A Trend Micro Technical Brief | **November 2021**

Three Steps to Keep Smart Factory Operations Running

» Cybersecurity best practices for each industrial environment.

Table of contents

EXECUTIVE SUMMARY

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 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.

Considering these issues and challenges, cyber risk can be minimized through three steps: "Prevention", "Detection", and "Resilience" via security design. Especially 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 effective to protect with security that combines technology optimized for OT and IT. These approaches should help ensure the continuity of operations in smart factories.

Therefore, this technical brief introduces practical security countermeasures that should be considered at the system planning and design phase. In particular, based on the above issues, we propose the following best practices for each environment:

- The existing environment that many companies should work on first
- Smart factory environments that will be newly constructed in the future

By developing such countermeasures, it is possible to efficiently reduce cybersecurity risk and thereby achieve continual operations in smart factories. As a result, it will lead to the original goal of the smart factory, which is to improve productivity.

SECURITY ISSUES AND IMPLEMENTATION CHALLENGES

Recently, manufacturers have been conducting asset visualizations as a first step towards establishing an appropriate strategy to secure factories. Almost all manufactures, however, face the following security issues and technical challenges after they gain an understanding of their environment and what should be protected within it. (Figure 1)

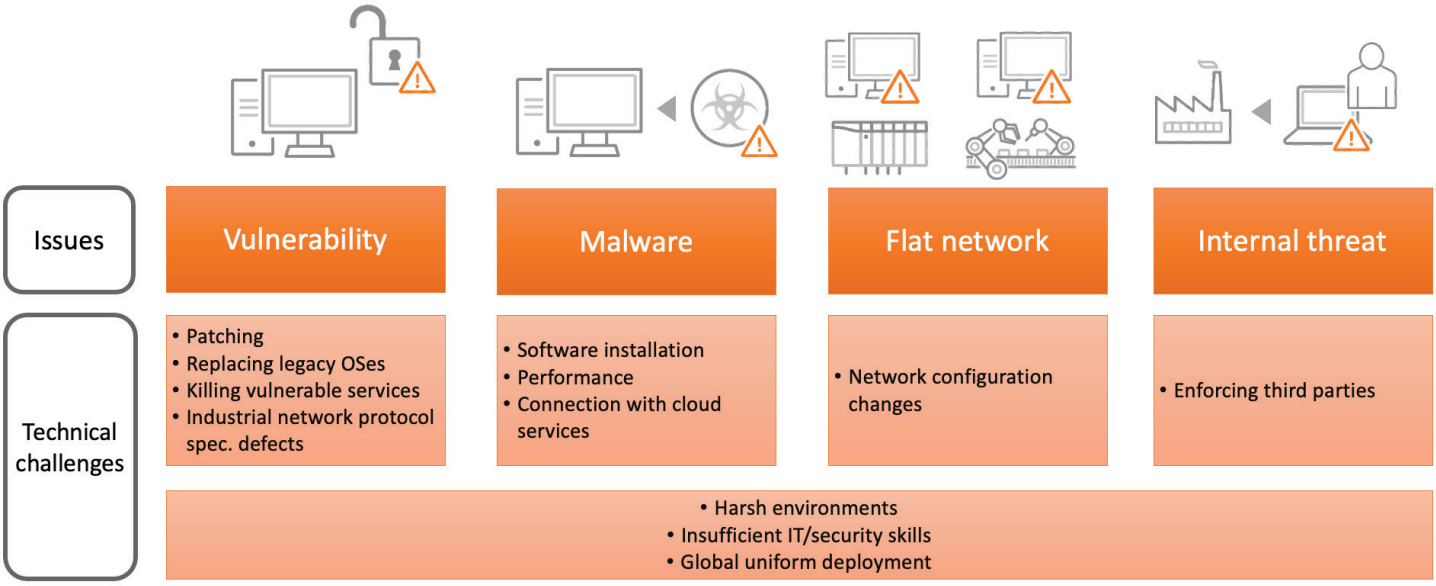

Figure 1 Security issues and challenges commonly seen in factories

Issue 1: Vulnerability

The first security issue is vulnerability. This includes software bugs, legacy OSes, and lack of authentication and authorization in OT protocols. Unlike IT systems, OT prioritizes system availability, so in general, security patches are not applied, and field engineering teams tend to keep using legacy OSes. Mission-critical devices such as programmable logic controllers (PLC) accept any order, no matter where it comes from, because of how an OT system has been developed. However, it's very difficult for field engineering teams to resolve those issues due to its environmental characteristics.

Firstly, patching is very difficult because there is a risk that business application running on the target facility may not run properly due to software confliction after patching. So, facility providers or vendors do not allow asset owners to install security patches into the system. Even if patching is allowed, it takes a long time to complete it since it is not easy for asset owners to halt a 24/7 running factory. Furthermore, almost all maintenance period time is reserved for system maintenance, leaving little room for security deployment.

Secondly, replacing legacy OSes is difficult. Because facility providers or vendors request that asset owners not just replace legacy OS only, but replace the overall system. From a vendor's perspective, the replacement of legacy OS brings huge workload issues for them just to guarantee system availability after replacement. That's why they request that the asset owner fully replace the system. For those who cannot apply security patches and cannot replace legacy OSes, there are few options. One is to kill vulnerable services used in a factory—SMB v1 being one of the options. But unfortunately, it's also difficult for them to do this because killing important services may impact existing standard operating procedure (SOP) and system availability.

Lastly, resolving authentication and authorization issues also remains difficult due to defects in protocol level specifications.

Issue 2: Malware protection

The second security issue is malware. In general, deploying generic anti-malware protection into some devices such as human-machine interface (HMI) and other mission-critical devices cause issues for field engineering teams because of system availability. Like a vulnerability issue case, the facility provider or vendor does not allow asset owners to install any kind of software into the system, this is to avoid software conflict with business application running on the target system. Even if a vendor allows asset owners to install software, performance issues can arise. Generic blocklist-based anti-malware software requires malware scanning and usually impacts system performance, making it not acceptable for asset owners to install it into mission-critical devices from a system availability perspective.

Alternately, there are some devices on which we can install malware protection (i.e., Engineering Workstation (EWS)). An EWS is used for the development of a program and to write it to PLC during maintenance phase. For that reason, EWS is not a mission-critical device. In this case, asset owners are able to install anti-malware software. However, there are several concerns to consider in the case of new factories. Recently, on the EWS, field engineers use the system vendor's application store to download productivity enhancing apps, connects to cloud services to enable Digital Twin, and also download third-party source code to accelerate their software development. Unfortunately, those "cloud service-connected environments" can introduce new attack vectors and vulnerabilities. So, asset owners need to protect EWS by installing anti-malware software, but also, they need to manage network access of EWS on the premise that some compromise will happen.

Issue 3: Flat network

The third security issue is flat network. It's very easy for a threat to compromise an entire system because of the number of vulnerable devices available in a factory. So, if a worm infects one device, it can easily move laterally, making the incident scale bigger with massive loss at risk.

A solution to this issue is network segmentation. It's easy for a new factory to do it, however, it's difficult to do it from a system availability perspective in the case of an existing factory. Because deploying network segmentation requires configuration setting changes in existing networks, it may impact system availability. Furthermore, even though it is acceptable to deploy it, it is a time-consuming task for them to prepare a network connection map for proper settings, to change settings, and to verify network segmentation across the entire system. However, unfortunately, some business applications have hard-coded IP addresses in its program. Because of this, it's very difficult for them to change it, especially for old system of which a vendor no longer exists.

Issue 4: Internal threat

The last security issue is internal threats, especially for outside laptops and machines brought into a factory by third-party maintenance engineers. Maintenance engineers often plug their laptop to a factory network which can become a threat's entry point. Asset owners are able to ask third parties to install necessary security measures into laptops brought into a factory, however, there is no way for asset owners to make sure all laptops are protected properly.

Asset owners have challenges when resolving those security issues. The first being harsh environments. For example, when asset owners try to resolve a vulnerability by using security appliances, it must run properly under high temperature environments and must be attached with an industry specific mount system, which is called DIN rail mount, since those devices are usually placed in the cabinet at a shop floor. So those environment characteristics should be addressed.

The second challenge is insufficient IT and security skill sets of stakeholders. In general, a portion of security operations should be conducted by engineers. But unfortunately, their IT and security skills are limited, highlighting the importance in installing easy-to-operate and/or easy-to-manage security rules.

Lastly, global uniform deployment is also crucial. Very large manufacturers have 50 to 100+ factories worldwide. If they deploy a different vendor's security for each factory, it can bring major operation problems due to the fact that it requires a lot of time to evaluate each product and to create an SOP for each factory and is quite unproductive. Thus, whether or not asset owners can deploy identical solutions globally and deploy single SOPs is very important. Additionally, CISO and security operation teams have a concern about multiple consoles that need to be monitored and the massive alerts they receive every day. So how can they reduce the number of consoles and distinguish the most important alerts among them are very important.

“KEEP OPERATIONS RUNNING” DEFENSE STRATEGIES

As mentioned above, security issues need to be addressed in order to overcome cyber risks. To “keep operations running”, Trend Micro proposes a three-step approach that consists of prevention, detection, and resilience.

1st step: Prevention

In this step, we aim at reducing the threat intrusion risk as much as possible at data exchange points like network and DMZ between IT and OT, USB storage used in a factory, laptops/machines brought into a factory by third parties during maintenance, IoT gateway, engineering workstations connected to the cloud, and private mobile networks. We offer several solutions to make sure these data exchanges remain safe.

2nd step: Detection

Secondly, we detect threat activities in OT environments on the premise that there is no such thing as 100% “prevention”. Anomaly network behaviors such like command and control (C&C) communication and multiple log-in failures in short periods of time should be detected as soon as possible to prevent massive damage. We offer passive detection solutions which is connected to mirror port of L2 SWITCH/L3 SWITCH in DMZ and/or the shop floor so that asset owners can detect anomaly situations at early stage of the cyberattack without impacting system availability.

3rd step: Resilience

The last step is to protect the most critical environments on a shop floor and to minimize any affected areas. On a shop floor, there are a lot of critical assets which directly link to production and its control. To protect those environments from cyberattacks, which may get through prevention and detection layers, we offer solutions for industrial network security and industrial endpoint security which are developed as a purpose-built solution to handle OT environment issues like high temperatures, the need for easy-to-use systems, and the need for minimal performance impact.

TREND MICRO’S PRACTICAL SOLUTIONS TO “KEEP OPERATIONS RUNNING”

As shown in Figure 2, Trend Micro offers comprehensive total security solutions for smart factories which covers level-1 to level-5 of the Purdue Reference Architecture Model with OT-centric solutions, ICT-centric solutions, IT-centric solutions, a purpose-built threat defense platform (Trend Micro Vision One™), and professional services.

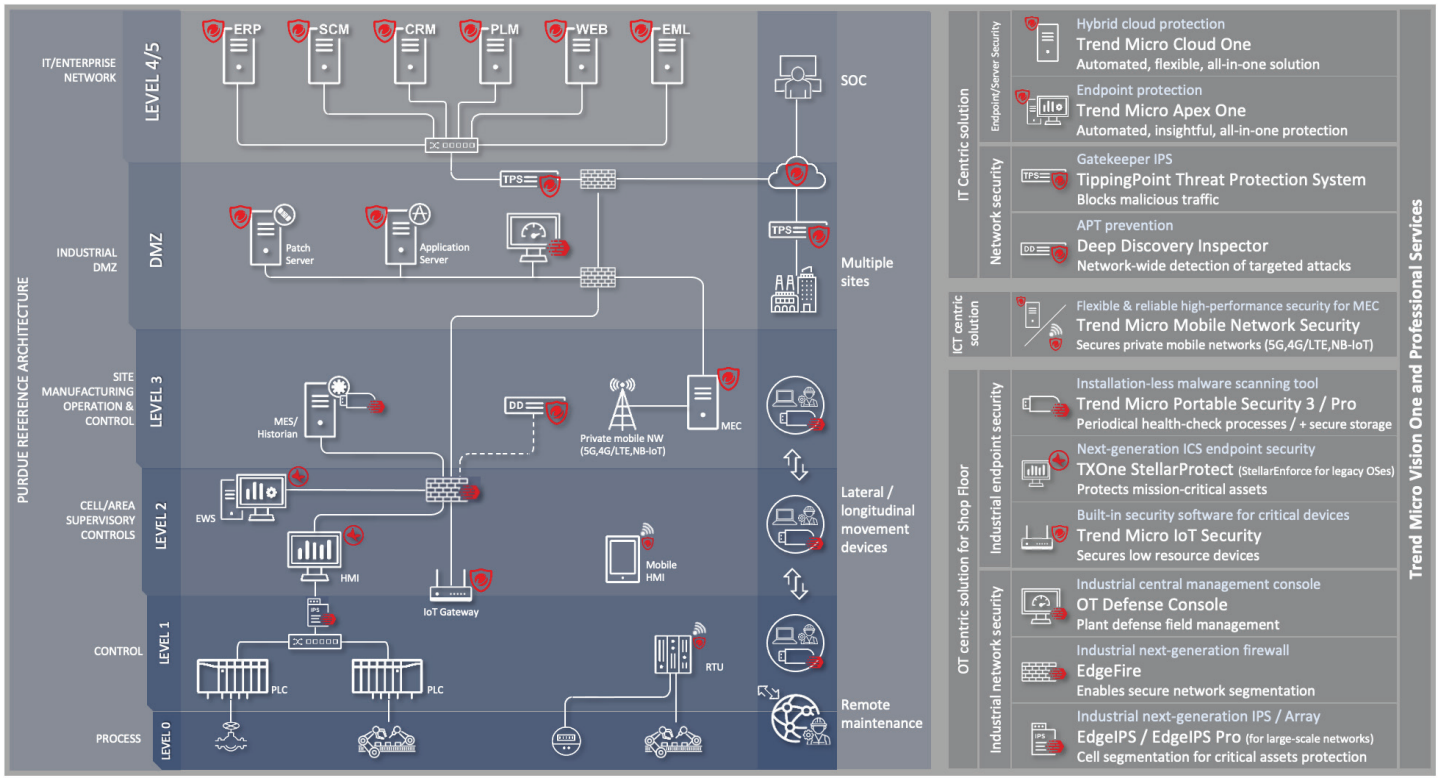

Figure 2 Total security solutions for smart factories

OT-centric solutions, in other words—purpose-built solutions—includes industrial endpoint security and industrial network security. ICT-centric solutions offer security for private mobile networks such as local 5G in a factory. IT-centric solutions offer network security, endpoint/sever security, and cloud security. A purpose-built threat defense platform brings a single view console for advanced alert detection and automatic responses. Our professional services, such as incident response, fully supports and improves asset owner’s security posture to “keep operations running.”

From here, let’s look at specific measures for each environment.

Best practices for existing factories: Protect without affecting availability

An asset owner's major concern is how to secure their existing factory. Figure 3 represents a protection approach overview for existing factories. In the prevention part, there are mainly four types of data exchange points. In the detection part, passive network monitoring is needed to detect anomalous situations in OT network. And in the resilience part, critical assets and its operation should be secured.

In case of existing factories, the engineering workstation (EWS) is not connected with the cloud and private mobile networks are not available. Therefore, we do not mention EWS and private mobile networks in this case.

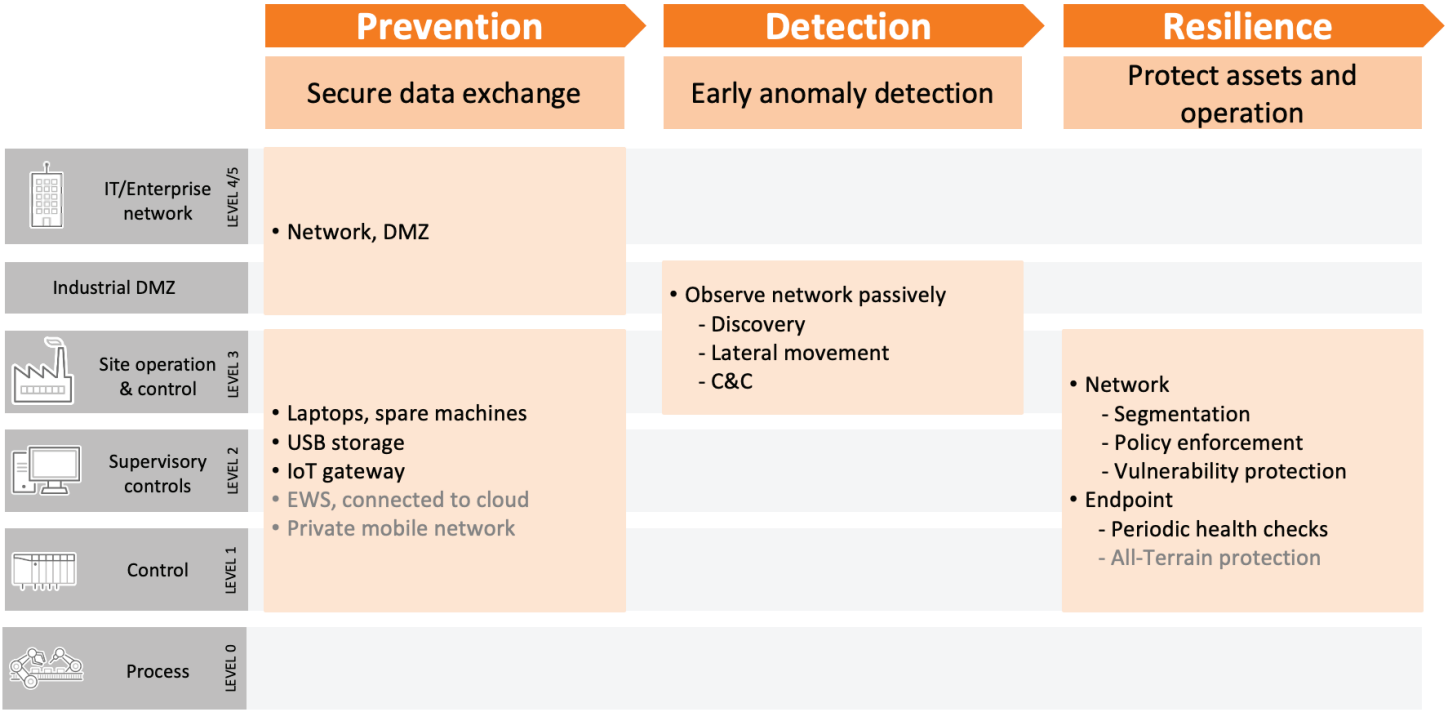

Figure 3 Approach overview for existing factories

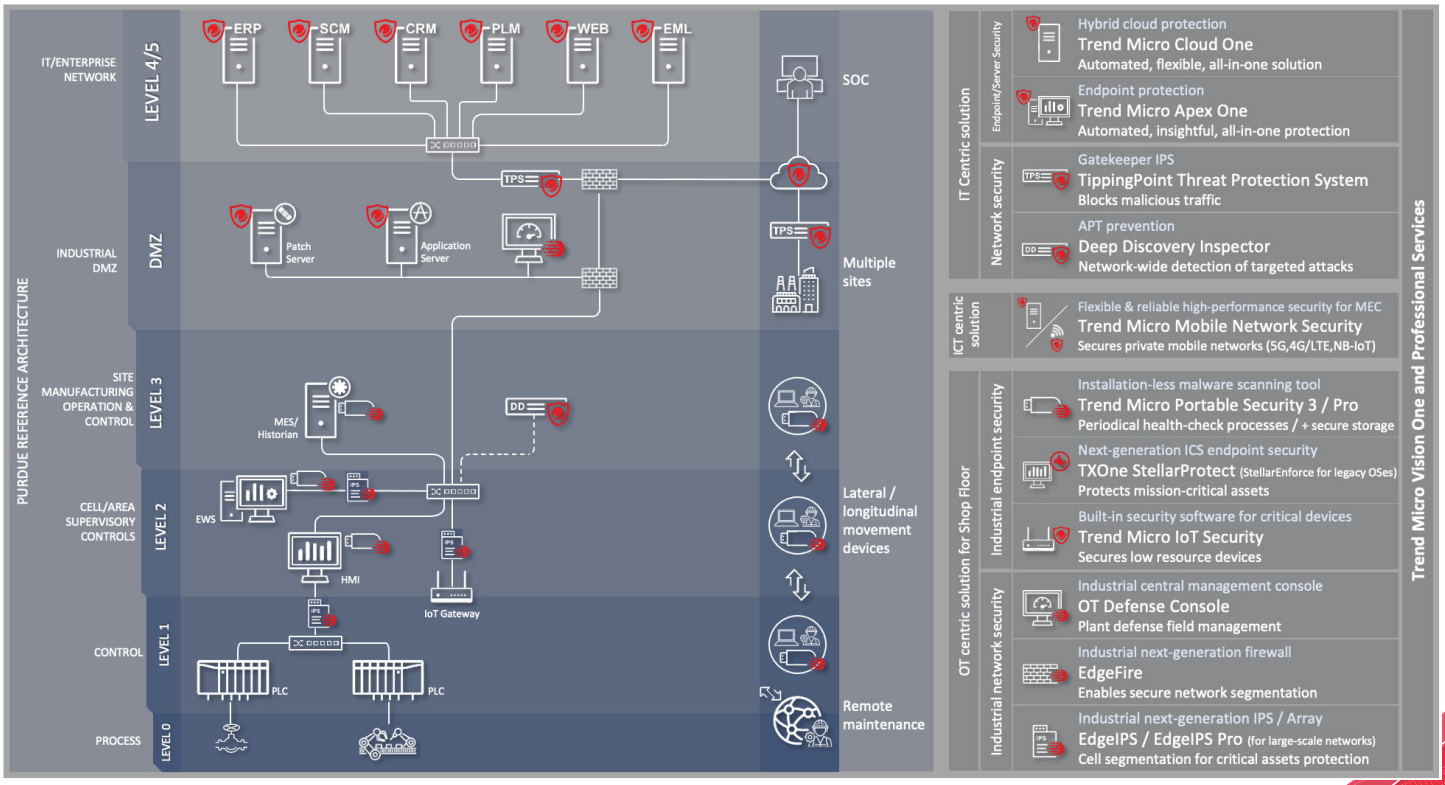

Figure 4 Deployment example for existing factories

Based on this approach, asset owners can deploy the right security solutions at right place. (Figure 4)

The first step is prevention at four data exchange points.

Network and DMZ

Almost all asset owners have already deployed a firewall between IT and OT networks. It enables sufficient access control; however, it cannot prevent vulnerability attacks such as WannaCry ransomware. To protect OT networks from vulnerability attacks, asset owners can use Trend Micro™ TippingPoint™ Threat Protection System for perimeter protection. Furthermore, there are several servers in DMZ for data and file exchange, and those are permitted to install software so asset owners can utilize Trend Micro Cloud One™ for sever protection. Trend Micro also protects cloud platforms and severs in level 4/5 layers.

Outside laptops and machines

Third-party engineers often bring their outside laptop and machines to maintain asset owner's facilities. The best way to make sure it is safe is to impose engineers to install anti-malware protection into the laptop. However, there is no guarantee that they will fully follow this rule. Furthermore, regarding outside machines, it's difficult to install additional security software because environmental changes may bring system availability issues. For those, asset owners can use Trend Micro Portable Security™ 3 as an installation-less malware scanning tool to make sure all outside laptops and machines are safe at factory gates.

USB storage

Third-party engineers sometimes use USB storages to exchange data. For those cases, asset owners can utilize Trend Micro Apex One™ endpoint protection to make sure USB contents are safe prior to use.

If field engineers need to consecutively use a USB storage to collect or move data from one terminal to another on a shop floor, Trend Micro Portable Security™ 3 Pro Edition's secure storage functions can provide increased security and operational excellence. This is due to all files stored in secure storage being scanned and encrypted in real time via its AES-256 encryption engine.

IoT gateway

Some asset owners have already integrated an IoT gateway to enable remote monitoring or similar services. In this case, since attackers may enter OT networks via IoT gateways, asset owners can place EdgeIPS™ in front of IoT gateways as a transparent network device to enable policy enforcement and vulnerability protection without impacting system availability.

Second step is detection.

To detect anomaly network behaviors such like C&C communication and multiple login failures in a short period of time, asset owners can use Trend Micro™ Deep Discovery™ Inspector as a passive monitoring network appliance. It can detect anomaly network behaviors without impacting availability at level 3/DMZ4/5 since it does not require inline deployment but rather connects with a mirror port of network switches.

Last step is resilience.

The most important thing is to "keep operations running" even when threats invade the production line between layers level 1, 2, and 3. In this layer, asset owners can use two types of solution, industrial network security and industrial endpoint security. At the shop floor, we often see flat networks, vulnerabilities, and insufficient authentication and authorization. To resolve those issues, asset owners are able to use EdgeIPS as a transparent industrial next generation IPS hardware appliance which supports harsh environment and HW bypass in order to implement network segmentation. Deploying EdgeIPS in front of L2 SWITCH uplink side can prevent vulnerability attacks and enforces access policies without changing the network configurations of existing facilities. This allows asset owner to establish secure network segments without impacting system availability. Similarly, it can protect vulnerable critical assets like HMI and PLC from vulnerability attacks and impose granular access controls. For asset owners who need to deploy EdgeIPS into large-scale industrial networks and prefer IT-like operation, we offer EdgeIPS™ Pro, a transparent IPS array with 48/96 ports and IT-rackmount 1U/2U form factor in order to enable easier deployment and processes for network operation teams. In existing systems, the transparency of EdgeIPS is attractive because it can be deployed without changing the network configuration of existing facilities. On the other hand, if asset owners have already deployed the L3 SWITCH to establish network segments, EdgeFire™, an industrial next-generation firewall, may be an option instead of EdgeIPS, due to its more secure network segmentation and support of harsh environments. By replacing existing L3 SWITCH from EdgeFire with virtual patching and policy enforcement capacities, asset owners can establish more secure network segmentation without changing network configuration of existing facilities.

When we look at endpoint or devices in level 1 and 2, it is very difficult for asset owners to additionally install endpoint protection into those devices, instead they can use Portable Security 3 as an installation-less malware scanning tool for periodical health check purposes. Thanks to an LED implemented in the back face of the tool, they can easily use it to scan target devices.

As result, by this approach and solution deployment, asset owners are able to protect their existing factories without impacting availability or heavy OT pushback.

Best practices for new factories: Making security a default

Asset owners are able to implement necessary security into a new factory. In this case, asset owners follow the same approach as existing factories, and furthermore they can apply additional and/or enhanced security as a default to make it more secure. (Figure 5) There are four additional ways to protect their new factory; additional protection for the IoT gateway, additional protection for the EWS connected to the cloud, more secure network segmentation, and additional endpoint protection for mission-critical devices by all-terrain protection. (Figure 6)

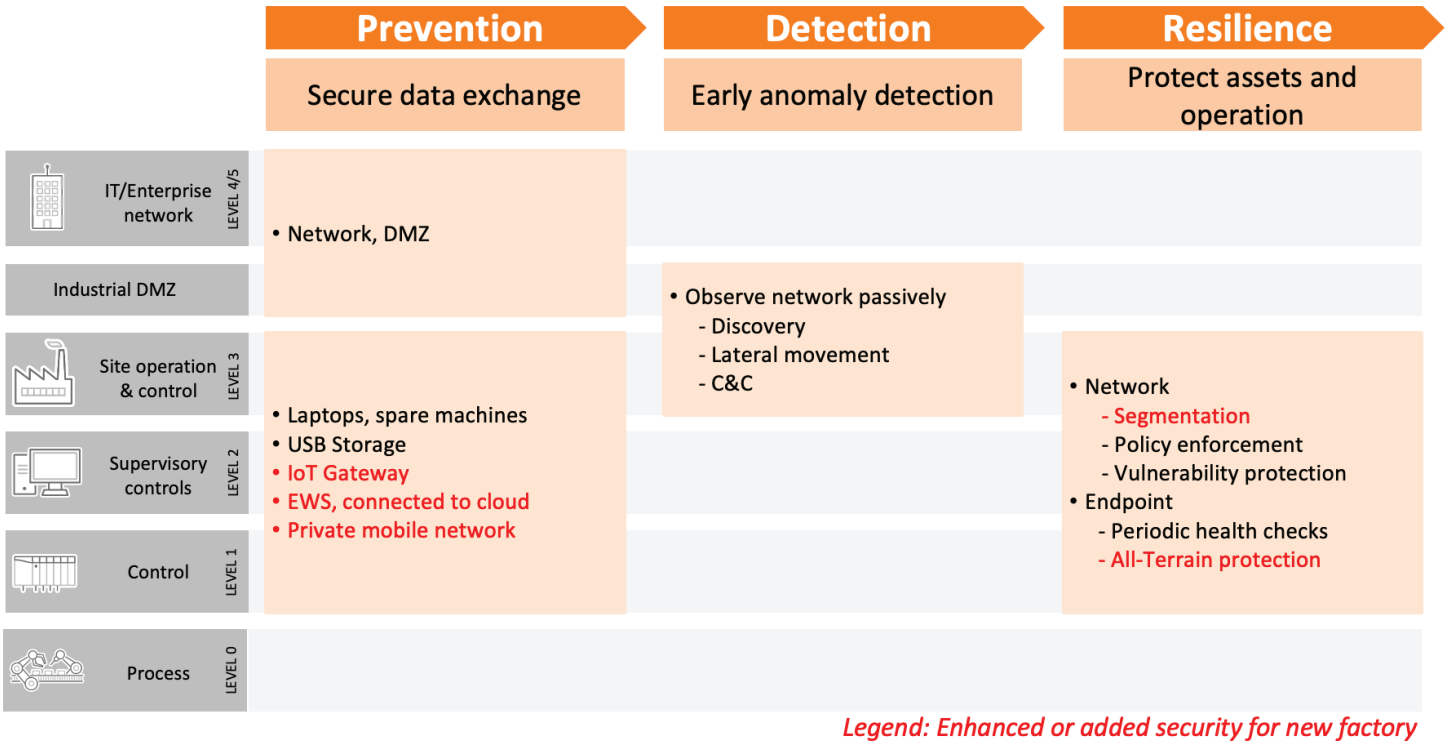

Figure 5 Approach overview for new factories

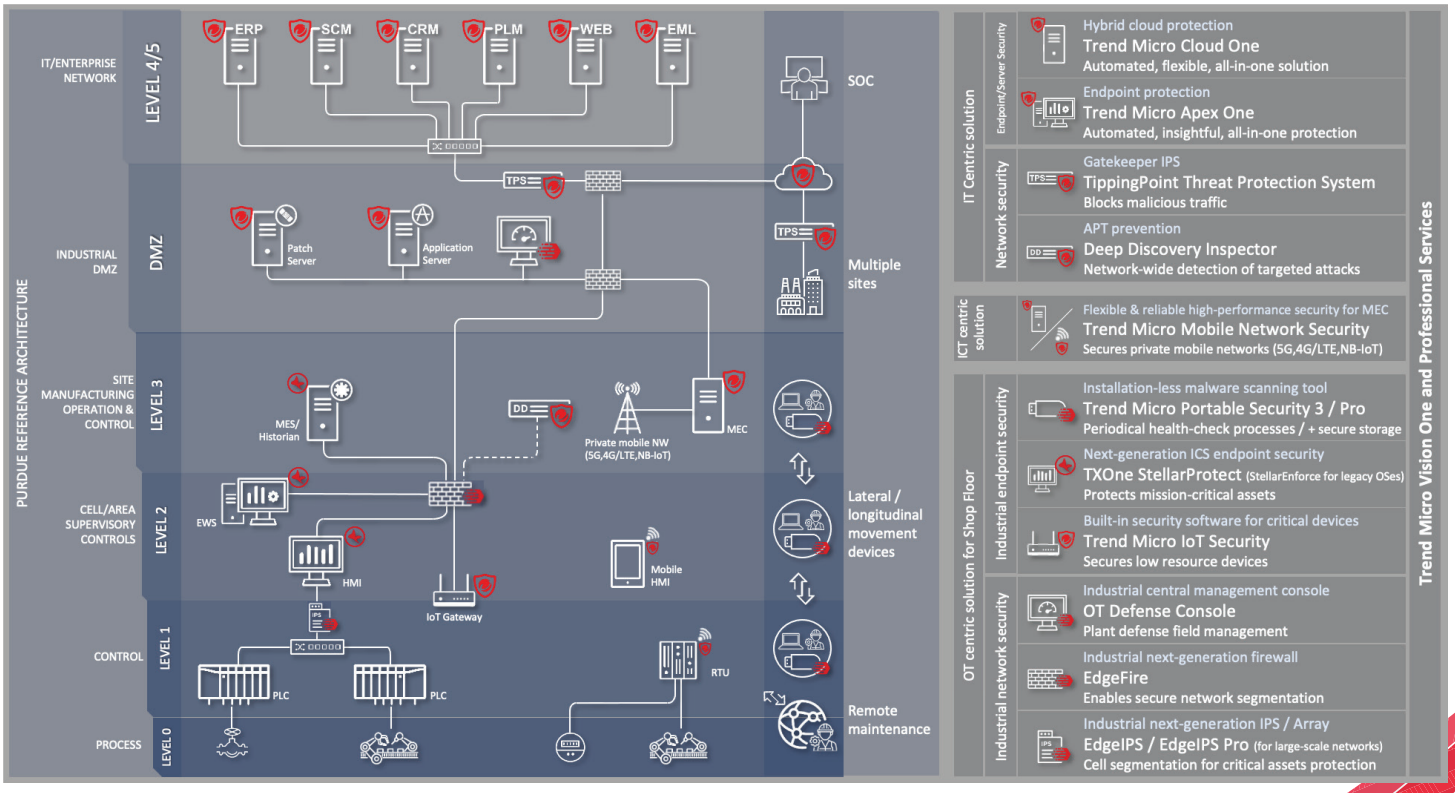

Figure 6 Deployment example for new factories

IoT gateway

To protect IoT gateways or edge devices running on Linux/AndroidTM/Raspberry Pi from cyberattacks, asset owners are able to ask device makers to add Trend Micro™ IoT Security (TMIS)—a built-in security software that monitors and protects critical devices—to implement secure devices as default. Asset owners who develop their own application on Raspberry Pi can utilize TMIS to protect it by themselves as well.

EWS connected to cloud

EWS (which connects to cloud services like the system vendor's app store, Digital Twin, and third-party source codes on Github) asset owners can utilize TXOne StellarProtect, an industrial-grade next-generation ICS endpoint security solution. It delivers patternless protection against both known and unknown malware via machine learning and ICS root of trust, enabling all-terrain protection with less performance impact and operational efficiency. On the premise a compromise may occur in the future, asset owners should deploy policy enforcements—like access control by EdgeIPS or EdgeFire.

Private mobile network

To protect private mobile networks, we offer Trend Micro™ Mobile Network Security to prevent private mobile networks from both lateral and vertical cyberattacks by securing multi-access edge computing (MEC) and mobile edge devices. In addition, Mobile Network Security allows for clear visibility of the entire network's cybersecurity environment.

Mission-critical endpoints

To protect other mission-critical assets like SCADA and HMI, asset owners can utilize TXOne StellarProtect. TXOne StellarEnforce, trust-list based ICS endpoint protection, can be deployed as well while they protect legacy OSes. It does not require malware scanning during operation so it can efficiently protect mission-critical devices without performance issues for both known and unknown malware along with fileless attacks.

L3 SWITCH

To enable more secure network segmentation in order to segregate networks and minimize affected zones when an incident happens, asset owners are able to use EdgeFire—an industrial next-generation firewall—on the shop floor since it supports 10 ports L2 SWITCH with routing/NAT/FW/IPS/protocol filters and harsh environment proof capabilities.

Benefits: Efficiently securing factories with minimal TCO

As a total security solution provider, Trend Micro helps to "keep operations running" with minimal TCO (total cost of ownership) through support during all phases—including prevention, detection, and response—over a long period of time. And thanks to our efficient solutions, there are thousands of customer deployments worldwide.

IT, OT, IoT integrated threat intelligence and solution

Trend Micro utilizes many attack vectors and TTPs (tactics, techniques, and procedures) around IT/OT/IoT and protection points like endpoint/network/server/cloud so that we can integrate the latest threat intelligence and technologies into our solution. Furthermore, insight and intelligence integrated from Trend Micro™ Zero Day Initiative™ (ZDI); the largest vulnerability hunting organization, as well as Trend Micro Research; which looks at future threats to make our solutions more efficient.

The Trend Micro Research team actively conducts research to improve the security of the OT and IoT area (i.e., research using a honeypot to observe actual cyberattacks on smart factories). Trend Micro Research also conducts explorations on uncovering vulnerabilities in notable technologies such as industrial robots, SDR (software-defined radio), MQTT, and CoAP, and their attack feasibility. Through such investigation, Trend Micro Research has been accumulating information on OT environments.

ZDI feeds information to Trend Micro Research, publicly disclosed the most verified vulnerabilities of 11 vendors in 2020 (60% of the global total of 1,378)[1]. In addition, ZDI's "Pwn2Own™" hacking competition has been uncovering vulnerabilities and providing survey results to vendors since 2007. In the 2020 contest, ZDI took on ICSs (industrial control system) to try to strengthen the security of the ICS/OT associated platform.

On top of that, our connected products and Trend Micro Vision One platform brings more precise alert detection and automatic responses as well as huge benefits for CISO and security operation teams looking to offload overworked and overstretched IT teams and operation costs.

Single vendor, global support

When incidents happen, unified support is very efficient for a quick response to minimize downtime. In the case of multi-vendor solution deployments, an asset owner needs to communicate with a number of vendors in order to properly contain or respond to incidents, needs excess time to handle the situation or to transfer important information among different vendors, causing extended downtime. Asset owners can otherwise deploy a single solution, utilize a single SOP worldwide, and quickly respond when incident happens, giving them more stable operations and minimal TCO.

Sustainability

From an availability perspective, the stability of a solution provider is very important. Trend Micro, as a trusted global company, has been in business for over 30 years with a strong financial base and fully commits to securing customers in both private and public sectors.

1 Quantifying the Public Vulnerability Market: 2021 Edition, Omdia Research

CONCLUSION

As more smart factories face cybersecurity risks, causing production stoppage and revenue loss, a security solution which combines IT and OT is needed more than ever. However, it's not feasible to efficiently and effectively "keep operations running" by just deploying IT-centric security solutions within a factory, deploying detection solutions—which just increases operation costs—or by deploying different vendor security solutions.

To resolve security issues and implementation challenges, Trend Micro offers total security solutions for factories which can efficiently achieve stable operations with minimal TCO for long period of time. In particular, Trend Micro realizes this by offering a combination of IT-centric solutions and OT-centric solutions based on a three-step approach; "prevention", "detection", and "resilience", to accurately detect sophisticated attacks and respond quickly, and offers sufficient customer support when security incidents do happen. Furthermore, our solutions—which do not impact system availability—minimizes the downtime of the production within existing factories. In the case of new factories, we can increase security with advanced preventative solutions. Thanks to these comprehensive solutions and approaches, there are over 1,000 customers efficiently securing their factories globally.

TREND MICRO INC.
U.S. toll free: +1 800.228.5651
phone: +1 408.257.1500
fax: +1 408.257.2003