) or browser-based access.

Vendors often take time to respond to change requests; clear and direct requests should be made to make timely architecture changes. Behaviour analytics is a time consuming task. Collecting and analysing traffic can be resource-intensive, so this needs to be planned and budgeted for appropriately.

Phase 1

Our success relied on the strong partnership with a dedicated onsite team at the customer's location. By establishing a clear, key point of contact, we were able to streamline communication and ensure all project activities remained aligned from start to finish.

Initial discovery and configuration required a thorough, meticulous process to navigate the existing network infrastructure. We successfully addressed the challenge of network traffic capture by innovating a solution to route data through the firewall, which improved performance and reliability. Although the project's start date was adjusted to accommodate the customer's changing design needs, this allowed for a more comprehensive and well-aligned final plan, ultimately leading to a successful implementation.

Phase 2

Navigating local restrictions and government regulations was a key challenge during the initial delivery of firewalls. By adapting our approach and adjusting project timelines, we successfully met all legal requirements and ensured a compliant rollout in every region.

Although the initial segmentation phase began at a measured pace, it was essential for developing a robust and repeatable process. The team used this time to identify and address potential pitfalls, which allowed us to accelerate the pace of future work significantly. This methodical approach paid off, as each subsequent location benefited from a refined process and a clear understanding of the project's design, leading to a much faster and smoother completion for every new site

Phase 3

Successfully executing the second phase of microsegmentation required a careful, phased approach to prevent any disruption to business operations. A key factor of success was the insight gained from the local contact, whose in-depth asset discovery proved to be invaluable. To ensure accuracy, extensive firewall log analysis was performed to fully understand all asset flows, a crucial step before securely implementing deny rules.

Phase 4

Aligning different teams is essential for developing effective and efficient automation playbooks. By ensuring all teams are in sync, the team can create solutions that work seamlessly and as intended.

Phase 5

To enhance security, Verizon is helping the business move to a more controlled access model for vendors. This includes establishing a new standard that limits access to SSH, RDP, or browser-based methods only. This change is being implemented through direct requests and close collaboration with vendors to ensure their access needs are met while fully aligning with the new architecture.

Phase 6

Behavioural analytics, while requiring a significant effort, provide critical insights. The process of collecting and analysing this traffic is a valuable, high-impact investment that yields a deeper understanding of network activity.

verizon
business