Cyber Security for Operational Technology (OT)

Protect your critical production networks and assets

We understand your challenges

Manufacturing and utilities industries are striving to digitally secure their Operational Technology (hardware and software that control industrial equipment). Are the results up to requirements? With the rise of IT connectivity comes the added exposure to cyber attacks. Ensuring effective secure digital operations to maximize uptime and worker safety, to protect customer and business data and to avoid supply chain disruption is not a one off-challenge.

Proactively limiting risk of OT networks is key to embracing the rapid pace of digital disruption. Our experts are committed to offer you a secure network that provides around the clock protection for your industrial processes and business critical assets. We support you to assess, protect and manage your people and critical infrastructure, seamlessly, safely and securely.

Fujitsu collaborates with customers using three complementary services:

OT assessment and asset discovery
analyzing your existing networks, identifying gaps in compliance and standards, establishing your risk profile and baselining your networked digital assets.

OT network transformation
applying priority remediations to protect your OT networks.

OT managed monitoring service
a 24/7 service identifying anomalous behaviors across OT environments.

Differences between IT and OT

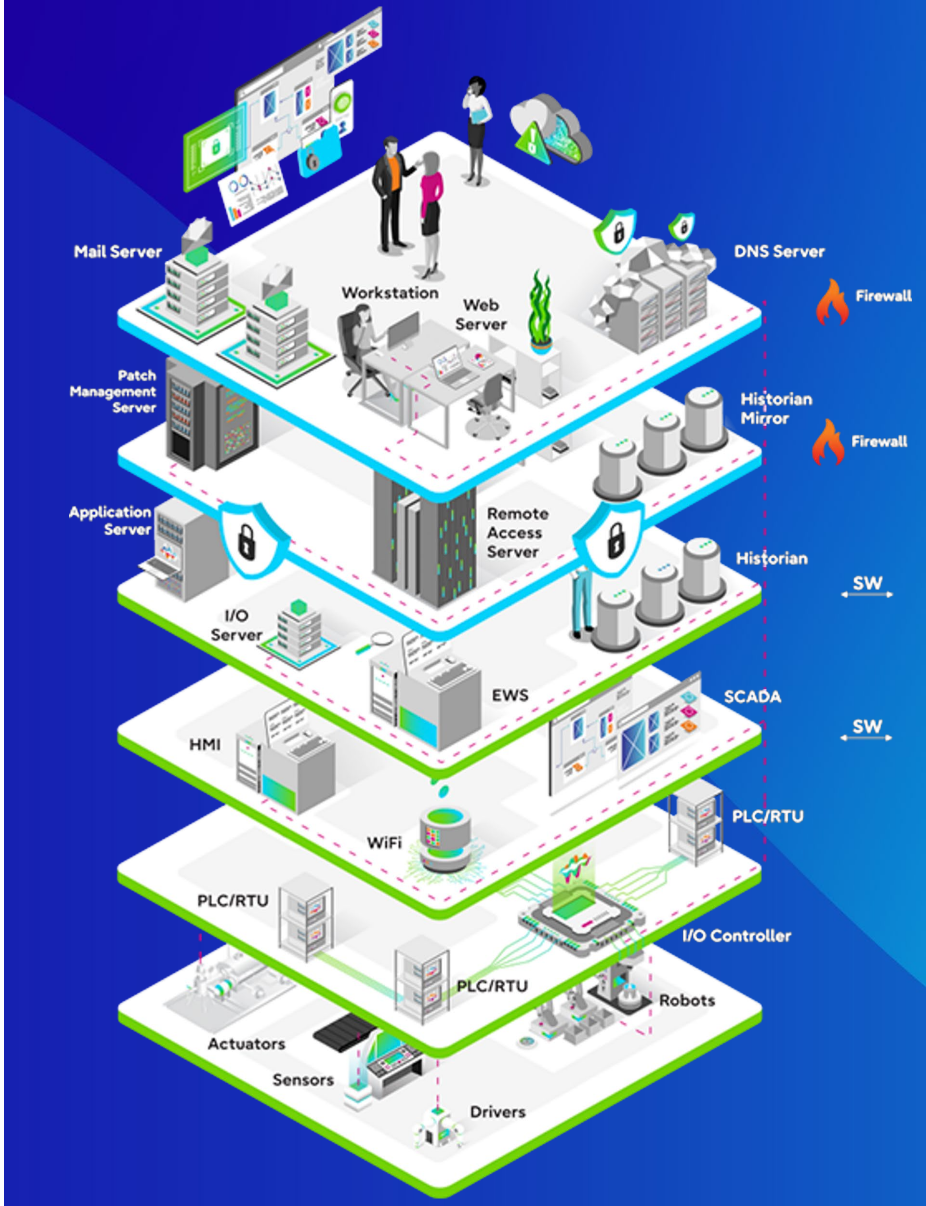
IT mindset

- The world is virtual
- Priority is data confidentiality, availability and integrity
- Corporate management of networked assets
- Agility

OT mindset

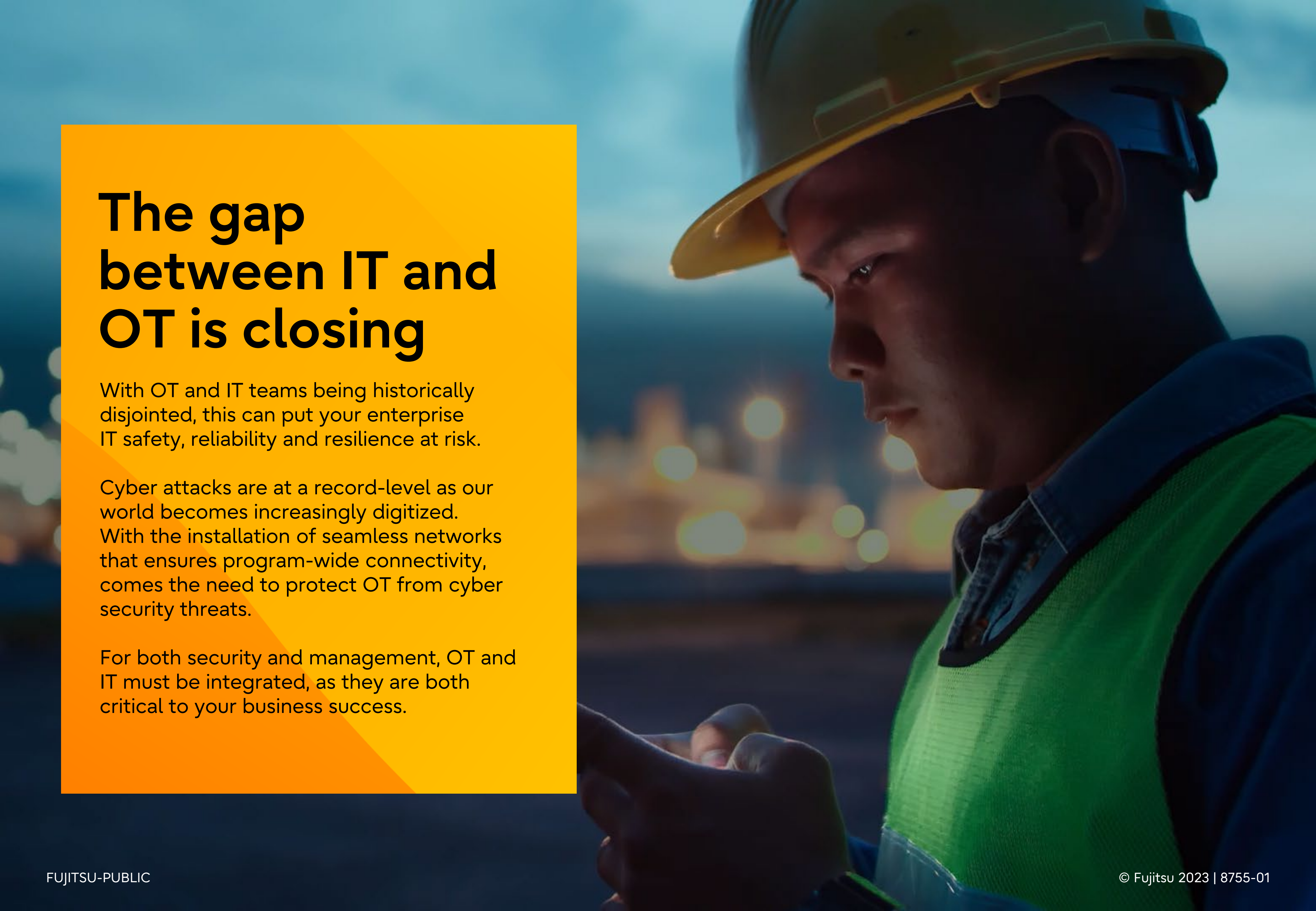
- The world is physical
- Priority is safety, availability and resilience of production processes
- Plant-level management of networked assets
- Measuring overall equipment effectiveness
- “Don’t touch, don’t break” culture

The differences between IT and OT are not only in technology, but also in people, training, organization and culture.



Manufacturers and utilities companies need to...

- Ensure production process continuity and physical safety
- Achieve sustainable & compliant production
- Continuously improve Overall Equipment Effectiveness (OEE)
- Gain competitive advantage in new value chains
- Be data driven to improve business outcomes



The gap between IT and OT is closing

With OT and IT teams being historically disjointed, this can put your enterprise IT safety, reliability and resilience at risk.

Cyber attacks are at a record-level as our world becomes increasingly digitized. With the installation of seamless networks that ensures program-wide connectivity, comes the need to protect OT from cyber security threats.

For both security and management, OT and IT must be integrated, as they are both critical to your business success.

Smart production requires smart cyber security

If digital threats aren't addressed, they can impact production targets, causing damage to machines, workers and even whole communities, resulting in a loss of intellectual property. These threats may come from external actors, malicious insiders or via suppliers. Our goal is to alleviate any stress surrounding cyber security by drastically diminishing these threats.

Together, we can manage the pressures of cyber security under the imperatives of reliable and compliant operations. Comprehensive guidelines state the necessary requirements for the operators, integrators and component suppliers of the physical processes. We know it can get complicated.

That's why we're here to help put that theory into practice.

New connectivity networks and evolving demands will require increased security monitoring of core internal assets and processes. Many production environments also lack visibility of their digital assets. We aim to help you identify and harness your data, so you can utilize it effectively, therefore improving business operations. So, what are the next steps?

Manufacturers and utilities companies were the **No.1** cyber-attack target in 2021*, even ahead of Financial Services

On average, every hour of unplanned downtime costs the business **$532,000****

* Source: IBM Security X-Force Threat Intelligence Index 2022 report
** Source: The True Cost of Downtime report

Our approach

Our approach is simple: assess, protect and help you to manage your critical infrastructure safely and securely. We'll work together with you to create a solid foundation, capable of taking the weight of an ever-evolving technological landscape. Each of the three complementary services can be ordered and delivered independently.

Fujitsu OT cyber security services comprises three elements:

OT assessment and asset discovery

Analyzing your existing networks, identifying gaps in compliance and standards, establishing your risk profile and baselining your networked digital assets.

OT network transformation

Applying priority remediations to protect your OT networks.

OT managed monitoring service

A 24/7 service identifying anomalous behaviors across OT environments.

OT assessment and asset discovery

‘You can’t control what you can’t see’

Initially, we will baseline your existing network infrastructure from the cyber security perspective of people, processes and technology. Using the analysis, we recommend a development roadmap which reflects the technical, organizational and compliance-oriented demands unique to your business.

The assessment includes an automated discovery of networked OT assets (e.g. PLCs, RTUs, SCADA systems, workstations, HMIs, historians). Enhanced with staff knowledge of their use, this allows a qualitative risk assessment mapped to the production process. The asset data that is captured during the security assessment is available for further use, for instance to feed a Configuration Management Database (CMDB).

OT network transformation

To transform your network infrastructure, we’ll start by evaluating existing connectivity points within and, if applicable, between sites. Making use of previous investments (e.g. firewalls), we’ll implement a segmented network architecture that mirrors the Purdue model, demonstrating the functional demands and the risk profiles across your entire production line.
During implementation and transformation, we’ll work closely with you, your OT field team and your specialist OT partners to minimize the chance of disruption to your critical processes.

We use tested and cost-effective techniques, such as SD-WAN, to strengthen wireless connectivity between sites and the enterprise network. Underlying our secure network architecture are the zones and conduits approach of IEC 62443-3-2.

OT managed monitoring service

Our OT monitoring service is provided remotely from our Security Operating Centers (SOCs), which continually monitors and directs information about your OT assets to your own control center interface. Actionable insights are instantly reported to your operations management team, enabling you to prevent, detect, mitigate and recover from cyber incidents.

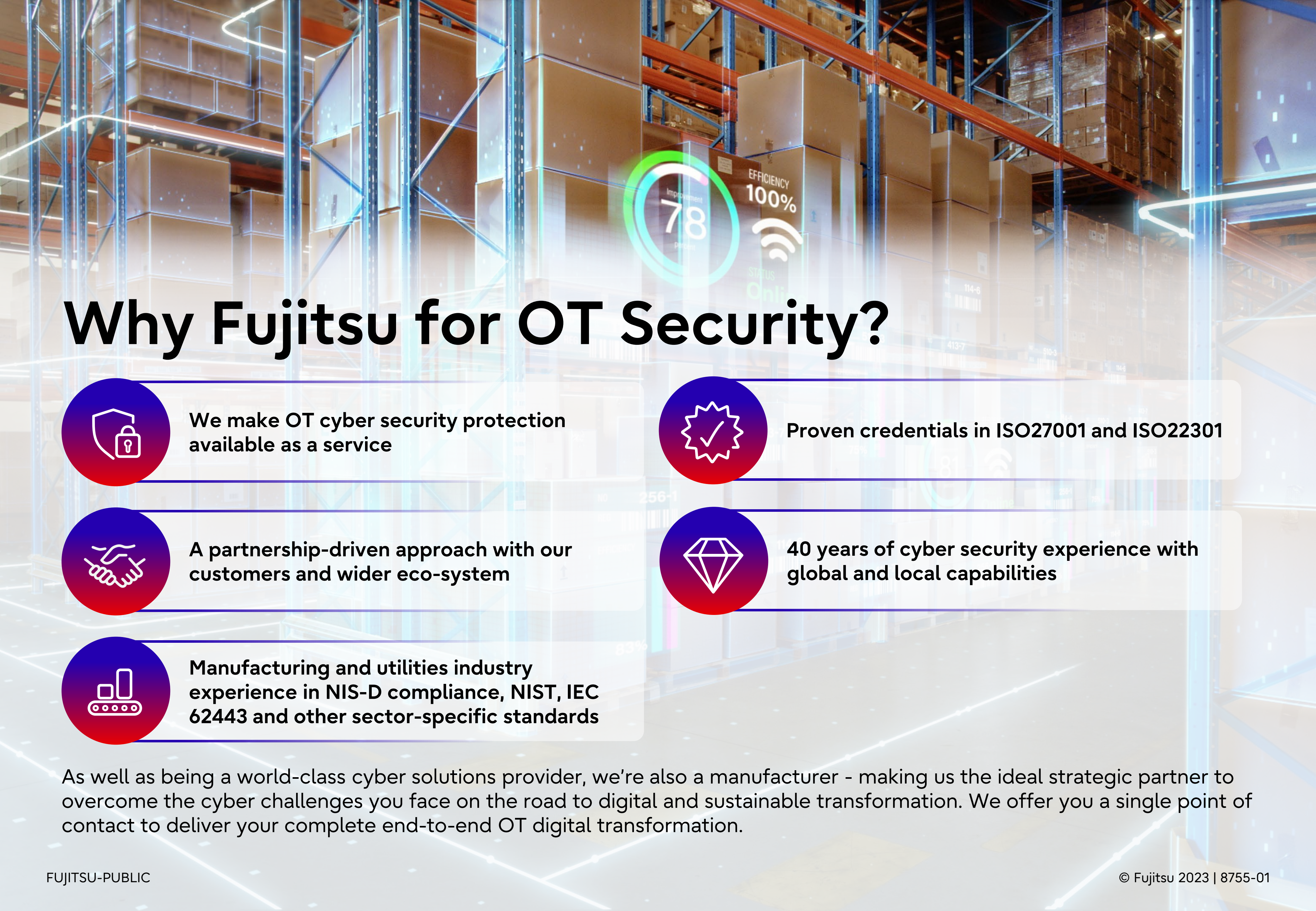
By establishing the wider picture of your working model and data exchange, we can fully understand the scope of your normal cyber OT behavior. Rehearsing communication between our team and yours guarantees a quick reaction in the event of a threat.

It is important to us that you feel confident in your OT cyber security, so we regularly undertake performance reviews, analyzing effectiveness and customer satisfaction.

Business benefits

Delivering five key business benefits to manufacturing and utilities customers:

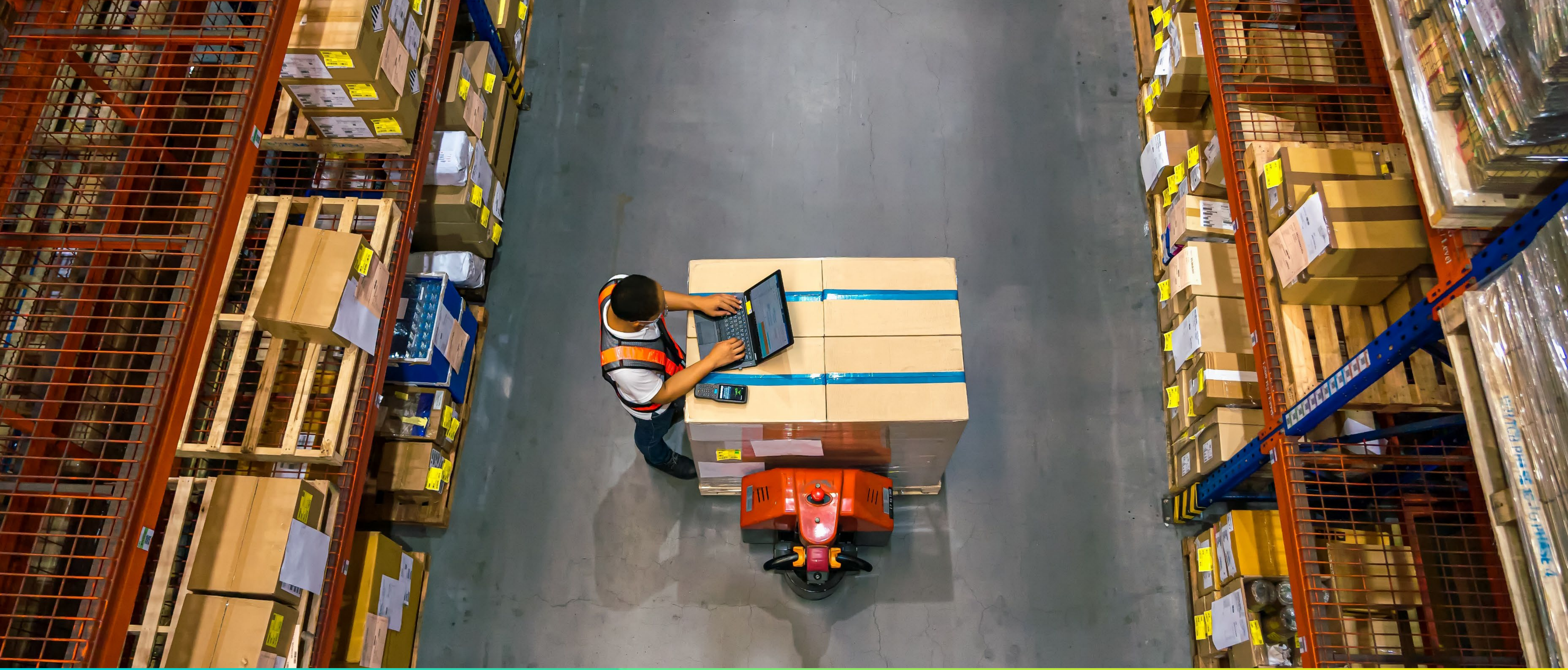
- Maximizing production process continuity
- Sustain worker wellbeing and physical safety standards
- Cyber security risk mitigation - protecting IP from cyber attacks
- Secure access to production data for all types of enterprise-wide improvements
- Compliance in regulated industries - CNI, industry standards & policies and data



Why Fujitsu for OT Security?

- We make OT cyber security protection available as a service
- Proven credentials in ISO27001 and ISO22301
- A partnership-driven approach with our customers and wider eco-system
- 40 years of cyber security experience with global and local capabilities
- Manufacturing and utilities industry experience in NIS-D compliance, NIST, IEC 62443 and other sector-specific standards

As well as being a world-class cyber solutions provider, we're also a manufacturer - making us the ideal strategic partner to overcome the cyber challenges you face on the road to digital and sustainable transformation. We offer you a single point of contact to deliver your complete end-to-end OT digital transformation.



You think your OT environment is secure?

Let's talk about how we can take your OT security to the next level.

Learn more about Fujitsu OT security **here**.

FUJITSU

OT Security Technology Partner:

Radiflow | FORTINET | servicenow

This document is current as of the initial date of publication and subject to be changed by Fujitsu without notice. This material is provided for information purposes only and Fujitsu assumes no liability related to its use.