A Trend Micro Technical Report | **December 2021**

ICS/OT Security for the Electric Utilities Industry

» Situational awareness across OT, IT, and CT

OVERVIEW

Trend Micro provides visibility into cybersecurity risks and threats in the electric utilities industry. This combines IT (information technology), OT (operational technology), and CT (communication technology) and enhances detection and response capabilities to ensure critical infrastructure resiliency. Operations in the electric utilities industry are supported by a mix of legacy and modern systems. Our unified cybersecurity platform across OT, IT and CT for protection, detection, and response in complex environments solves security teams challenges stemming from organizational silos and alert fatigue with minimal total cost of ownership (TCO) for security operations.

BACKGROUND

The risk of security incidents is rapidly increasing in the electric industry, which plays a crucial role in critical infrastructure. This is due to the increasing vulnerability of the system caused by the modernization of the electricity generation, transmission, and distribution systems (i.e. digitalization, network connectivity, and the use of generic software and IT). There is also a growing threat of state-sponsored attacks. For example, in 2015, a cyberattack in Ukraine caused a power outage that severely affected many of its citizens.[1]

This has led to a review and strengthening of cybersecurity regulations and guidelines throughout the power industry in recent years. For example, in April 2021, the U.S. Department of Energy (DoE)/Cybersecurity and Infrastructure Security Agency (CISA) developed a 100-day plan to improve visibility, detection, and response capabilities in industrial control system (ICS) environments.[2] [3] This includes improving detection, mitigation, and investigation capabilities, developing specific 100-day milestones to identify and deploy technologies (to enable virtual real-time situational awareness and response), strengthening the security posture of critical infrastructure IT systems, and a voluntary industry initiative to deploy technology to increase visibility of cyber threats in ICS/OT environments.

Furthermore, the White House issued the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems in July.[4] The following September, The Cybersecurity and Infrastructure Security Agency (CISA) and National Institute of Standards and Technology (NIST) issued certain performance goals as cybersecurity baselines for each sector.[5] This encouraged asset owners and operators in each industry to review their systems and organizations in order to meet these goals.

However, these directives are not unique to the United States. In Europe, the Critical Entities Resilience (CER) mandate will be expanded to the NIS Directive 2.0. Revised in December 2020, the NIS Directive 2.0 strives to improve resiliency of critical infrastructure in both physical and cyber spheres.[6] In addition, the Japanese government has been discussing their next cybersecurity strategies, which will include the protection of critical infrastructure.[7]

ICS/OT security has a unique history that differs from IT security, but the current and future ICS/OT environment utilizes IT; such as the cloud, CT, and private 5G. This defines ICS/OT environments as a mixture of modern and legacy systems. It is time for asset owners and operators in the electric industry to reassess their risks and update their cybersecurity strategies from this latest perspective.

CHALLENGES AND SOLUTIONS

Trend Micro provides advanced solutions to ensure critical infrastructure reliability and resilience by gaining situational awareness across OT, IT, and CT.

1 Feb 2016, Cyber-Attack Against Ukrainian Critical Infrastructure
2 Apr 2021, Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats
3 May 2021, Securing the United States Bulk-Power System
4 Jul 2021, National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems
5 Sep 2021, Critical Infrastructure Control Systems Cybersecurity Performance Goals and Objectives
6 Dec 2020, Revised Directive on Security of Network and Information Systems (NIS2)
7 Sep 2021, Draft of the Next Cybersecurity Strategy of Japan

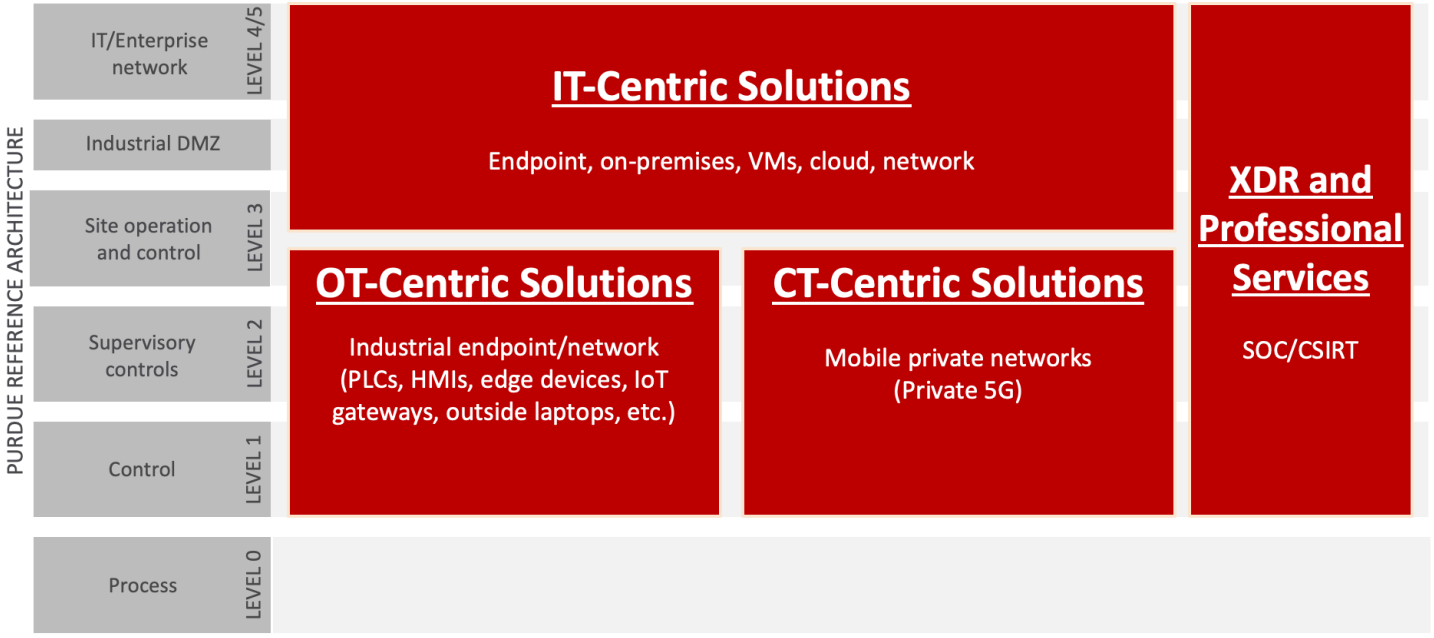
Unified platform for OT with IT and CT	Risk and threat visibility	Protects legacy and modern systems
Delivers global purpose-built OT, CT (5G), IT, and extended detection and response (XDR) security solutions and professional services for the prevention, detection, and resilience of critical operations.	Interconnected solutions send data to security platform. This enables complete visibility that delivers risk insights, detect threats faster, investigates more thoroughly, and responds better across the entire environment.	This includes programmable logic controllers (PLCs), human machine interfaces (HMIs), robots, legacy and modern OSes, edge devices, hybrid cloud environments, industrial networks, and private 5G networks.

Three Different Technologies and One Platform

The current system of electric utilities is an environment in which different technologies; OT, IT, and CT, are combined to supports businesses. Trend Micro improves your security posture and situational awareness with OT, IT, CT, as well as XDR solutions that manage them in an integrated manner.

1. **IT**: This refers to not just enterprise IT, but systems located within the demilitarized zone (DMZ) bordering the station, as well as any remote access that requires IT technology. Our IT-centric solution protects office endpoints, physical, virtual, and cloud server workloads, containers, serverless environments, and networks.
2. **OT**: This refers to power generation systems as well as electric power transmission and distribution systems. These systems are monitored by supervisory control and data acquisition (SCADA)/HMI and controlled by distributed control systems (DCS), programmable logic controllers (PLC), and remote terminal units (RTU). This requires OT-centric solutions that are suitable for industrial endpoints and networks.
3. **CT**: Cellular networks such as 5G are beginning to be used in the station or bay systems through a hybrid deployment of public and private. This requires adaptive mobile security solutions for core networks and devices.

> **XDR**: Even if management is siloed in a system that contains technologies with different functions and characteristics, the flow of data and operations is connected, and cross-environmental attacks are possible. It is important for the security operations center (SOC) and computer security incident response teams (CSIRT) to identify risks and gain visibility for context-based detection and response across the entire environment.



Six Protected Areas

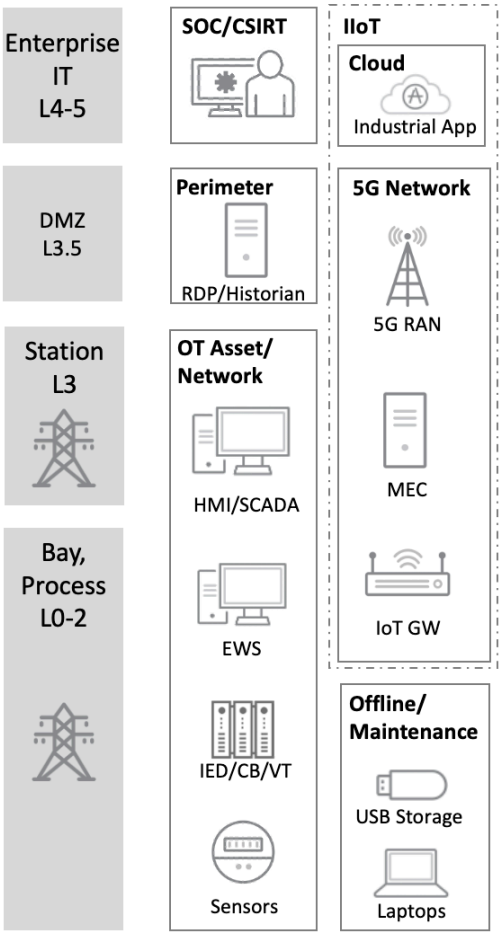
There are six areas to protect in electric utility environments. We help you solve specific security challenges in each area.

1. **OT and IT perimeter**: Establish a boundary of defense between the corporate network and the factory base, or between the office area and the field area.
2. **OT assets**: Protect industrial endpoints that are unable to patch or install security software.
3. **OT network**: Receive network security adapted to the industrial protocols used in field networks.
4. **Offline operations**: Secure removable media and outside terminals brought in during maintenance.
5. **Industrial Internet of things (IIoT)**: Secure the use of new technologies such as industrial clouds, private 5G, and internet of things (IoT) sensors.
6. **SOC/CSIRT**: Gain integrated monitoring of the entire environment to streamline threat detection and incident responses.

Challenges	Solutions
OT and IT Perimeter	
Preventing malware infection on servers in the internal DMZ.	**Trend Micro Cloud One™ – Workload Security** All-in-one hybrid cloud protection without compromising performance.
Preventing vulnerability attacks from the IT to the OT environment.	**Trend Micro™ TippingPoint™ Threat Protection System** Inline deployment between OT and IT networks to prevent vulnerability attacks at wire speed.
OT Assets	
Protecting legacy devices/OSes without impacting system performance.	**TXOne StellarEnforce™** Protects legacy devices by system lockdown or application control.
Protecting software-installation prohibited devices or recovering infected devices.	**Trend Micro Portable Security™ 3** Provides malware scanning and cleanup on the device without software installation.
Preventing critical assets from vulnerability attacks without impacting system availability in the existing environment.	**EdgeIPS™ or EdgeIPS™ Pro (for large industrial networks)** Transparent network security for critical assets, enables a firewall, protocol filter, and intrusion prevention system (IPS) to protect against vulnerabilities without changing logical network configurations.
OT Networks	
Segregating flat networks without impacting system availability in an existing environment.	**EdgeIPS or EdgeIPS Pro (for large industrial networks)** Transparent network security for the uplink port of existing L2 switches, enables a firewall and protocol filter without changing logical network configurations.
Building secure network segments by default.	**EdgeFire™** Ensures network segments by network address translation (NAT), firewall, protocol filter, and IPS functions.
Low visibility and identification of IT/OT network protocols on a shop floor.	**EdgeIPS or EdgeIPS Pro (for large industrial networks)** Deep packet inspection improves situational awareness by inline deployment or passive monitoring.
Anomaly behaviors in level-3 to level-5 networks.	**Trend Micro™ Deep Discovery™ Inspector** Detects anomaly behaviors by connecting it with a mirror port of network switches.

Challenges	Solutions
Offline environments	
Malware infection via USB storages brought into the OT environment	**Trend Micro Apex One™ or Trend Micro Portable Security™ 3 Pro Edition** **Trend Micro Apex One**, an all-in-one endpoint security ensures USB contents are safe prior to use when third-party engineers bring USB storages into a factory. **Trend Micro Portable Security 3 Pro Edition**, a secure transporter, offers 64 GB of secure storage for consecutive use of USB storages on a shop floor by scanning and encrypting all files stored.
Ensuring cyber hygiene of outside laptops and machines brought into the OT environment.	**Trend Micro Portable Security™ 3** Scans devices before they are brought into the OT environment without software installation.
IIoT	
Protecting modern devices/OSes without impacting system performance.	**TXOne StellarProtect™** Protects modern devices via ICS purpose-built next generation malware prevention software.
Protecting low resource devices, such as Raspberry Pi and Jetson.	**Trend Micro™ IoT Security™** Build firmware with security modules to protect devices from various threats.
Resolving cloud environment misconfigurations.	**Trend Micro Cloud One™ – Conformity** Monitors and improves your security and compliance posture of the cloud environment and remediates automatically.
Open-source software (OSS) vulnerabilities of in-house applications.	**Trend Micro Cloud One™ – Open Source Security by Snyk** Uncovers open-source vulnerabilities and prioritizes it in your source code repository.
Preventing threat intrusions from IoT gateways on a shop floor.	**EdgeIPS™** Transparent network security for the IoT gateway, preventing unauthorized access and vulnerability attack.
Preventing unauthorized access, malware infection and spread in private 5G networks.	**Trend Micro™ Mobile Network Security™** Prevents illegitimate device attachment and vulnerability attacks, and recognizes malicious content and suspicious network behaviors at the data network.
SOC/CSIRT	
Alert fatigue caused by disconnected point solutions.	**Trend Micro Vision One™** Collects and correlates deep activity data across multiple vectors, enabling security teams to detect faster, investigate more thoroughly, and respond more efficiently.

Solution Map for Electric Utilities Transmission Substation Systems



SOC/CSIRT

- Trend Micro Vision One

IIoT

- Trend Micro Cloud One – Conformity
- Trend Micro Cloud One – Open Source Security by Snyk
- Trend Micro Mobile Network Security
- EdgeIPS
- TXOne StellarProtect
- Trend Micro IoT Security

IT and OT Perimeter

- Trend Micro Cloud One – Workload Security
- Trend Micro TippingPoint Threat Protection System

OT Network

- Trend Micro Deep Discovery Inspector
- EdgeIPS / Pro
- EdgeFire

OT Asset

- TXOne StellarEnforce
- TXOne StellarProtect
- Trend Micro Portable Security 3

Offline

- Trend Micro Apex One
- Trend Micro Portable Security 3 / Pro Edition

BENEFITS

Minimizes downtime and safety risks

The solutions based on prevention, detection, and response as well as Trend Micro Vision One™ XDR capabilities help protect critical operations from attacks. This is done by detecting threats at early stages, recovering rapidly from an incident, and enabling preventative measures. In addition, Trend Micro Vision One risk insights are interconnected with each layer of security, promoting efficient and effective risk management by visualizing vulnerabilities and its priorities. This helps minimize downtime and safety risks.

Improves operational excellence with minimal TCO

Our unified platform improves operational efficiencies and eliminates prolonged incident response and capital inefficiencies caused by duplicate support contracts and inconsistent standard operating procedures (SOPs) due to multi-vendor control. This contributes to improved operational excellence with minimal TCO.

Compliance and accountability

Asset owners are given the tools to comply with industry standards such as NIST Cybersecurity Framework and IEC 62443, along with regulations such as NERC CIP and NIS Directive. Trend Micro Vision One extends detection and response across every security layer for visibility into vulnerabilities and other risks across the entire corporate environment, as well as critical security events and attack flows. This provides greater visibility of the environment to stakeholders.

WHY TREND MICRO

As a unified cybersecurity platform provider, Trend Micro helps to "keep operations running" with minimal TCO by providing ongoing support throughout every phase—prevention, detection, and response. And thanks to our efficient solutions, there are thousands of customer deployments worldwide.

IT-, OT-, and CT-integrated threat intelligence and solutions

Trend Micro focuses on the many attack vectors and TTPs (tactics, techniques, and procedures) around IT/OT/CT so that we can integrate the latest threat intelligence and technologies into our solution. We leverage the insight and intelligence gathered from our Trend Micro™ Zero Day Initiative™ (the world's largest bug bounty operation), ICS-/OT-centric technology, and intelligence from TXOne (a company formed by a joint venture between Trend Micro and Moxa), and Trend Micro™ Research (which looks at future threats to make our solutions more efficient).

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

Single vendor, global support

In the case of multi-vendor solution deployments, an asset owner needs to communicate with several vendors to properly contain or respond to incidents and needs excess time to handle the situation or to transfer important information among different vendors. This causes extended downtime.

When incidents happen, Trend Micro provides unified support immediately to minimize 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 with 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 is fully committed to securing customers in both private and public sectors.

For more information on our intelligence and ICS/OT security solutions, please visit:

https://www.trendmicro.com/en_us/research.html?category=trend-micro-research:environments/smart-factories

https://www.trendmicro.com/en_us/business/solutions/iot/ics-ot.html

TREND MICRO™

Securing Your Connected World

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, our cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. With 7,000 employees across 65 countries, and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com

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