Products Included in our solution

Prevention	Trend Micro Cloud One™	Hybrid cloud security
	Trend Micro™ TippingPoint™ Threat Protection System	Intrusion prevention system
	Trend Micro IoT Security™	Built-in agent security for IoT devices
Detection	Trend Micro™ Deep Discovery™ Inspector	Threat visualization and early detection
Resilience	EdgeFire™	Industrial firewall
	EdgeIPS™ / EdgeIPS™ Pro	Industrial IPS
	TXOne StellarProtect	Purpose-built ICS endpoint security
	TXOne StellarEnforce	Trust-list based ICS endpoint protection
	Trend Micro Portable Security™ 3	Malware scan and clean-up tool without installation
	OT Defense Console™	Industrial central management console

Threat intelligence supporting our solutions

TREND MICRO | research

Cyber Threats · Vulnerabilities & Exploits · Targeted Attacks · AI & ML · IoT · OT / IIoT · Cybercriminal Undergrounds · Future Threat Landscape

Research security risks to the manufacturing industryspecific, which covers both IT and OT

ZERO DAY INITIATIVE

Vulnerability discovery community operated by Trend Micro

Discovered and reported over half (52%) of the vulnerabilities in the public market throughout 2019

Source: Omdia, 2019 Public Vulnerability Market

https://www.trendmicro.com/smartfactories

TREND MICRO™

Securing Your Connected World

USA Headquarters Trend Micro Incorporated
225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone: 1-888-977-4200 Email: us_info@trendmicro.com

Canada Headquarters Trend Micro Canada Technologies Inc.
40 Hines Road, Suite 200 Ottawa, Ontario, Canada K2K 2M5
Tel: 1-866-684-7332 Email: CanadaChannelSales@trendmicro.com

[BR001_Smart_Factory_Overview_210419US]

TREND MICRO™

Security Solutions for Smart Factories

Keep operations running

Operational stoppage risks due to cyberattacks

Risk 1
Stoppage of manufacturing system due to virus infection

Risk 2
Equipment damage due to system malfunction

Risk 3
Production of defective products due to malfunction of equipment

Convergence of IT and OT:

Protecting interconnected systems to improve efficiency.

Smart factories aim to improve production efficiency by using industrial IoT (IIoT) technologies and integrating with business systems.

However, its adoption expands the attack surface, which benefits cyber attackers and increases the risk of operation stoppages. This makes foresight-driven IIoT security essential to smart factories.

Security challenges faced by smart factories

Low visibility

There may be cases where there is no appropriate visibility from a security perspective.

Therefore, if there is a vulnerable device, effective and timely patching cannot be applied.

Unpatched devices

You may have to wait for a planned outage.

As a result, patches cannot be applied even if the device is known to be vulnerable.

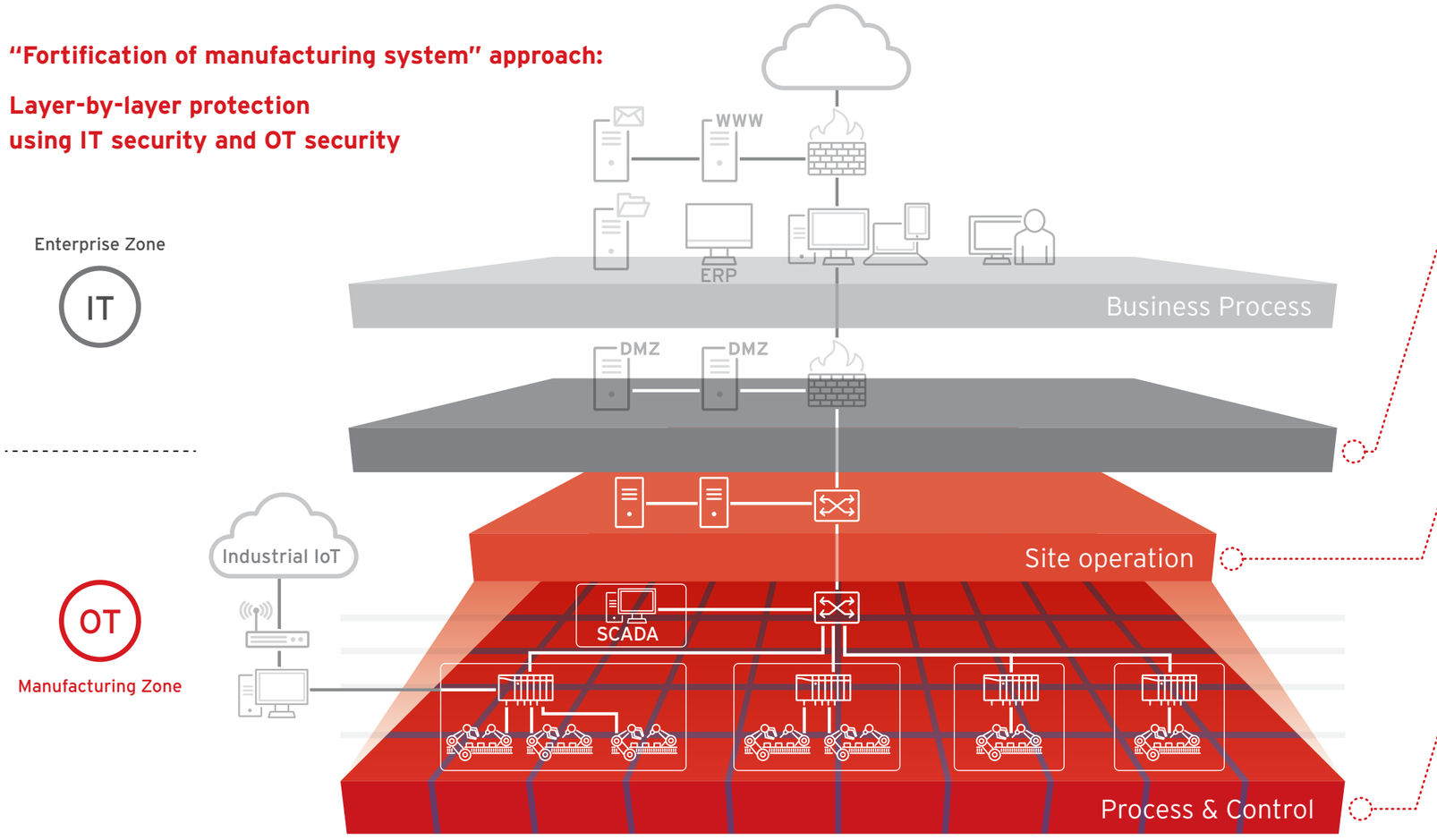
Weak authentication

There are devices that can be accessed without authentication. If it is used, a malicious actor may be able to operate a critical device.

Trend Micro security solutions for smart factories

"Fortification of manufacturing system" approach:

Layer-by-layer protection using IT security and OT security



PREVENTION

Stop cyberattacks from the IT environment to the OT environment

- Perimeter defense to prevent cyberattacks designed to exploit vulnerabilities
- Protection of various IoT devices such as IoT gateways used in industrial services

DETECTION

Identify internal activities of cyberattack in the OT environment

- Monitor network traffic from multiple perspectives. Receive early detection of suspicious movements

RESILIENCE

Defend industrial control devices

- Prevent the spread of infection by network segmentation
- Protect critical equipment at the network level from cyberattacks designed to exploit vulnerabilities
- Protect ICS endpoints
- Prevent the execution of malware and unauthorized programs on legacy OS terminals (Lockdown)
- Scan and clean up malware in the devices where security software cannot be installed
- Gain visibility into the asset information of production devices