Trellix

SOLUTION BRIEF

Trellix® for Operational Technology (OT) Security

Why Trellix for OT Security

- Comprehensive security platform backed by industry-validated solutions
- #1 security solution for ATM and POS systems
- 90% of world's utilities secured by Trellix
- 75% of U.S. water systems protected by Trellix
- Decades of partnership with industry-leading ICT/OT vendors

Protect your industrial control systems with the Trellix Security Platform

In recent years, the cyber threat landscape has been marked by a noticeable escalation in the frequency and impact of ransomware. Industrial companies have been specifically targeted, leading to production outages and subsequent financial losses. The increase in ransomware has put the spotlight on the security of industrial control systems (ICS), and led internationally to a push for increased regulation (NIS2 in Europe and NERC-CIP and others in the U.S., for example) and for CISOs to address the security of their operational technology (OT) systems.

In addition to unique threats and regulatory requirements, OT systems place a different emphasis on their approach to security compared to traditional corporate IT environments. Due to the nature of controlling "always on" environments such as critical infrastructure, manufacturing, healthcare, and more, OT systems must often operate with minimal, or almost zero downtime, and focus on availability and safety factors first. These considerations dictate a distinct approach to security in comparison to traditional corporate IT. These unique challenges include:

- **Availability before security:** In 24x7 production environments, any interruptions must be avoided. This applies with regards to availability of maintenance windows, as well to any active detections that could automatically block and therefore interrupt a critical production process (as antivirus software or a network intrusion prevention system may do).
- **Safety over security:** The primary target on a production site is the safety of employees. Anything that relates to securing the actual ICS is typically a secondary consideration.

- **Longer product lifetimes:** In IT, it is relatively common to exchange infrastructure components regularly—perhaps every five years. In OT, however, components or even the whole production infrastructure may have a lifecycle of 10 years or more.
- **Legacy operating systems:** With long product lifetimes, OT environments often involve systems that are considered "legacy," such as Microsoft Windows NT or Windows XP. These systems may not be easily replaced, changed, or even upgraded or migrated to a newer version, as very strong quality controls apply.
- **ICS vendor responsibility:** The vendor that built an ICS must validate components in use, and will also bring specific requirements (for example, remote access to the system). Due to the complex, vendor-mandated portfolio for industrial parts, they must perform extensive testing. As a result, it may take a year or more for vulnerabilities in an ICS to have a patch available.
- **Access to components:** Many production plants and power utilities can be accessed by people who are onsite. However, there are also industries with remote locations, such as offshore wind farms or oil platforms, where access is limited to certain intervals or even weather conditions.

Trellix partners with ICS manufacturers to help them operate their systems in a secure manner. Across the whole portfolio, Trellix offers tailored solutions for industrial environments, with a focus on endpoints as well as network monitoring. These solutions are available fully on-premises, but can also be operated in a hybrid or cloud environment.

Trellix architecture for OT systems

Trellix provides an array of solutions to monitor and protect your OT environment. In conjunction with OT system provider partners, our strategy is to help organizations secure their combined IT and OT enterprises with protection and detection technologies.

Our solutions span intelligence, consulting, and a security platform backed by industry-validated solutions, strategic partnerships, and decades of expertise to help our clients improve maturity, meet compliance goals, assess risks and identify OT specific and cross-over threats.

Control and visibility are provided for lower levels of control systems that prevent OT specific threats, lock down systems to known good images to prevent unauthorized change, detect lateral movement and provide

policy and reporting via a single console. Solutions can operate in air-gapped environments, hybrid and cloud architectures and integrate with other OT vendor monitor and control solutions.

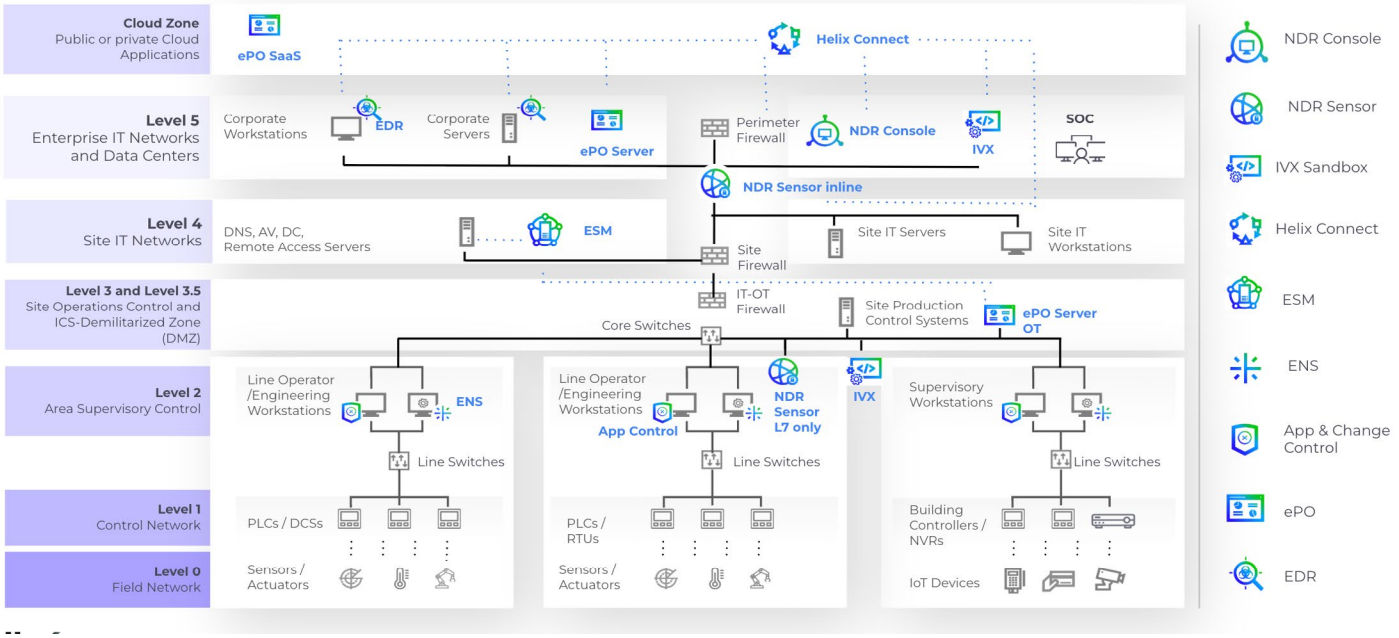

Figure 1: Trellix for Industrial Control Systems Architecture

Trellix solutions for OT

Trellix Asset Visibility for OT

The Trellix Agent proactively discovers unmanaged systems and reports the findings into Trellix ePolicy Orchestrator (ePO). Since control system networks are restricted access, unknown and unmanaged systems may be a security violation. In addition, the Trellix Agent reports on installed software, providing a basic inventory of the managed system. As control systems are managed by the vendor, any unknown software installed could be a safety or security risk. This asset inventory information is also reported into ePO for compliance reporting and configuration monitoring. Finally, through an API, Trellix ePO can export or import other asset information discovered by network security tools like Nozomi, Armis, and Tenable, making ePO ideally suited for both IT and OT asset visibility in control system environments.

The Trellix Agent with SIR extension provides the ability to view installed software on OT systems. Important for software supply chain visibility and compliance requirements, this helps sites prioritize patching and reduce vulnerabilities.

Trellix Endpoint Security for OT

Engineering or operator workstations may be from different ICS vendors and often not managed by a central management system like Active Directory. It is difficult, therefore, to identify these systems, check their status regarding patches or security alerts, and continuously monitor them.

Trellix ePO helps companies achieve central management of machines in the OT environment. Available fully on-premises or as a SaaS solution, ePO can be used to manage the machines and apply specific Windows settings. Its reporting engine also allows administrators to give information about machines in use to the higher level management, to ensure that risk management can be done in an appropriate manner.

The ePO architecture allows both customers and the ICS vendors to check and verify content updates before they are brought into the production environment, therefore adding an extra layer of security when it comes to managing an antivirus solution in critical infrastructures.

Trellix Endpoint Security (ENS) has been certified by many vendors (including ABB, Siemens, Emerson) to be used as antivirus software for ICS. In the ICS context, ENS is a classic Endpoint Protection Platform (EPP), looking for and blocking cyber threats at the moment when they would be executed on an endpoint. In this scenario, ENS adds the minimum layer of security on the endpoint to protect it from known malicious attacks. However, this functionality can be extended to exploit prevention and machine learning modules as well, which is also supported and recommended by some vendors.

As endpoint security becomes an increasing concern in OT environments, customers and vendors may seek to bring endpoint detection and response (EDR) capabilities into critical infrastructures, to be able to respond to incidents faster and extend the capabilities of a traditional antivirus software. Trellix offers on-premises EDR solutions that can be fully offline for environments that require it in addition to a hybrid approaches, for example, where OT is managed from an on-premises ePO server, but IT systems (e.g., user endpoints) are managed from a SaaS ePO.

Trellix Application and Change Control for OT

The most important requirement for OT workstations is that any agents or clients are lightweight and must not interrupt any processes that are vital for the ICS to operate. If certain systems can't be protected by an antivirus solution (because the ICS vendor does not approve, or it is a

legacy operating system), Trellix Application and Change Control can still ensure that potentially malicious applications are not executed, and very important files cannot be changed by anyone (or only by certain people).

With Trellix Application and Change Control, only allowlisted applications can be executed on a system by an authorized user. Any execution of unknown and therefore prohibited executables can be forbidden. If a user would like to execute a certain file, permissions can be granted by the administrators to execute it exceptionally. In a similar fashion, Application and Change Control protects the operating system itself, because users are not allowed to edit or delete any system files. Since those allow lists are, compared to a classic antivirus with regular updates, relatively static, Application and Change Control may have less administrative impact on an organization than maintaining an antivirus solution.

Central management via ePO allows, for example, updater files to deploy updates to critical applications by allowing only a previously verified file. Application and Change Control can even prohibit the use of USB devices in your environment by denying access to the necessary Windows Registry Keys, effectively prohibiting USB keys from being used in the critical environment.

In OT, configuration files that define what production is currently doing are the crown jewels. A malicious attacker could look into changing the configuration files of a PLC, and therefore manipulate the OT process itself and what happens in your production, potentially even causing harm to people working onsite. Application and Change Control protects changes to files by unauthorized users, while allowing your production engineers to adjust files as necessary, ensuring compliance in critical infrastructure. Application and Change Control helps to fulfill the important regulatory requirement of file integrity monitoring (FIM).

Trellix NDR for OT (in partnership with Nozomi Networks)
Legacy operating systems and specialized OT equipment often cannot be directly protected with traditional endpoint security, making continuous network monitoring essential. While micro-segmentation with firewalls provides initial protection by creating smaller industrial cells, firewall technology alone cannot provide complete visibility into network communications or detect threats already inside the perimeter. OT equipment uses proprietary protocols unfamiliar in IT environments, requiring specialized knowledge of ICS operations.

Continuous network monitoring addresses this challenge through a fundamentally different approach than IT environments. Rather

than automatically blocking threats, OT monitoring systems focus on detection and alerting to maintain operational continuity, notifying trained personnel through integrated SIEM/SOC platforms to enable rapid human-driven response.

Network sensors deployed in passive "listening only" mode (SPAN/TAP) analyze traffic to detect cyber threats traversing the network. These threats include classic malware, unauthorized configuration changes to production machines, and rogue devices appearing in what should be a static environment. Real-time alerts enable SOC teams to respond immediately to any anomalies or threat detections that could compromise production operations.

Trellix NDR analyzes network communication patterns to automatically build comprehensive asset inventories, identifying device details such as OS versions, protocols in use, and communication behaviors. This deep visibility into OT infrastructure enables complete risk assessment and management of every device within the network environment. By understanding normal operational patterns, the system can quickly identify new or changed devices that may represent security risks, providing essential baseline documentation for compliance and incident response.

In addition, built-in IVX sandbox technology in the Trellix NDR solution analyzes files traversing the network within isolated real operating system environments, detecting previously unknown threats through behavioral analysis. This capability identifies zero-day malware and sophisticated attacks that traditional signature-based detection methods cannot recognize in OT environments.

Trellix NDR provides unified security across IT and OT environments through a single platform, with particular focus on analyzing IT-to-OT traffic flows—the primary attack vector for most OT system compromises. This convergence eliminates security gaps between operational domains.

Trellix Threat Intelligence for OT

Trellix provides several ways to operationalize threat intelligence to improve both protection of OT systems and IT environments.

Trellix Threat Intelligence Exchange (TIE) acts as a localized reputation service within an OT environment and allows customers to supplement or override reputations provided by Trellix Global Threat Intelligence (GTI). TIE enhances security in OT environments in the following ways:

- Trellix products can automatically block files TIE deems unknown.
- TIE integrates with Trellix sandboxes (IVX, Cloud IVX) to automatically analyze new OT environment files, then allow or block them.
- Customers can import reputations from OT-ISAC, WaterISAC, ONE-ISAC, or other OT threat feeds.
- TIE can store and share third-party reputations via OpenDXL.
- TIE allows customers to override Trellix reputations to prevent custom tools from impacting the OT environment.
- TIE acts as a GTI reputation proxy, allowing restricted internet access to only the TIE server in OT environments without compromising security.
- TIE tracks file prevalence (systems seen, execution locations), aiding in identifying lateral movement or unexpected software spread in OT.
- TIE reputation lookups via Trellix DXL are fast and lightweight, ideal for OT environments.
- TIE integrates with Trellix Private GTI for air-gapped OT environments or networks with strict data sovereignty/ compliance needs.

Trellix GTI is a global reputation database that powers all Trellix products. For closed or secure environments that have limited or no access to the internet, Private GTI can be deployed within the environment to provide security. Private GTI can also be used with TIE for more granular reputation analysis and control.

Trellix Insights enables customers to view, research, and investigate Trellix's vast collection of threat intelligence, including campaigns, actors, tools, malware, and CVEs that may target or affect OT environments. This information can help customers anticipate potential threats and create an effective protection strategy for their IT and OT environments.

Trellix offers threat intelligence reporting and analysis services tailored to OT systems and industry verticals. Trellix's Tailored Intel Reports service is designed to meet the specific intelligence needs of your organization through comprehensive, all-source research and analysis.

To schedule a demo, visit trellix.com.