TREND MICRO

Securing Your
Connected World

Manufacturing Cybersecurity Case Studies

Mitigating four major challenges: Infrastructure, Organization, Threat, and Factory

In this e-book, Trend Micro, a trusted cybersecurity partner for manufacturing companies around the world, identifies and helps solve four major challenges; infrastructure, organization, threat, and factory.

Infrastructure

Global Data Center

How do you securely operate a system when cloud, virtual, on-premises, and legacy consoles needs to coexist?

Hybrid Infrastructure

How do you keep the performance and security of data centers' core networks connected around the world?

Organization

Compliance

How do you provide reports and confirmation of security audits?

Small Security Team

How do you overcome management pressures and handle daily alerts with a small team of people?

Threat

Incident Response

What to do when production is stopped due to a cyberattack?

Visibility

How can we visualize stealthy and undetected active threats?

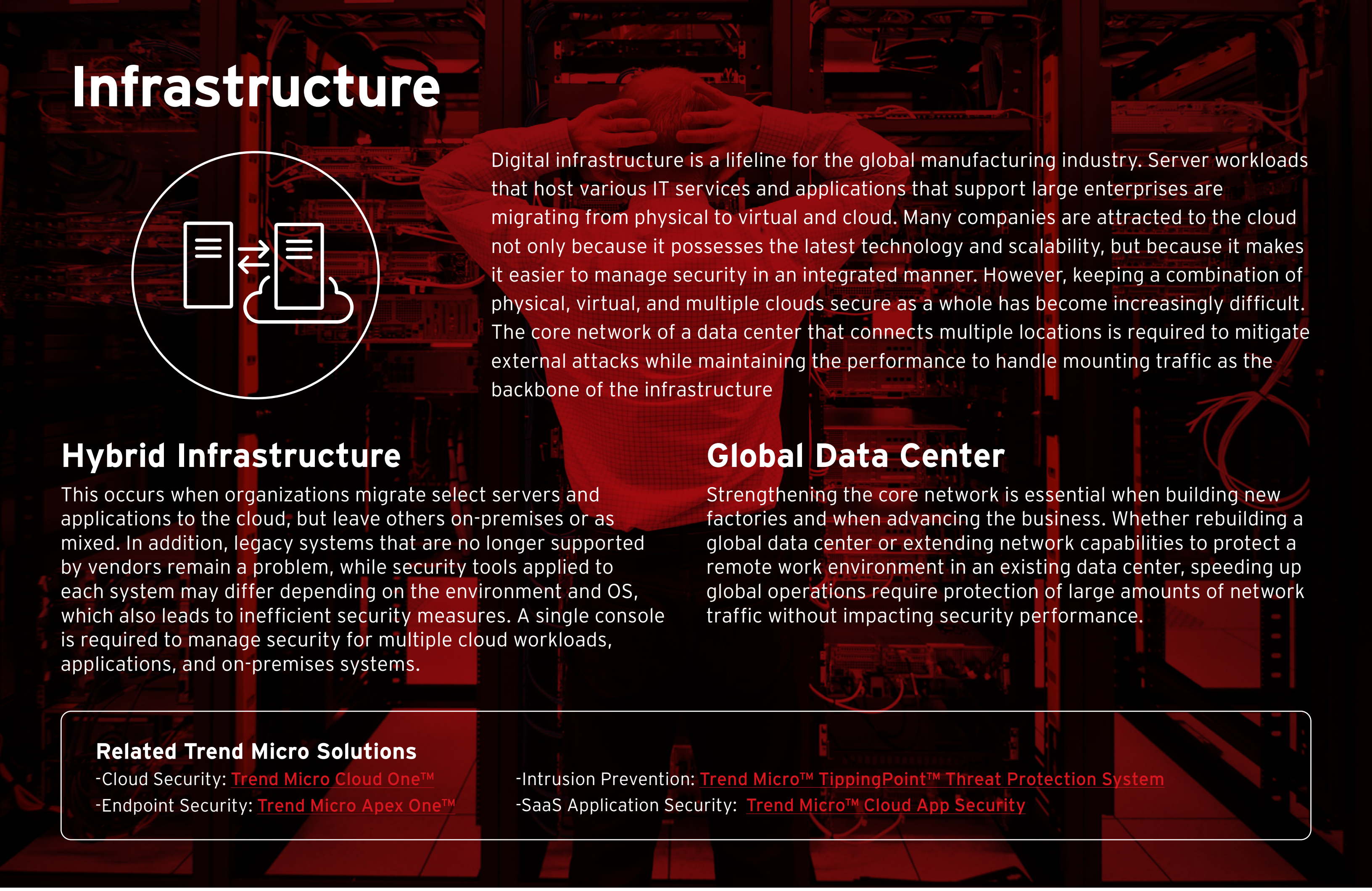
Factory

OT/Shop Floor

How do you protect the critical assets and network on a shop floor?

Industrial Products

How to secure industrial products and provide service with safely?



Infrastructure

Digital infrastructure is a lifeline for the global manufacturing industry. Server workloads that host various IT services and applications that support large enterprises are migrating from physical to virtual and cloud. Many companies are attracted to the cloud not only because it possesses the latest technology and scalability, but because it makes it easier to manage security in an integrated manner. However, keeping a combination of physical, virtual, and multiple clouds secure as a whole has become increasingly difficult. The core network of a data center that connects multiple locations is required to mitigate external attacks while maintaining the performance to handle mounting traffic as the backbone of the infrastructure

Hybrid Infrastructure

This occurs when organizations migrate select servers and applications to the cloud, but leave others on-premises or as mixed. In addition, legacy systems that are no longer supported by vendors remain a problem, while security tools applied to each system may differ depending on the environment and OS, which also leads to inefficient security measures. A single console is required to manage security for multiple cloud workloads, applications, and on-premises systems.

Global Data Center

Strengthening the core network is essential when building new factories and when advancing the business. Whether rebuilding a global data center or extending network capabilities to protect a remote work environment in an existing data center, speeding up global operations require protection of large amounts of network traffic without impacting security performance.

Related Trend Micro Solutions

-Cloud Security: Trend Micro Cloud One™

-Endpoint Security: Trend Micro Apex One™

-Intrusion Prevention: Trend Micro™ TippingPoint™ Threat Protection System

-SaaS Application Security: Trend Micro™ Cloud App Security

Trend Micro helps solve infrastructure challenges with integrated security in mixed environments and never slows down the performance of data center networks.

Region: UK
Product: Food
Revenue: $50 billion+
Employees: 100,000+

- ✓ Move from traditional data center to hybrid cloud
- ✓ AWS, Microsoft® Azure®, Microsoft® Windows®, Linux®, AIX

Region: Germany
Product: Electric motor
Revenue: $2 billion+
Employees: 10,000+

- ✓ Heterogeneous infrastructure
- ✓ Visibility and transparency

Region: US
Product: Automotive
Revenue: $100 billion+
Employees: 100,000+

- ✓ High bandwidth
- ✓ Asymmetrical routed network

Region: US
Product: Industrial pump
Revenue: $4 billion+
Employees: 10,000+

- ✓ Legacy OS servers (W2008, 2003, Linux)
- ✓ Security as a service to deploy easily on legacy and new platforms

Region: Korea
Product: Semiconductor
Revenue: $30 billion+
Employees: 30,000+

- ✓ Create new network section for new plant extension
- ✓ Heavy traffic

Region: UK
Product: Jet engine
Revenue: $50 billion+
Employees: 30,000+

- ✓ New data center
- ✓ High performance and low maintenance

Region: US
Product: Optical lenz
Revenue: $10 billion+
Employees: 50,000+

- ✓ Multi-cloud, VDI, on-premises
- ✓ Consolidate security agents and consoles

Region: Germany
Product: Automotive
Revenue: $100 billion+
Employees: 100,000+

- ✓ IPS deployed inline in front of DCs
- ✓ 100% uptime and security effectiveness

Region: Austria
Product: Heavy equipment
Revenue: $1 billion+
Employees: 10,000+

- ✓ Migration to M365 E3, but some workloads coexist on-premises or on other cloud

Organization

The manufacturing industry plays a role in the supply chain that supports people's lives as one of the critical infrastructures. In each country, governments and regulatory agencies require companies to remain compliant and require a high level of policy, preparedness, security control, and processes. Management must submit a report to respond to regular audits, however, security teams are often too small and overstretched to provide these intricate reports to management. In addition, these limited teams must also manage the security of a wide range of systems, operations, and employees. While responding to event alerts that are raised daily by security systems, it is also necessary to respond to security standards and implementations based on system plans.

Compliance

Organizations need to implement security controls that are in compliance with the regulations, while preparing for regular audits through logging and reporting. Security tools that include controls required for multiple regulations, prevent attacks, and document the status of security events and compliance policy is useful when reporting, reducing the preparation time and effort required to support auditing.

Small Security Teams

Security teams are busy responding to alerts from countless security tools at multiple layers and locations. While SIEM is an effective tool, it can often be too complex to operate with limited personnel and skills. In addition, as the cloud shift progresses, the same security must be used for multiple projects. Streamlining operations within your organization is key to receiving actionable alerts, while managed services, are also an option worth considering.

Related Trend Micro Solutions

-Cloud Security: Trend Micro Cloud One

-EDR, Endpoint Security: Trend Micro Apex One

-Package: Trend Micro™ Smart Protection Complete

-Advanced Threat Detection: Trend Micro™ Deep Discovery™

-Managed Detection and Response: Trend Micro™ Managed XDR

Trend Micro helps security teams achieve operational tasks, including reporting for security audits and responding to day-to-day alerts, which contributes to solving business challenges.

Region: New Zealand
Product: Construction
Revenue: $3 billion+
Employees: 5,000+

- Periodic security audits required
- Making new contracts require a certain level of security posture and proof
- Increasing alerts and pressures on small team

Region: Australia
Product: Iron ore
Revenue: $10 billion+
Employees: 5,000+

- Keeping up with the alerts from the various layers of security
- Small security team
- Already have a managed SIEM/SOC, but saw this as ultimately complimentary

Region: Germany
Product: Metal
Revenue: $10 billion+
Employees: 5,000+

- IMDAX listed company has to fulfil compliance requirements
- Unhappy with MSP of data center
- Move SAP from on-premises to "SAP on Azure"
- Rollout Microsoft® Office 365™ E3
- Very small security team

Region: US
Product: Chemical
Revenue: $800 million+
Employees: 3,000+

- Compliance reporting
- Remediate/remove threat without impacting performance

Region: Brazil
Product: Petrochemical
Revenue: $600 million+
Employees: 1,000+

- Multiple data centers
- Mission-critical information and infrastructure
- Compliance requirements for this highly regulated industry

Threat

As IT teams become aware of a number of daily threats to the organization, like ransomware, zero-day attacks, and targeted attacks, the real challenge lies in identifying which threats are high-risk. The level of attack depending on the attacker's motives, skills, and resources should influence the level of security needed. Our research on factory honeypots have revealed that even low-level attacks can leave an impact on production activities. These factors, along with targeted attacks that can remain unnoticed for months or even years can lead to production downtime in the manufacturing industry. So it is required to improve visualization and build an on-premises incident response system.

Visibility

Although the Zero Trust architecture is gaining attention, in reality many companies have boundaries and are required to visualize threats at numerous entrances and inside networks. There is a need to detect unknown threats earlier in the attack stage in the cyber kill chain that consists of "reconnaissance", "weaponization", "delivery", "exploit", "installation", "command & control (C & C)", and "execution of purpose". To deal with this, it is effective to gain visibility of the entire environment, not just the point solution.

Incident Response

Security events that have a high probability of affecting your business are called incidents. In reality, it is considered an incident after it has already affected the business. You need to detect and analyze what is happening, contain the effect, and remove the identified cause. Repeat this cycle to return to usual operations. Security teams can rely on external experts throughout this process. Also, it should be noted that the lessons learned from experienced incidents will lead to the improvement in the level of security.

Related Trend Micro Solutions

-Advanced Threat Detection: Deep Discovery

-Managed Detection and Response: Managed XDR

-EDR, Endpoint Security: Trend Micro Apex One

-Package: Smart Protection Complete

Trend Micro delivers visibility of potential threats before an incident occurs and mitigates threats by supporting processes at the incident level.

Region: Germany
Product: Industrial Technology
Revenue: $300 million+
Employees: 2,000+

- ✓ Critical production outages by incident
- ✓ Built a new clean network and raised up the security level

Region: UK
Product: Food
Revenue: $400 million+
Employees: 500+

- ✓ Production site down by ransomware attack
- ✓ Large parts of their network including back-ups were encrypted on multiple sites

Region: Russia
Product: Cement
Employees: 3,000+

- ✓ Looking for breach detection system
- ✓ Modern threats, especially through email and web

Region: Germany
Product: Biopharmaceutical
Revenue: $14 million+
Employees: 300+

- ✓ Increased media attention and might be a vulnerable target
- ✓ Proactive incident response engagement

Region: US
Product: Building material
Revenue: $3 billion+
Employees: 5,000+

- ✓ East-west network visibility
- ✓ Blind-spots, C&C call backs
- ✓ Targeted attacks, IoCs

Region: India
Product: Textile
Revenue: $900 million+
Employees: 20,000+

- ✓ Multiple vectors like endpoint, email, servers
- ✓ Zero-day, unknown threats
- ✓ Visibility of threat life cycle with complete report

Factory

For factories and manufacturers, the need for cybersecurity is urgent. This is due to the concerns arising from operation stoppages caused by security incidents, resulting in loss of revenue. Unlike enterprise IT, system administrators face several issues within smart factory security, namely with difficult-to-eliminate vulnerabilities, the spread of malware, and flat network configurations. Furthermore, when implementing countermeasures, problems within the operating environment (i.e. prohibited software installation), makes it difficult to resolve these issues. In smart factories, IT is actively used in OT (industrial control system) environments and network connections are expanding. In such a complicated environment, it is important to utilize security that combines technology optimized for OT and IT.

OT/Shop Floor

One of the biggest differences between an IT environment, and OT, such as a shop floor, is that availability is prioritized over confidentiality. Therefore the security patch cannot be applied because it is not permitted to make changes to the terminal due to unavailability of legacy patches. In addition, flat networks can easily lead to lateral infections once malware enters. The challenge is to improve the security level without modifying the existing network environment as much as possible, and to standardize and protect factory bases across regions.

Industrial Products

Industrial control systems, such as SCADA, are no longer threat-free because they are included on general-purposed OS and network connections. It must be shipped as a "safe product" and kept secure in the customer's environment for long periods of time. Although services that build and operate industrial control systems require experts who understand IT security and have a knowledge and OT systems, it is recommended that a partner should have both knowledge and the ability to recognize security according to the customer's business process.

Related Trend Micro Solutions

-Industrial IPS: EdgeIPS™
-Industrial firewall: EdgeFire™
-Lockdown mission-critical asset: Trend Micro SafeLock™ TXOne Edition
-Install-less malware scan tool: Trend Micro Portable Security™ 3

Trend Micro helps factories "keep operations running" without significant system changes and with less security operation resources.

Region: Japan
Product: Heavy electric machinery
Revenue: $1 billion+
Employees: 4,000+

- ✓ Provide industrial terminals bundled with application control software
- ✓ Malware scan to solutions before shipment
- ✓ SCADA systems are possibly connected to office network

Region: Germany
Product: Chemical
Revenue: $10 billion+
Employees: 100,000+

- ✓ New guideline demands a higher security level
- ✓ Hundreds of production systems operating offline
- ✓ Not connected to the network and managed by old legacy OS

Region: US
Product: Industrial service
Revenue: $20 billion+
Employees: 50,000+

- ✓ Control systems bundled with ICS security assessments for IIoT cybersecurity and threats
- ✓ Develop best practices and resources
- ✓ Expertise to identify risk and threat vectors in specific OT environments
- ✓ Security solutions purpose-built for OT environments

Region: Japan
Product: Automotive
Revenue: $30 billion+
Employees: 10,000+

- ✓ SCADA in closed network
- ✓ 24/7 operation
- ✓ Visibility among multi-factory

Region: Japan
Product: Automotive
Revenue: $50 billion+
Employees: 100,000+

- ✓ Unpatched legacy OS
- ✓ Network switch replacement
- ✓ Global security standardization

Why Trend Micro?

Our Solutions

We help you solve advanced security challenges that affect infrastructure, organization, and threats with minimal TCO over a long period of time

Integrated threat intelligence

The Trend Micro Research team delivers 24/7 threat research from around the globe, vulnerability intelligence from our Trend Micro™ Zero Day Initiative™ (ZDI) program, and insights on the IT and OT cybersecurity landscape. Our connected solutions and XDR capabilities empower CISOs and security operation teams with more precise alert detection and automatic response, reducing monitoring complexity and operating costs.

Single vendor, global support

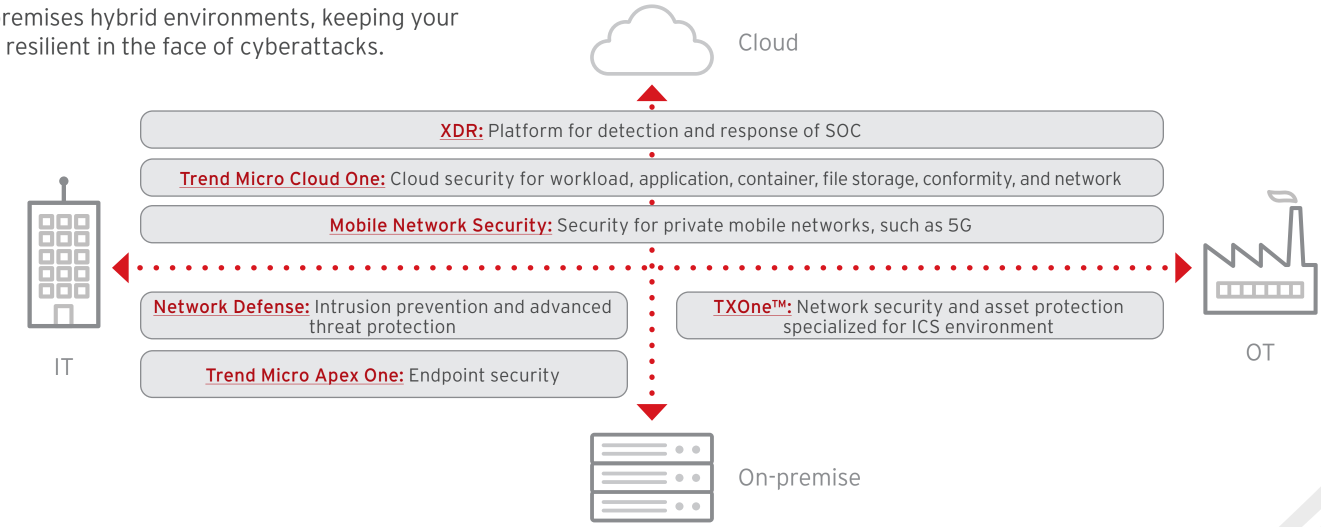
Using multiple products is not efficient—it creates complexity and requires a lot of time to evaluate, create SOP, and establish a support scheme. Deploy a single solution, utilize single SOP worldwide, and respond quickly and smoothly to incidents to ensure stable operations and minimal TCO.

Sustainability

As a trusted company with 30+ years of experience, Trend Micro has the strong financial base and robust cybersecurity offering required to protect customers in private and public sectors.

Looking towards the future of smart factories

We protect both IT and OT domains, as well as cloud and on-premises hybrid environments, keeping your business resilient in the face of cyberattacks.



XDR: Platform for detection and response of SOC

Trend Micro Cloud One: Cloud security for workload, application, container, file storage, conformity, and network

Mobile Network Security: Security for private mobile networks, such as 5G

Network Defense: Intrusion prevention and advanced threat protection

TXOne™: Network security and asset protection specialized for ICS environment

Trend Micro Apex One: Endpoint security

Keep Operations Running

Trend Micro provides complete solutions to secure smart factories. It merges IT and OT security and is implemented through three steps; prevention, detection, and persistence. See our Smart Factory solutions page for details.

Securing Your
Connected World