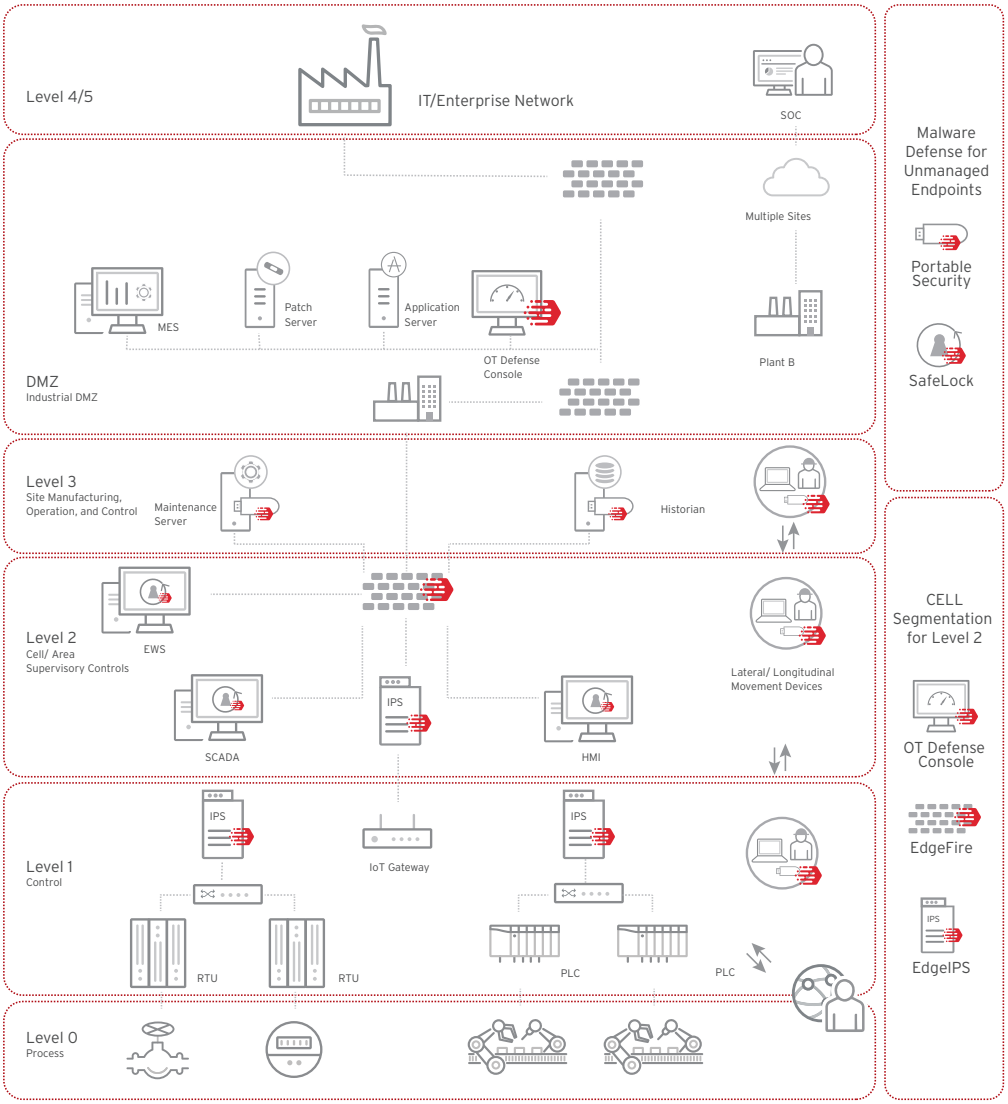
10 INDUSTRIAL IOT SOLUTIONS

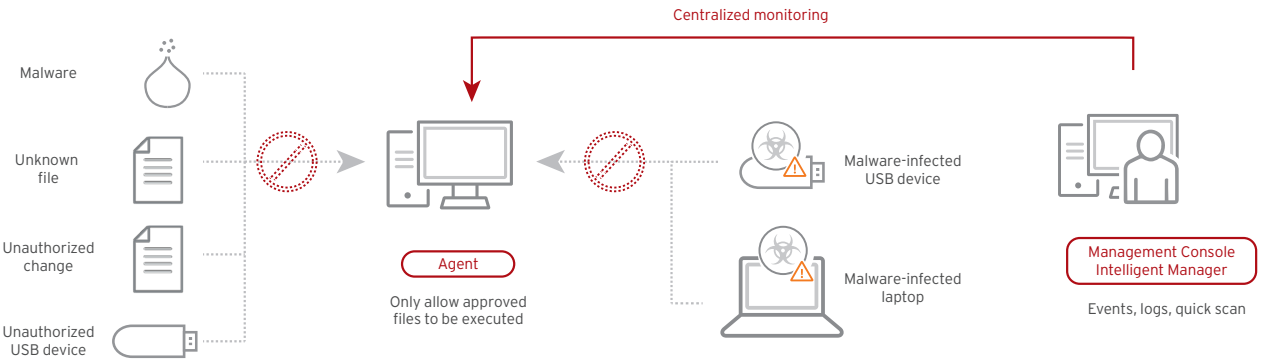
Industrial control systems (ICS) vulnerabilities are easy to exploit and are being attacked in ever-increasing numbers. In addition, many of these ICS systems include out-of-date equipment developed at a time when cybersecurity was not yet a serious issue. Therefore, these devices are particularly vulnerable to modern cyber threats. Installing patches and updates to address vulnerabilities can be very cumbersome. These complex environments span multiple layers, each of which needs to be protected. Traditionally, it remains unclear where the security responsibility for combining these levels lies. In the industrial environment, there are more and more security violations and incidents that could not only lead to operational disruptions, but could even endanger lives.

TXOne Networks

TXOne Networks provide solutions to address security vulnerabilities common in industrial environments. In doing so, TXOne Networks satisfies the needs of both critical infrastructure manufacturers and operators in order to develop the best approach with the greatest practicality. The result is a tailor-made technology that goes beyond conventional safety tools and assess complex challenges. Because ICS environments consist of multiple tiers and includes devices with different operating systems, TXOne Networks provides optimized network and endpoint-based products for real-time protection of OT networks and mission-critical devices.



Trend Micro™ Safe Lock™



Production, healthcare, and energy companies today face a growing number of cyber threats targeting ICS, industrial IoT devices, and embedded devices. Systems that use components of older operating systems are particularly vulnerable. They most likely don't match the current patch state and contain vulnerabilities that attackers can exploit. A lockdown can control the use of system resources and the execution of applications while limiting them to the minimum required for operation. Safe Lock protects against threats by effectively blocking the execution of malware even without signature files.

Benefits

- Minimal impact on performance
- Security solutions for industrial environments
- Easy deployment and maintenance
- Protection of older operating systems
- Security for mission-critical devices

Functions

- Agent application whitelisting
- USB device whitelisting
- Maintenance mode
- Write-protection integrity
- Monitoring protection against fileless attacks
- Protection against exploits
- Management of shared lists
- Pre-scan (malware verification during installation)
- Role-based administration
- Logging

Management Console (Intelligent Manager)

- Central monitoring notification
- Account management quick scan (checks files blocked by agent)
- Root-cause analysis
- Syslog forwarding
- Central management of trusted applications

Trend Micro™ Portable Security™ 3

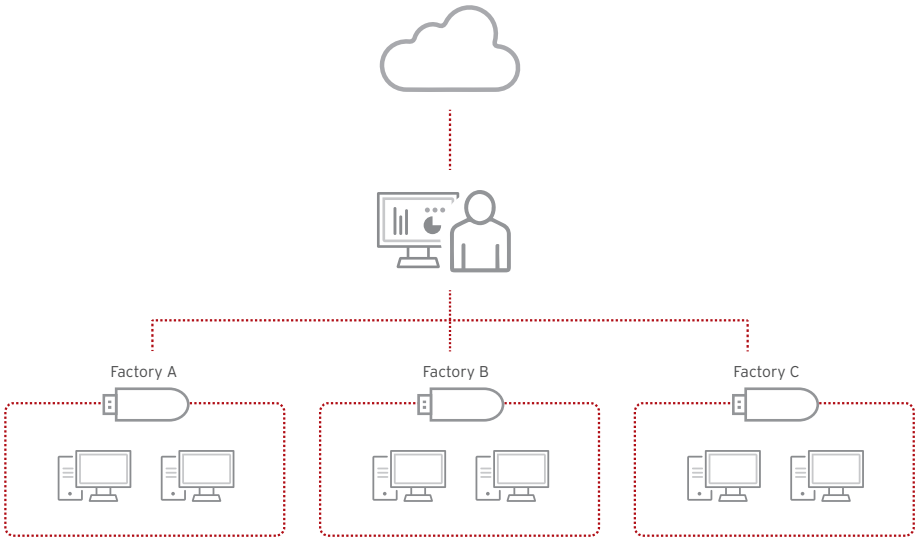
Trend Micro Portable Security 3 provides a solution for malware-scanning and removal in environments that include standalone and systems that are not networked, but allow data exchange via USB sticks, DVDs, and other ways. This portable tool can be connected to Windows or Linux-based devices via a USB port to detect malware and remove it (if necessary) without any software installation. When a scan is performed, colored LEDs indicate whether malware has been found or removed or if further investigation is required. In addition, Trend Micro Portable Security 3 collects important asset information during the scan, increasing the transparency of operational technology (OT) and eliminating undocumented Shadow OT. A centralized management program allows you to create policies and the investigation of scan logs for multiple Trend Micro Portable Security 3 tools and different locations, so that security responsibility provides a holistic overview of all endpoint devices. In addition, scan configurations can be transferred remotely or physically to multiple tools in different locations.

Benefits

- No installation required
- Easy operation
- Works across multiple platforms
- Eliminates Shadow OT
- Centralized management

Features

- Deletion or quarantine of malicious files
- Multiple options for malware scanning
- Current updates for malware signatures
- Supports on-demand and boot scans status
- Display via LED
- Integrated self-protection
- Integrated scan logs
- Supports Windows and Linux
- Collects asset information
- Supports case in file and folder names on Windows



TXOne EdgeIPS™

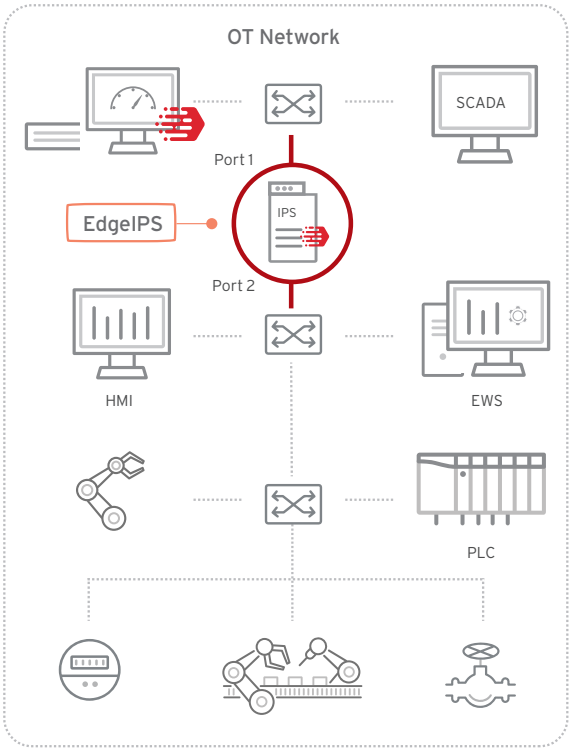
EdgeIPS protects business-critical machines, individual cells/systems, as well as small production zones and supports uninterrupted production line operations. This solution enables reliable OT visibility, OT protocol filtering, and inline or offline functionality. EdgeIPS is specially developed to integrate into the network without disturbing the existing configuration. Industrial environments usually include tools and devices that were not designed to be connected to a modern company network. This provides reliable security which does not necessitate changes to the manually configured network topology. EdgeIPS ensures visibility and protection of legacy systems and devices without a patch, which forms the backbone of the production line and ensures uninterrupted operations.

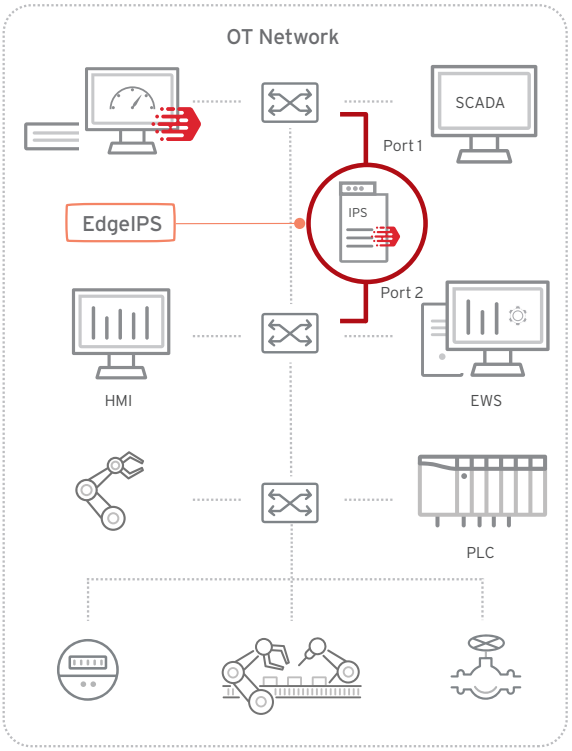
Advantages

- Minimizes time spent on configuration, maintenance, and administration
- Can be deployed at any location
- Increases the visibility and reliability of business-critical systems
- Does not require changes to network topology

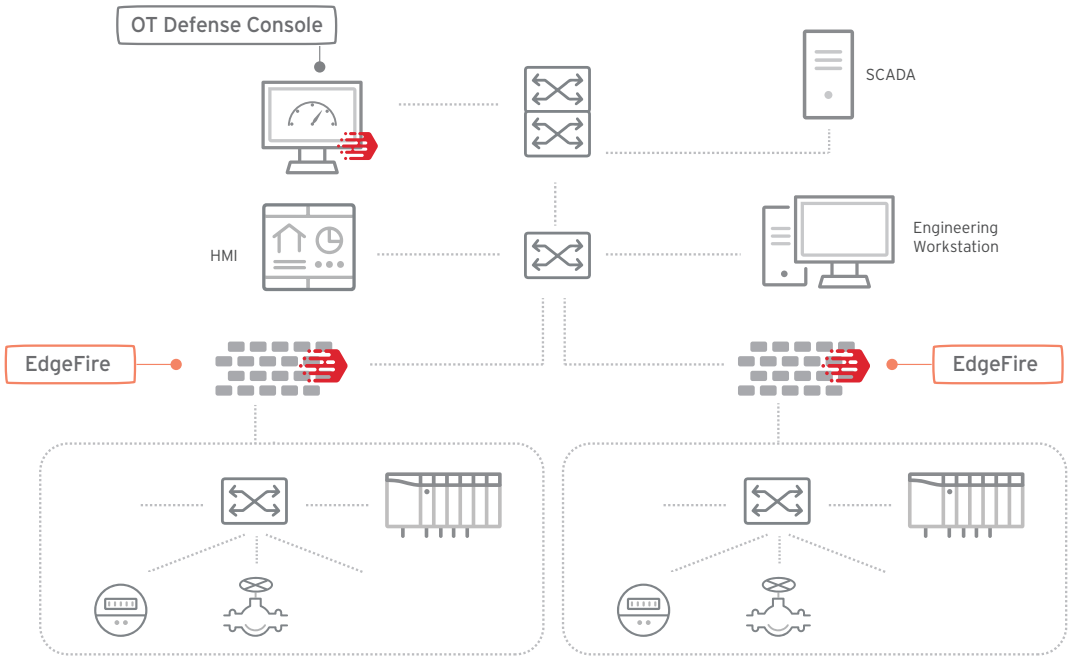
Features

- Visibility of network traffic
- OT protocol whitelisting controls for mission-critical systems
- Improved visibility of the Shadow OT through integration of IT and OT networks
- Signature-based virtual patching
- Switches between two flexible modes (monitor and protect)
- Uninterrupted operation in the event of network hardware failures
- Supports a wide range of industrial protocols
- Leading threat information and analysis
- Easy management centralization





TXOne EdgeFire™



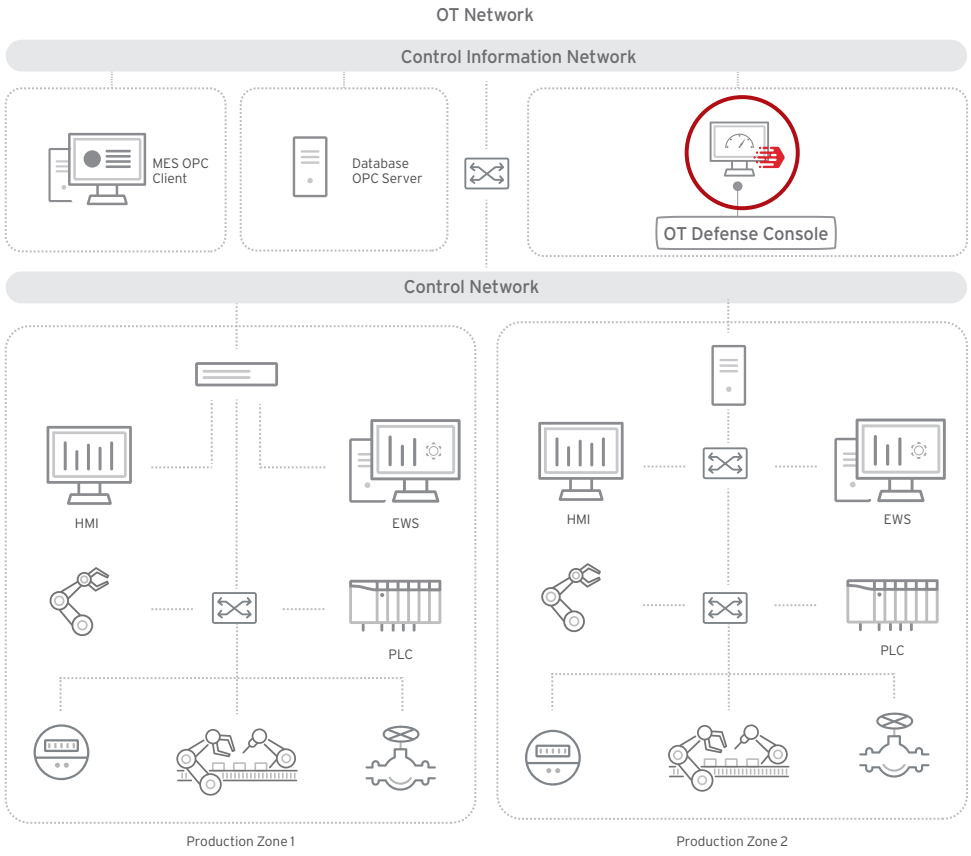
Due to the ever increasing integration of information and operational technology, the defense against threats must become an intuitive component. In traditional industrial environments, information technology (IT) and operational technology (OT) are usually operated separately from one another—each with its own network, maintenance team, goals, and requirements. In addition, industrial environments are made up of tools and devices that are not designed to connect to a corporate network. This makes the timely provision of security patches and updates extremely difficult. With EdgeFire Next-Generation Firewall, companies can optimize the effectiveness of their cyber defense.

Advantages

- Reliable firewall offers security, stability, and comfort
- Detects and blocks the spread of threats using unique hardware
- Offers full visibility into Shadow OT

Features

- OT protocol filter controls for mission-critical machines
- Improved visibility into Shadow OT through integration of IT and OT networks
- Signature-based virtual patching
- Switches between two flexible modes (monitor and protect)
- Supports a wide range of industrial protocols
- Leading threat information and analysis
- Flexible segmentation and isolation
- Centralized management



OT Defense Console

The manufacturing industry and critical sectors, such as oil and gas, mining, chemicals, energy, and defense have had to cope with crippling cyberattacks in recent years. Protecting infrastructure against threats is central to any operational technology (OT) environment. This poses a challenge for traditional IT security management because proprietary SCADA/ICS networks and devices are often used that are both business-critical and highly sensitive. Industrial plants also require remote access by the manufacturer in order to receive prompt support. This further increases the complexity of OT network security. With the OT Defense Console (ODC), companies can achieve complete OT visibility and, if necessary, make immediate adjustments to ensure the smooth operation of the production line.

Advantages

- Designed for industry standard reliability, security, and flexibility
- Full visibility of large OT networks
- Improves usability and interconnectivity

Features

- Organization of all information with the ODC dashboard
- Overview of the cyber environment
- Easily manage large amounts of network nodes
- IPS and policy enforcement by group
- Convenient pattern and firmware updates
- Log view and query
- Form factor: Hardware or virtual appliance