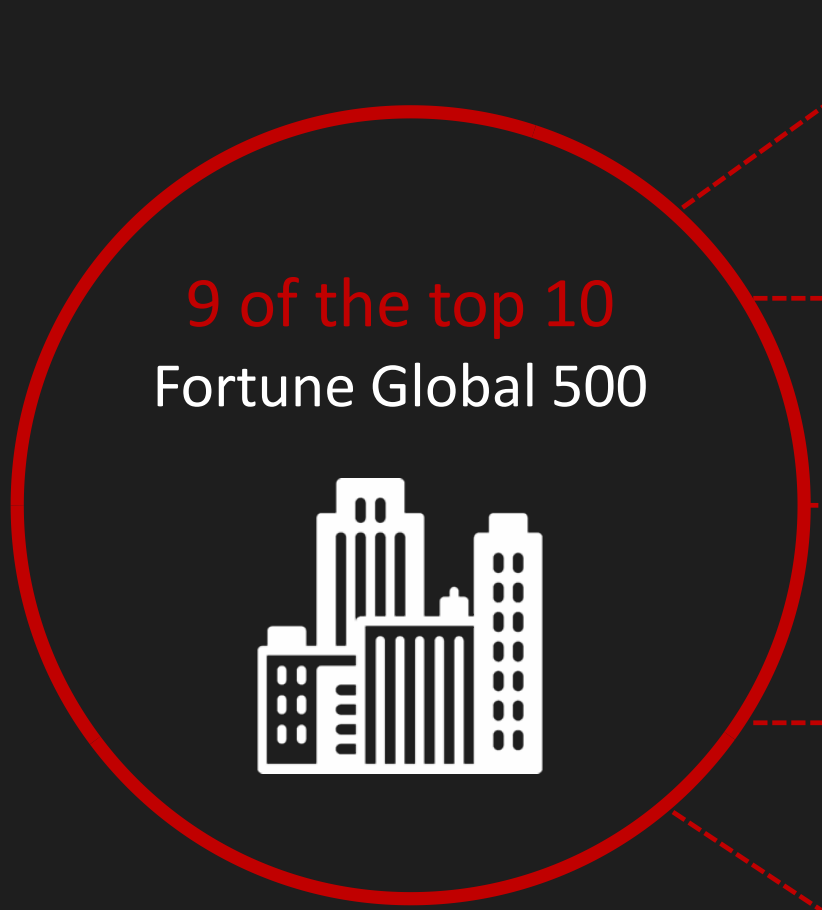
# Решения Trend Micro для защиты OT

Dmytro Ostapenko

Trend Micro Inc.

dmytro_ostapenko@trendmicro.com

# Лидер, которому доверяют Лидеры




8 of the top 10
Banking Companies

10 of the top 10
Telecom Companies

9 of the top 10
Healthcare Companies

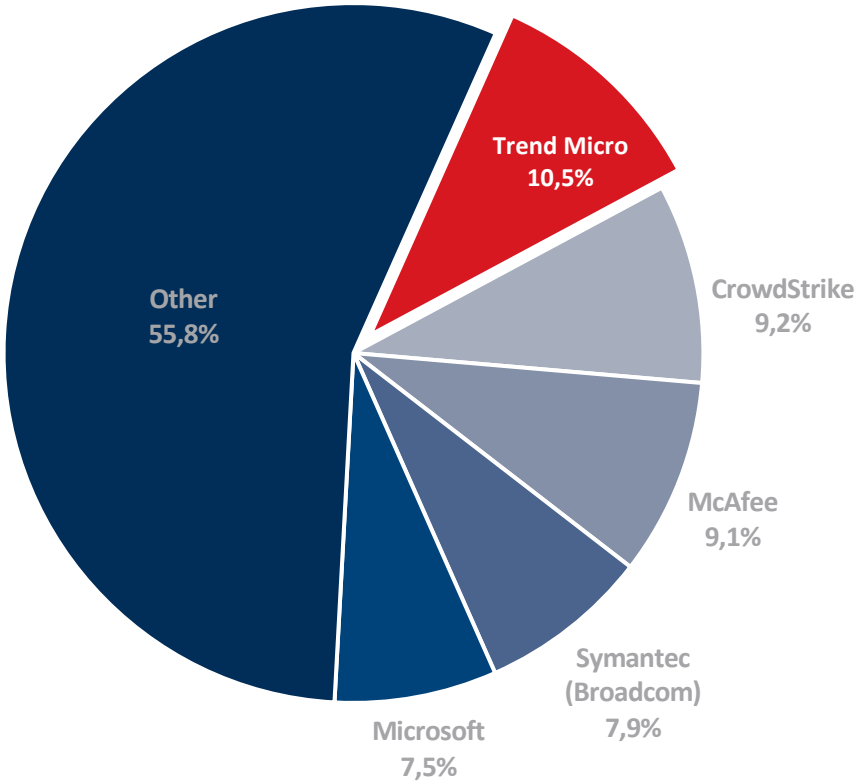
9 of the top 10
Petroleum Companies

8 of the top 10
Automotive Companies

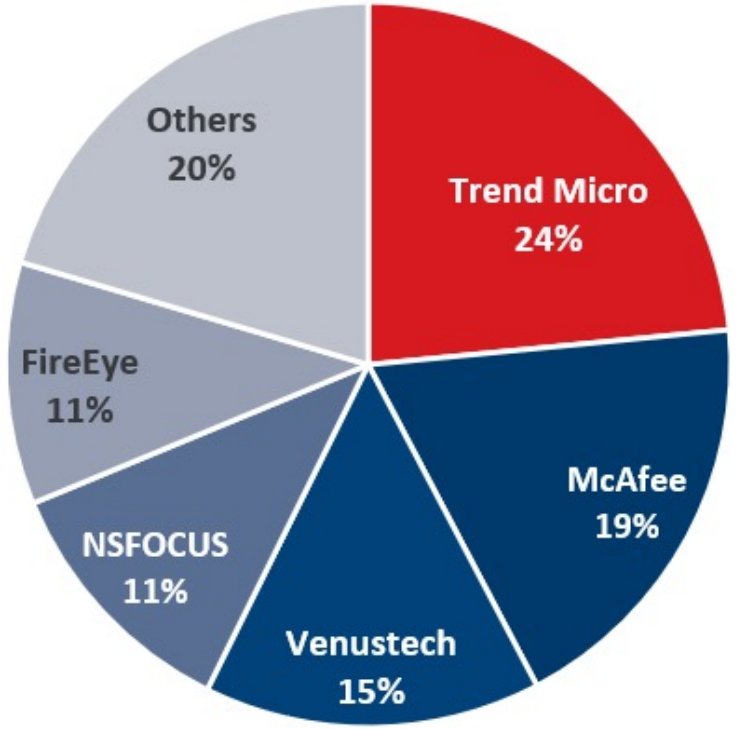
TREND MICRO

# Лидер в корпоративном сегменте по объему продаж

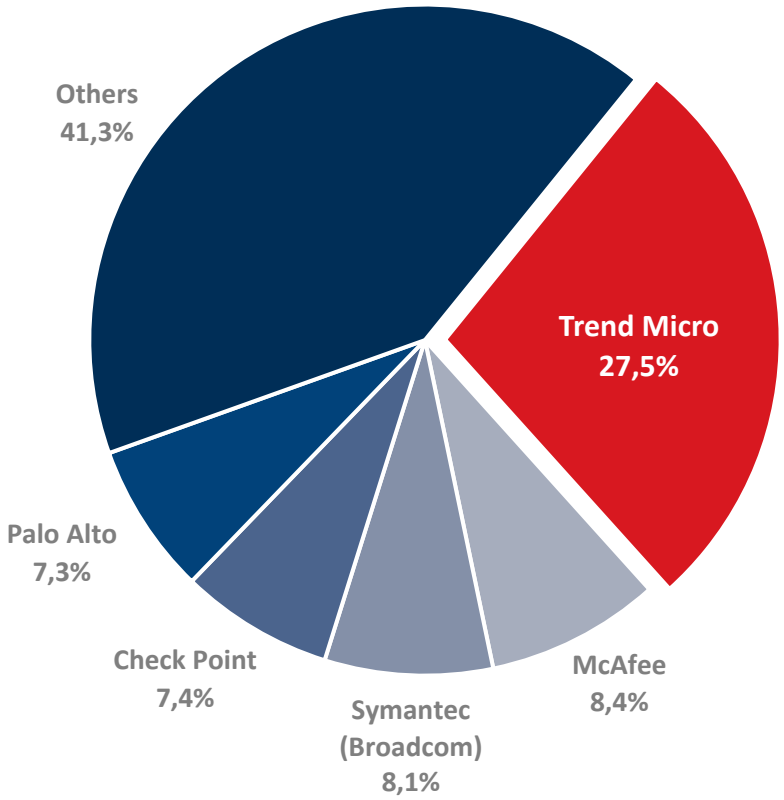
## #1 Market Share
### for Corporate Endpoint Security, 2020




## Market Share Leader in IDPS
2020




## #1 Market Share
### for Hybrid Cloud Workloads, 2020




Revenue in Million USD for 2019-20. Graphic prepared by Trend Micro based the Gartner report.
Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 4Q20, March 2021

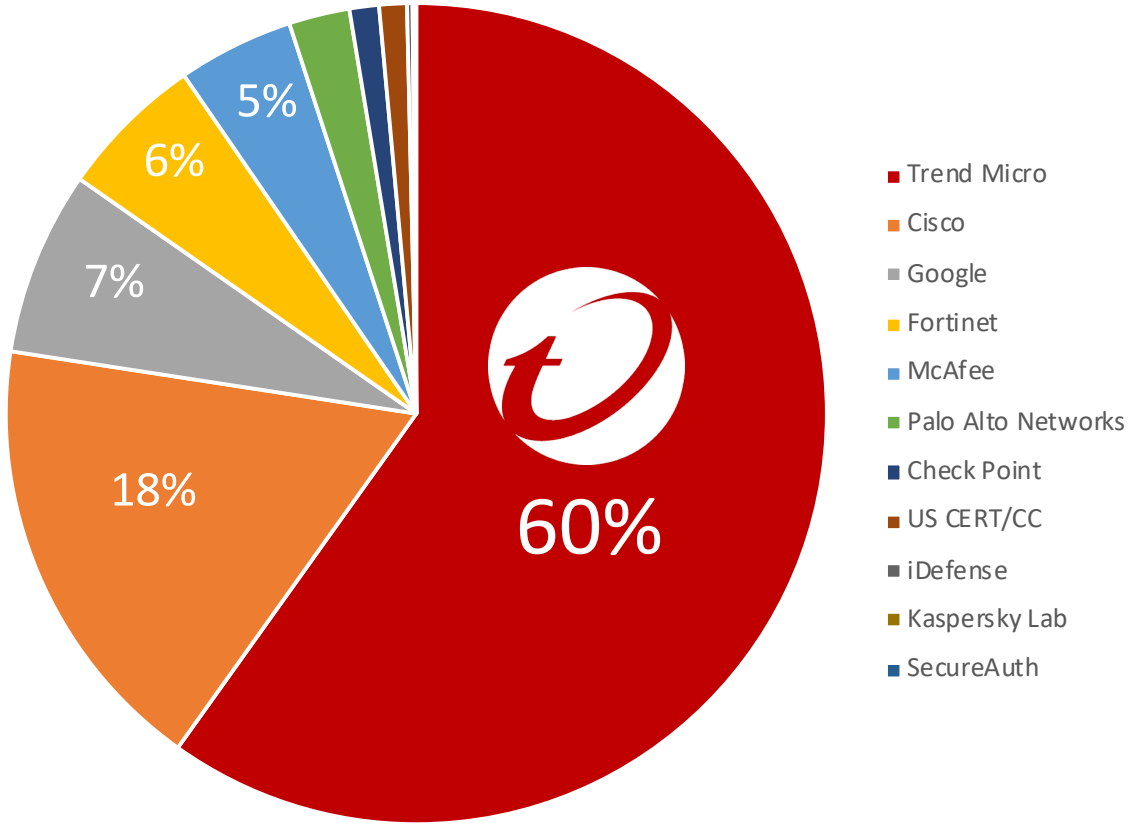
Source:
1. Worldwide Corporate Endpoint Security Market Shares, 2020: Pandemic and Expanding Functionality Propelled Market Growth, IDC #US47768021, June 2021
2. Worldwide Cloud Workload Security Market Shares, 2020 IDC #US47837121, June 2021

# Лидер рынка по выявленным уязвимостям в ПО и ОС

## Zero Day Initiative

(общественная платформа, выкупает информацию о выявленных уязвимостях у энтузиастов/специалистов/DarkNet)

- 10,000+ независимых исследователей
- Лидер рынка на протяжении прошедших 13 лет. Раскрыто и опубликовано порядка 60% от всех найденных уязвимостей в 2020




*Source: 2020 Public Vulnerability Market, Omdia, April 2021*




TREND MICRO | research

# Лидер рынка по выявленным уязвимостям в ПО и ОС

## Zero Day Initiative

(общественная платформа, выкупает информацию о выявленных уязвимостях у энтузиастов/специалистов/DarkNet)

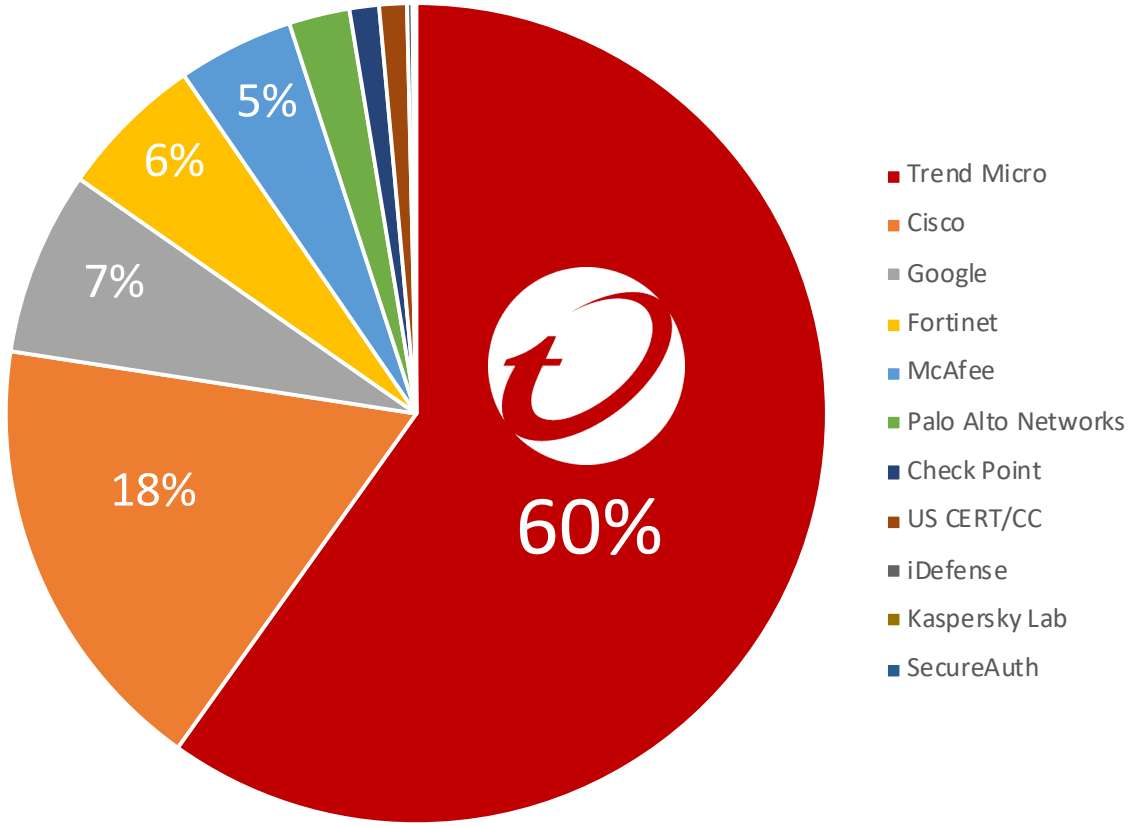
ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Adobe

Microsoft

Крупнейший поставщик для:

- ICS-CERT
- Adobe и Microsoft




*Source: 2020 Public Vulnerability Market, Omdia, April 2021*




TREND MICRO | research

# Количество выявленных уязвимостей в продуктах компании Microsoft

| Vendors | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|
| Trend Micro | 70 | 93 | 118 | 160 | **176** |
| Fotinet | 4 | 11 | 14 | 12 | **12** |
| Palo Alto | 9 | 16 | 3 | 34 | **58** |
| Cisco | 2 | 0 | 2 | 4 | **36** |
| Symantec | 0 | 0 | 0 | 2 | **0** |
| McAfee | 0 | 7 | 4 | 13 | **54** |
| Fireeye | 5 | 16 | 1 | 1 | **19** |
| Sophos | 0 | 0 | 0 | 3 | **0** |
| Crowdstrike | 1 | 1 | 8 | 0 | **9** |
| Carbon Black | 0 | 0 | 0 | 0 | **0** |

https://portal.msrc.microsoft.com/en-us/security-guidance/acknowledgments

Trend Micro vision one

# Threat Defense Platform for Security Operations

Risk Visibility & Insight

**XDR**
Extended Detection & Response

Agent & Policy Management

Trend Micro apex one

## Security for Users

- Workstations
- Mobile
- Mail
- Web
- Apps
- Android
- iOS
- Microsoft 365
- G Suite
- Windows
- Apple

Trend Micro cloud one

## Security for the Hybrid Cloud

- Servers
- Virtual Machines
- Cloud Workloads
- Containers
- Applications
- Open Source Scanning
- Cloud Network
- Cloud Security Posture Management
- File Storage
- aws
- Google Cloud
- Microsoft Azure
- Linux
- Windows
- docker
- kubernetes
- vmware

Trend Micro network one

## Security for Networks

- IPS
- Prevention
- Detection
- IOT Protection
- Sandboxing

TREND MICRO research

SECURITY POWERED BY **GLOBAL THREAT RESEARCH**

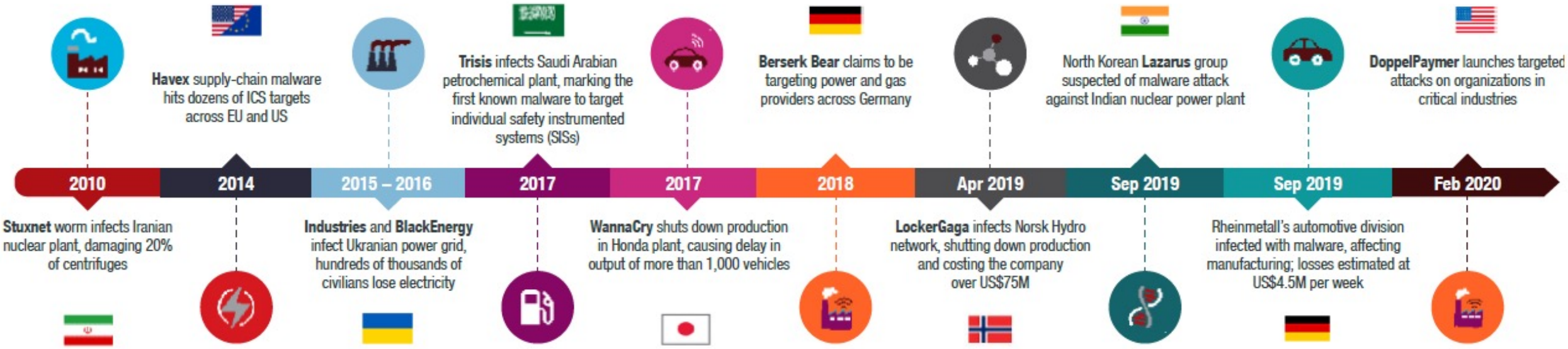
THREAT INTELLIGENCE | VULNERABILITIES | CYBERCRIMINALS | FUTURES

SMART PROTECTION NETWORK

# Отличия промышленной системы от корпоративной

| Промышленная система (ОТ) | Требование ИБ | Корпоративная система (ИТ) |
|---|---|---|
| Доступность | Главный приоритет | Конфиденциальность |
| 24x365 (без перезагрузок) | Доступность | В рабочие часы |
| Масштабный ущерб | Последствия инцидента | Денежный ущерб |
| 10-20 лет | Жизненный цикл | 3-5 лет |
| Реальное время | Скорость обработки данных | Допустима задержка |
| Нерегулярно (1—2 года) | Периодичность обновлений | Часто и регулярно |
| Инженерный департамент | Эксплуатация | Подразделение ИТ/ИБ |
| Осознаются после инцидента | Подход к рискам | Оценены заранее |
| Процесс/услуга (непрерывность) | Объект безопасности | Информация |

# Временная шкала существенных кибератак и их последствия




## 2010 — Iran Stuxnet centrifuges attack

? **Four zero-day vulnerabilities** on USB devices spread through the organization's network and infected Siemens equipment.

⚠ The centrifuges were out of control during operations, causing physical damage.

## 2014 — German steel mill attack

? Malicious actors accessed the office network through an **APT attack**, and then obtained privilege of control over the production system.

⚠ The steel mill shut down unusually, causing massive physical damage.

### Japan's Monju Nuclear Power Plant attack

? **Malware** was loaded onto vulnerable patch software.

⚠ More than 42,000 emails and personal training reports were leaked.

## 2015 — Ukraine power grid attack

? Malicious actors used spear-phishing emails with **BlackEnergy 3 malware** and gained employee login access.

⚠ They modified the system password and used a denial-of-service (DoS) attack on telephone lines, which meant systems could not be operated by employees. Around 220,000 people experienced blackouts.

## 2017 — Middle East Trisis plant attack

? **Trisis** malware attacked factory safety instrumented systems (SISs).

⚠ Plant operations were tripped up.

## 2018 — Taiwanese semiconductor company attack

? **Ransomware** attacked Taiwan Semiconductor Manufacturing Company (TSMC).

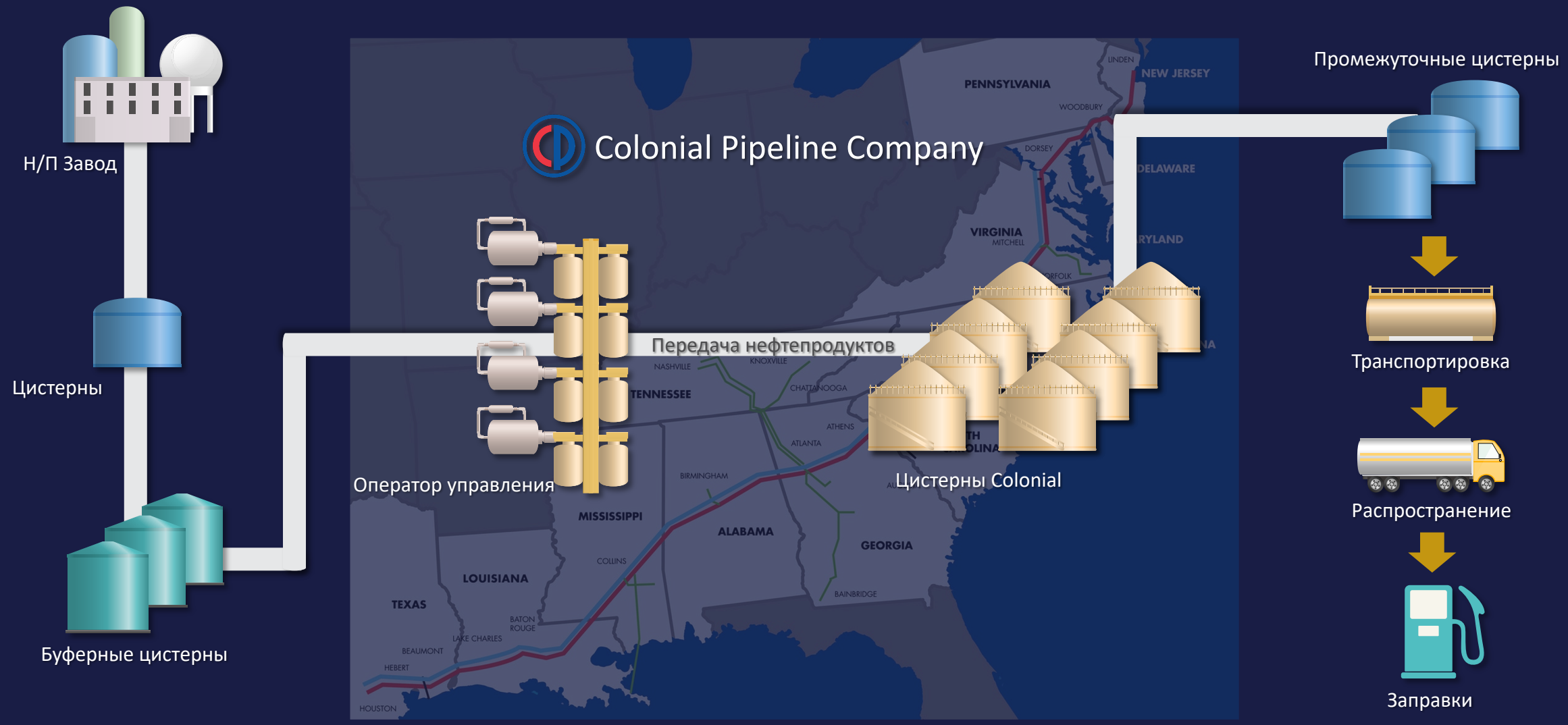
⚠ The company lost US$255M in downtime and 10,000 machines were affected.

## 2020 — US parts supplier attack

? **Ransomware** targeted the manufacturing company Visser Precision.

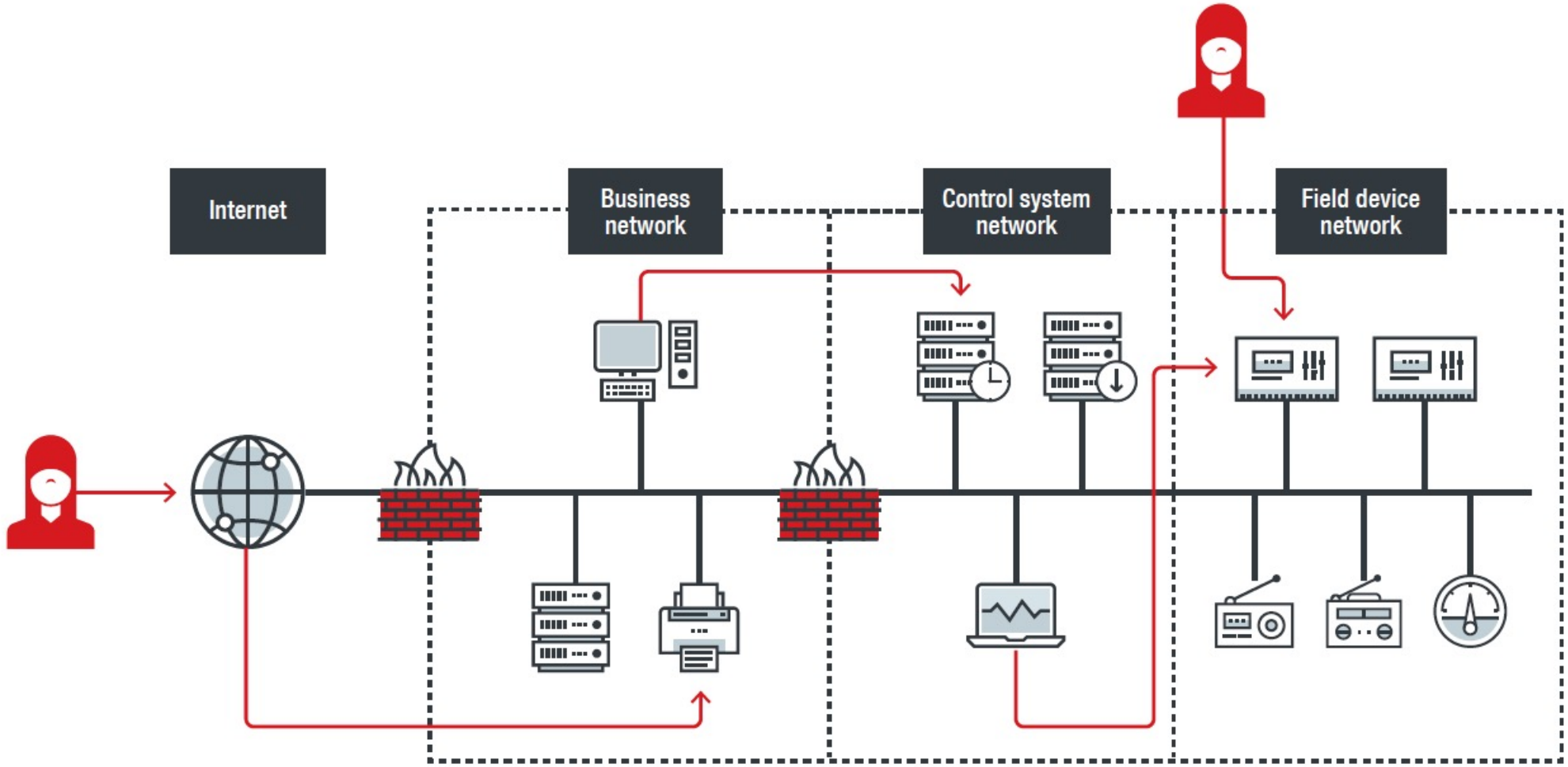
⚠ Files were encrypted and data exfiltrated.

# Colonial Pipeline (США). Кибератака 7 мая 2021г

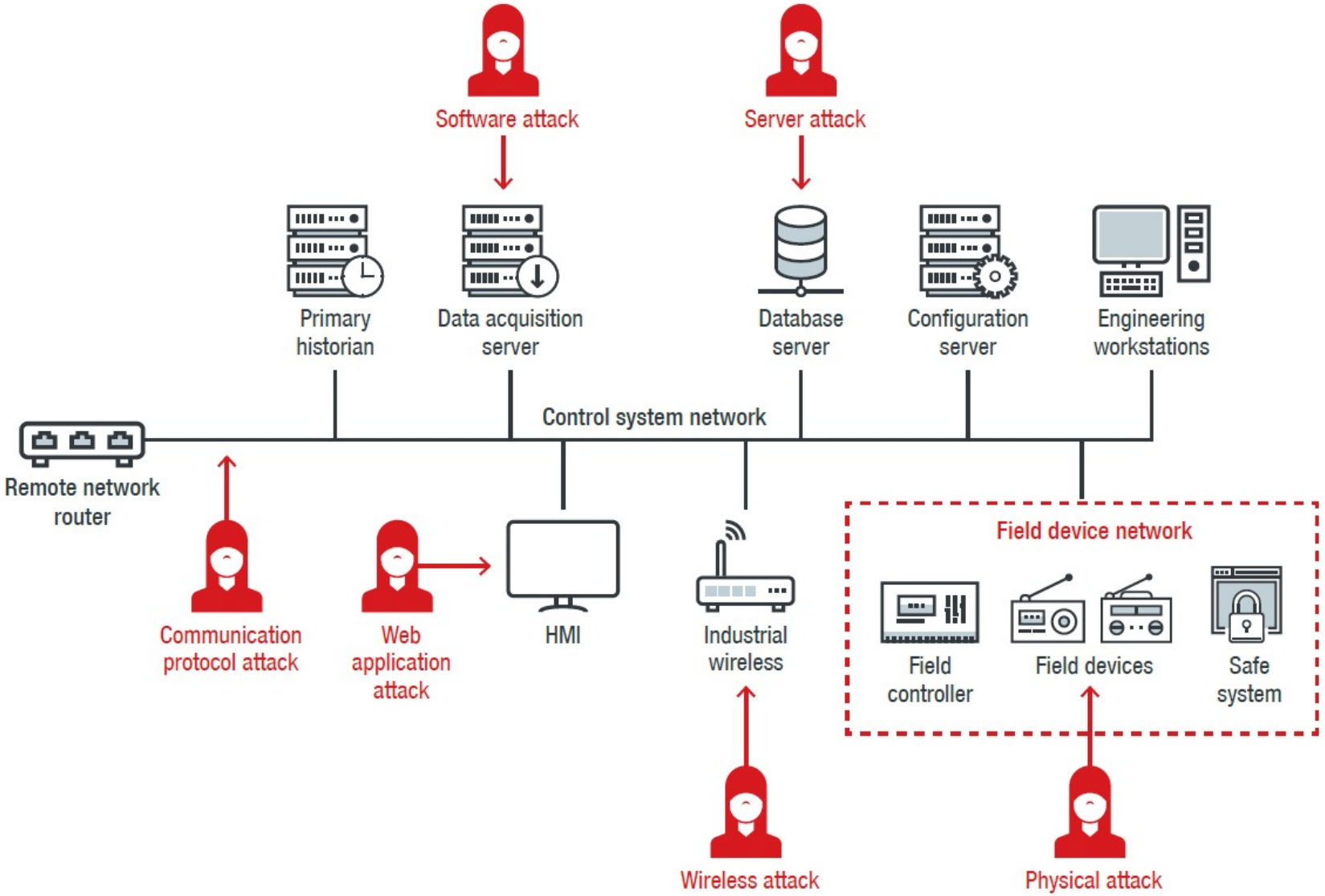



TREND MICRO txOne networks

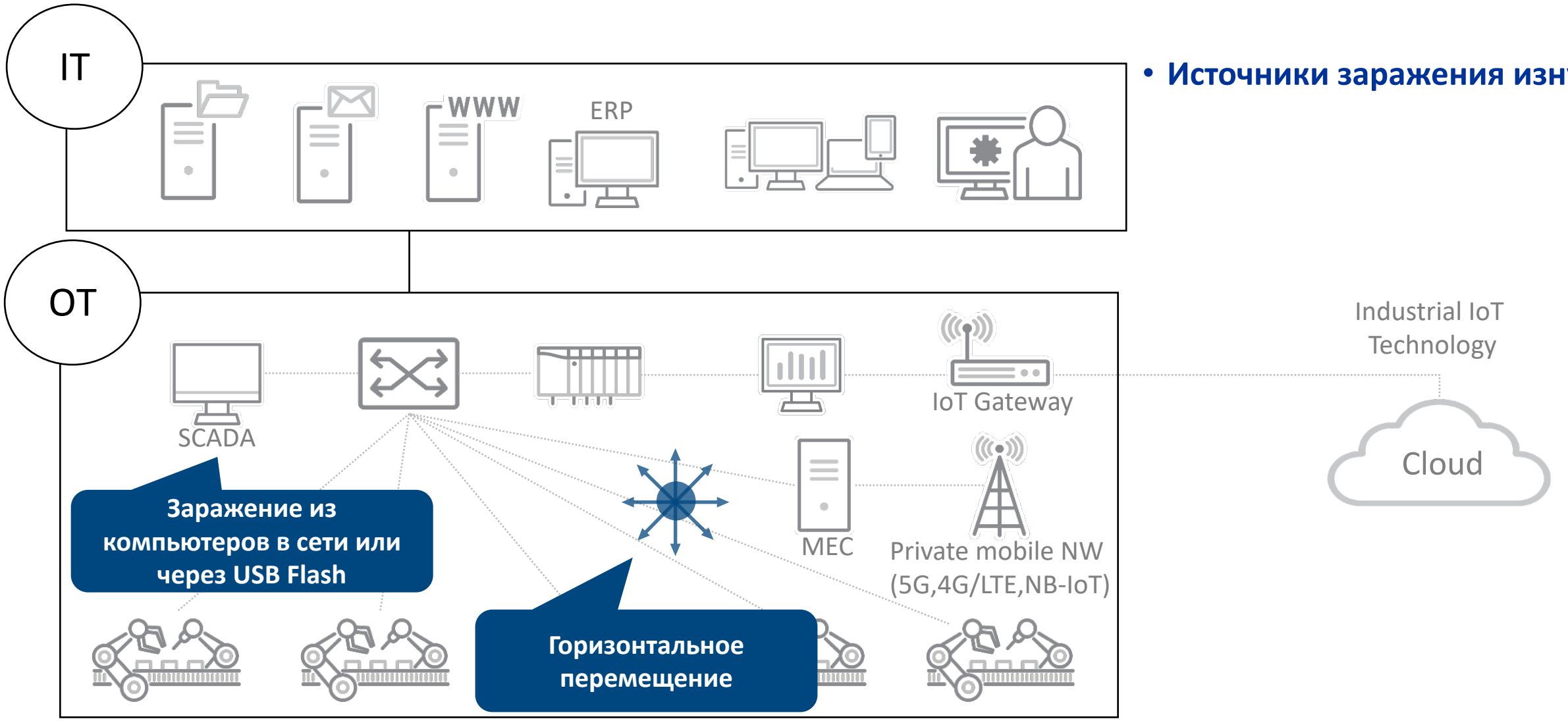
# Текущий взгляд на пробелы в кибербезопасности комбинированных сетей



# ICS (АСУ ТП) векторы атак

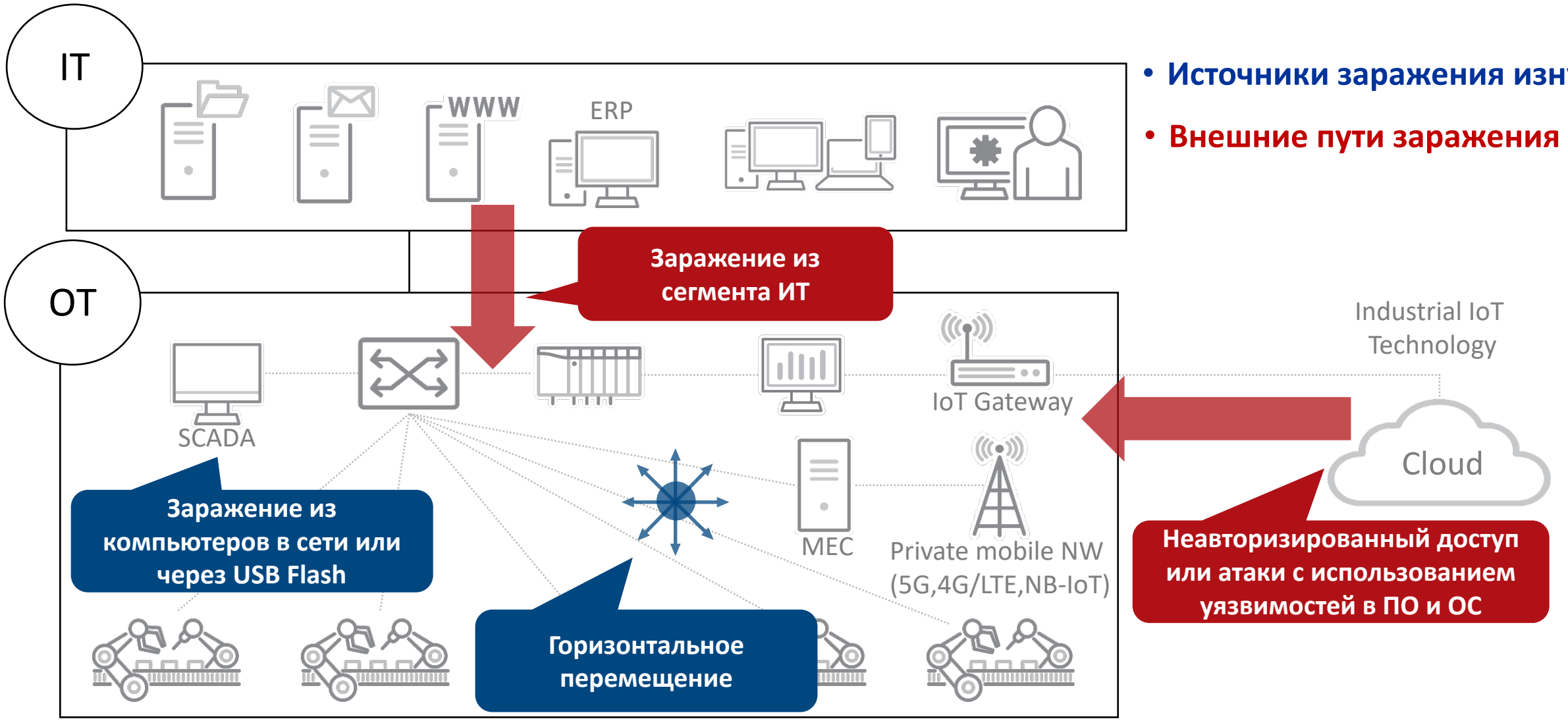


# Векторы заражения




- **Источники заражения изнутри**

# Векторы заражения




- **Источники заражения изнутри**
- **Внешние пути заражения**

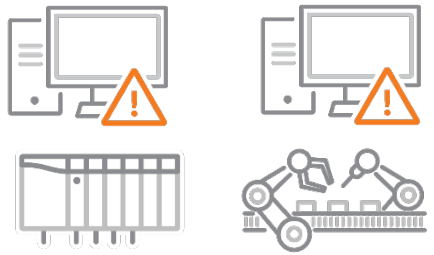
# Потенциальные риски, вызываемые кибератаками

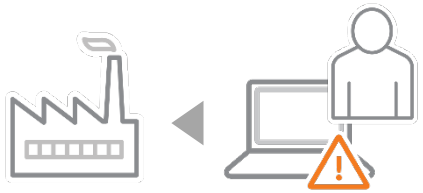
| | | | |
|---|---|---|---|
| Риски Бизнеса | Финансовые потери | Репутация компании | Вред здоровью |
| Риски Производства | Остановка производства | Доставка бракованной продукции | Глобальные поломки |

txOne networks

# Подход, предлагаемый Trend Micro

# Риски безопасности и технических реализаций





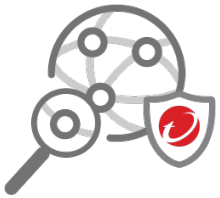
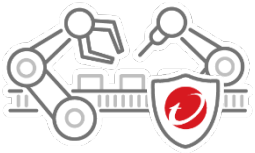
| | | | | |
|---|---|---|---|---|
| Риски | Уязвимости | Вредоносное ПО | Одноранговая сеть | Внутренние источники заражения |
| Технические задачи | • Патчинг<br>• Замена устаревших ОС<br>• Исключение уязвимых служб<br>• Изъяны в индустриальных протоколах | • Установка ПО<br>• Производительность<br>• Подключение через незащищенные каналы | • Конфигурация сетей | • Контроль сторонних работ/ПО |

• Суровые условия эксплуатации
• Недостаток IT/знаний по безопасности
• Глобальное единоразовое развертывание

# Обеспечение непрерывности процессов

## Защита от кибератак через “Укрепление производственной среды”

# Подходы по укреплению среды производства

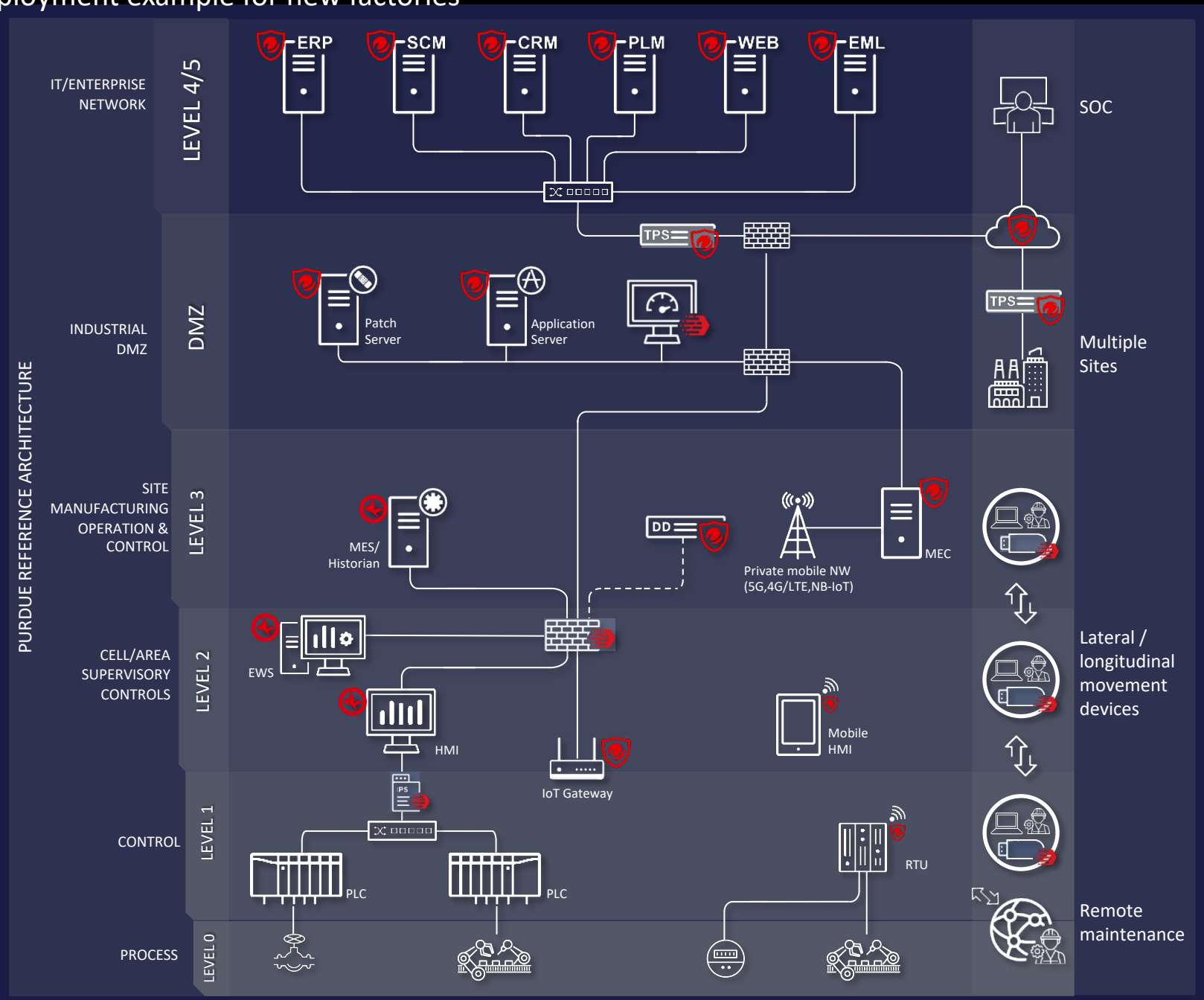
| Элементы | | Решения безопасности |
|---|---|---|
| **Предотвращение** |  | **Блокирование кибератаки со стороны ИТ, устройств IIoT и облака**<br>• Предотвращение атак на уязвимости, заражения вредоносным ПО и горизонтальных перемещений в точках обмена данными |
| **Детектирование** |  | **Выявление внутренних кибератак в среде ОТ**<br>• Визуализация киберугроз |
| **Защита и устойчивость** |  | **Защита промышленных устройств управления и минимизация зоны поражения**<br>• Безопасная сегментация сети и применение политик<br>• Всесторонняя защита, сканирование на вредоносное ПО |

# Подходы при планировании инфраструктуры

| | Предотвращение<br>Безопасность обмена данными | Детектирование<br>Раннее обнаружение аномалий | Защита<br>Защита устройств и операций |
|---|---|---|---|
| IT/Enterprise network (LEVEL 4/5) | • Сеть, DMZ | | |
| Industrial DMZ | | • Пассивный анализ сети<br>- Выявление<br>- Горизонтальное перемещение<br>- C&C | |
| Site operation & control (LEVEL 3) | • Ноутбуки, рабочие станции<br>• USB устройства<br>• IoT шлюзы<br>• EWS, подключенные к “облаку”<br>• Частная беспроводная сеть | | • Сеть<br>- Сегментация<br>- Применение политик<br>- Защита от уязвимостей<br>• Конечные точки<br>- Периодическая проверка<br>- Защита новейшими техниками |
| Supervisory controls (LEVEL 2) | | | |
| Control (LEVEL 1) | | | |
| Process (LEVEL 0) | | | |

**Красным выделены улучшения, которые можно заложить на этапе планирования новых объектов*

# Deployment example for new factories




IT Centric solution

Endpoint/Server Security

Hybrid cloud protection
**Trend Micro Cloud One**
Automated, flexible, all-in-one solution

Endpoint protection
**Trend Micro Apex One**
Automated, insightful, all-in-one protection

Network security

Gatekeeper IPS
**TippingPoint Threat Protection System**
Blocks malicious traffic

APT prevention
**Deep Discovery Inspector**
Network-wide detection of targeted attacks

ICT centric solution

Flexible & reliable high-performance security for MEC
**Trend Micro Mobile Network Security**
Secures private mobile networks (5G,4G/LTE,NB-IoT)

OT centric solution for Shop Floor

Industrial endpoint security

Installation-less malware scanning tool
**Trend Micro Portable Security 3**
Periodical health-check processes

Next-generation ICS endpoint security
**TXOne StellarProtect** (StellarEnforce for legacy OSes)
Protects mission-critical assets

Built-in security software for critical devices
**Trend Micro IoT Security**
Secures low resource devices

Industrial network security

Industrial central management console
**OT Defense Console**
Plant defense field management

Industrial next-generation firewall
**EdgeFire**
Enables secure network segmentation

Industrial next-generation IPS / Array
**EdgeIPS / EdgeIPS Pro** (for large-scale networks)
Cell segmentation for critical assets protection

**Trend Micro Vision One and Professional Services**

TREND MICRO | TXOne networks

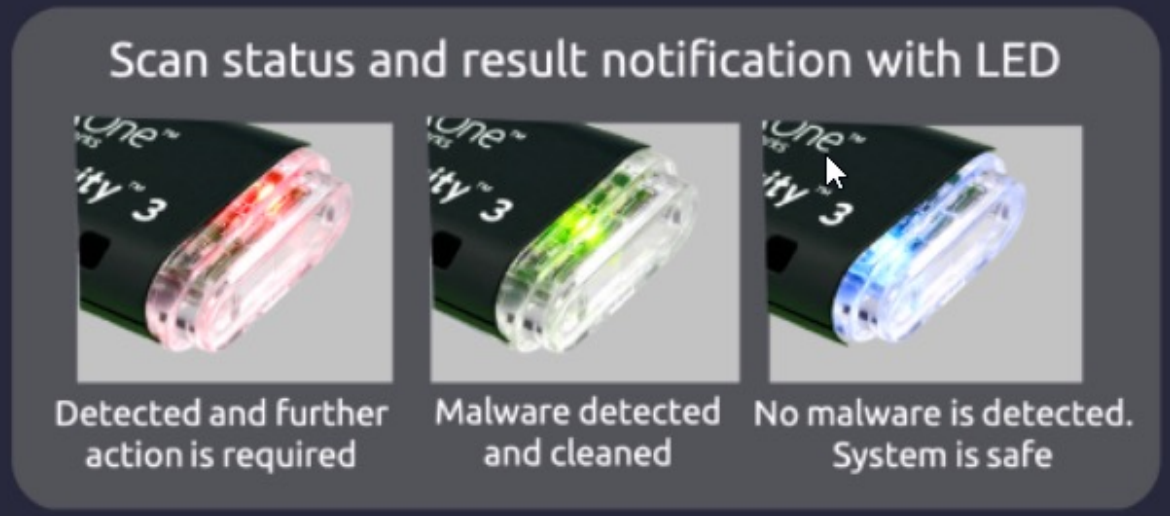
txOne networks

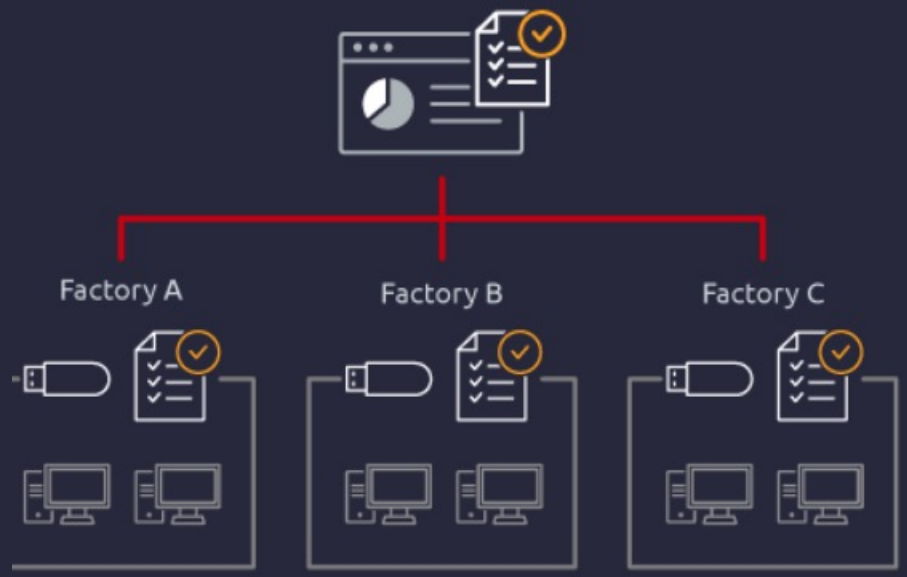
# Инструментарий Trend Micro Для применения в ОТ

# Стык IT/OT и инженерных работ

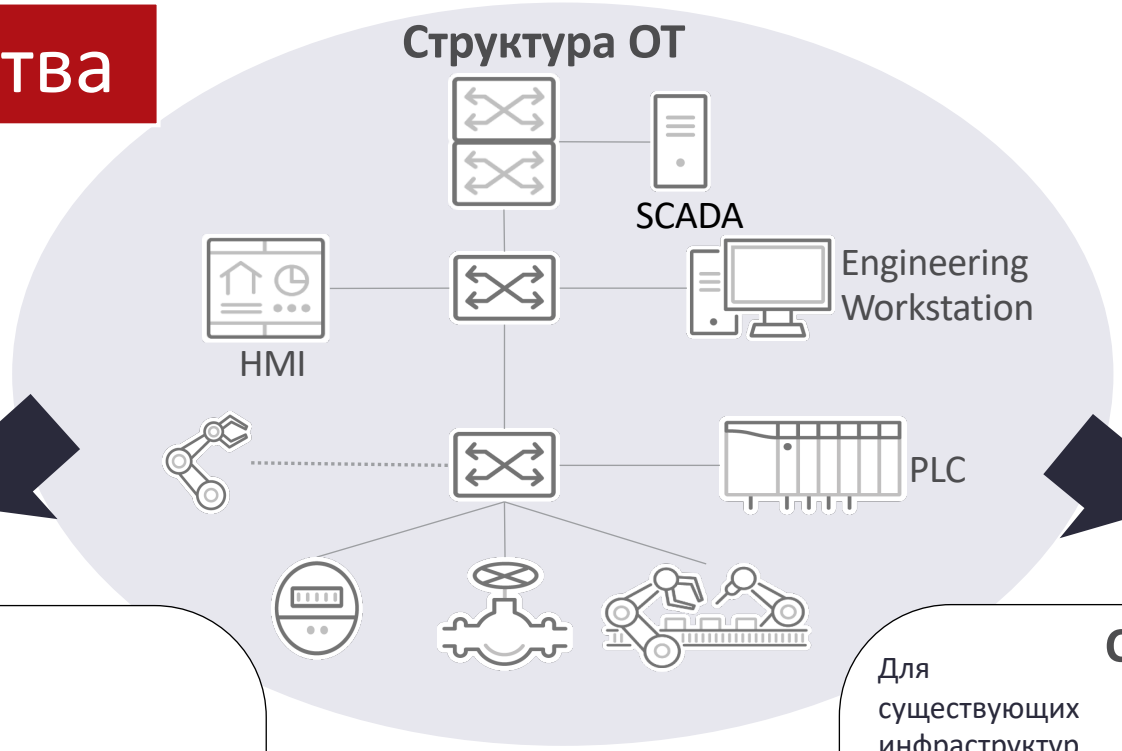

Недостаток понимания присущ как инженерам IT, так и операторам OT:

# Trend Micro Portable Security USB-устройство

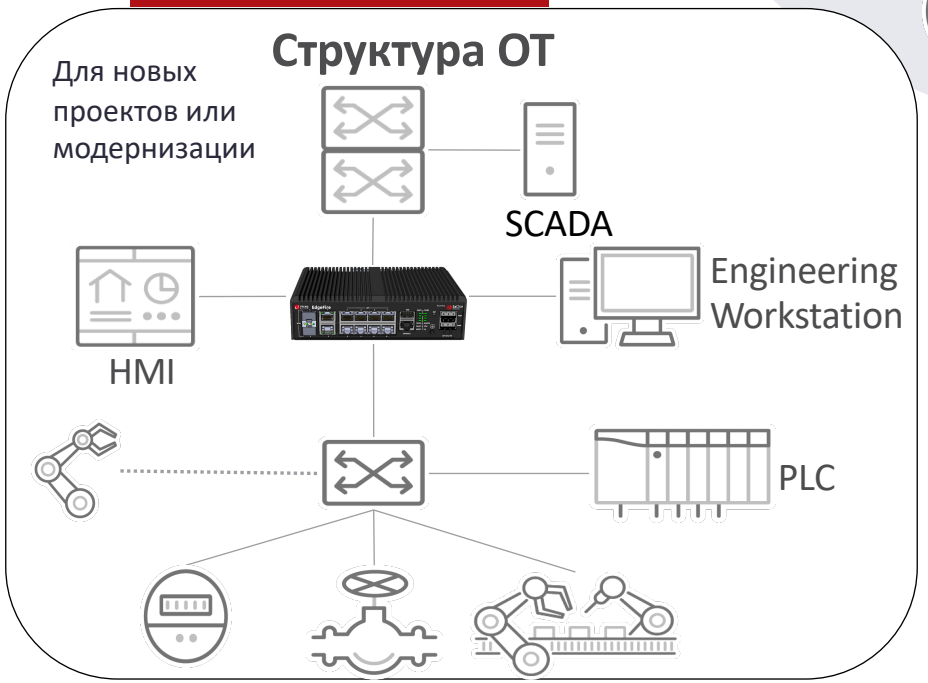


# Сетевые устройства

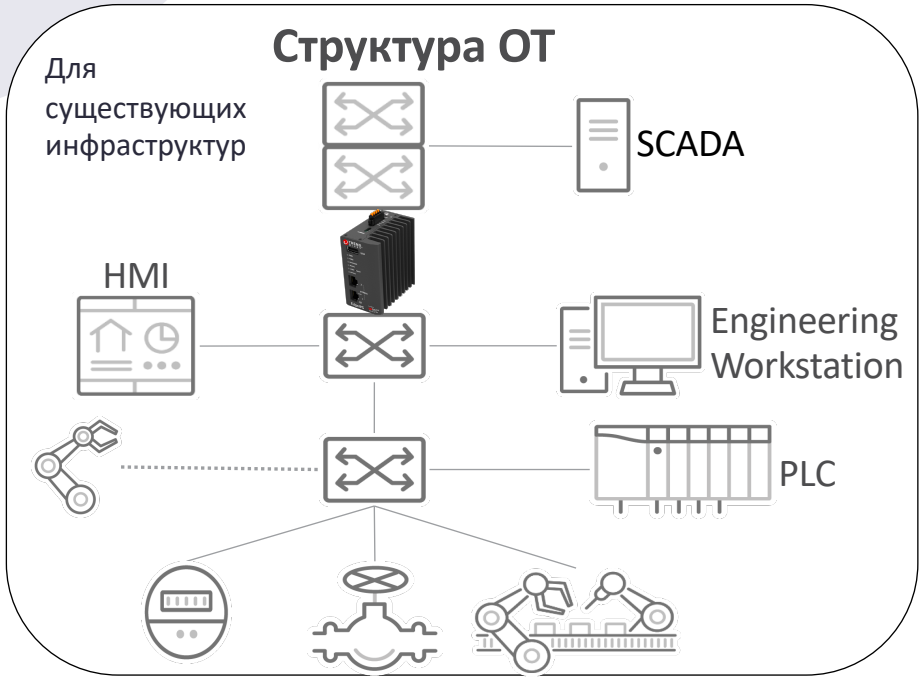



## EdgeFire (NGFW)




Сегментация и сдерживание

## EdgeIPS




Контроль разрешенных коммуникаций

# EdgeIPS Series: Next-Generation Industrial IPS

*L2-L7 Visibility and Protection*

- Network visibility
- Protocol Filter - Whitelisting Control
- Virtual Patch
- TXODI inside
- Hardware Bypass
- Dual Power input


(2 Copper ports + USB)

Product name : EdgeIPS
Short name : IPS

**Защитить критически важную инфраструктуру**

- Разворачивается перед важными активами (компьютеры, HMI и контроллеры) и обеспечивает двунаправленную защиту

**Реальная интеграция IT-OT**

- Обеспечение видимости и контроля OT, а также мониторинга и защиты кибербезопасности для обеспечения возможности совместной работы ИТ и OT.
- Аппаратный Bypass

**Простое управление**

- Централизованное управление с помощью OT Defense Console (ODC)
- Управление единым блоком через веб-консоль.
- Объектно-ориентированная конфигурация для IP и сетевой службы
- Zero-configuration

**Надежность системы**

- Высокая MTBF
- Dual power-Input
- -40 to 75°C wide temperature operation
- 5-years warranty
- Industrial grade hardware design
- Self-recovery watchdog
- *Wide Temperature (–40°C to 75°C)

| OT Protocol | | | | | | |
|---|---|---|---|---|---|---|
| OIL & GAS | Building Management | Distributed Control Systems | Safety | Electric & Distribution | Automation & Production | |
| Emerson ROC | Systems | Honeywell Experion | Triconex | ABB 800xA DCS protocols | OMRON Fins | GE PAC8000 |
| ABB TotalFlow | Siemens P2 | FTE (Honeywell) | Yokogawa ProSafe | ABB Bailey | Plus-S7/S7 | Mitsubishi Melsec / Melsoft |
| | Bacnet | Emerson Ovation DCS protocols | | MMS | Siemens IP/EtherNet | Sattbus |
| | | Emerson DeltaV DCS protocols | | ICCP TASE.2 | Rockwell including (CIP extension) | OPC DA/AE/UA |
| | | Yokogawa VNet/IP | | IEC104 | CSPv4/PCCC | Profinet-DCP |
| | | GE Mark6e (SDI) | | DNP3 | Compresson Controls | Profibus |
| | | Schneider Foxboro | | GOOSE | Corporation (CCC) | Modbus |
| | | | | Schweitzer | OPTO Control Technology Inc (CTI) | Modbus Schneider |
| | | | | Brüel & Kjær Vibro (BKV) | Lantronix | Modbus Altivar |
| | | | | Bently Nevada | GE-SRTP | Modbus Concept / Momentum |
| | | | | | GE QuickPanel | Modbus RTU |
| | | | | | GE EGD | OSISoft Pi |

| IT Protocol | | | | | |
|---|---|---|---|---|---|
| CDP | LLDP | DCE/RPC | DHCP V4/V6 | ARP | VNC |
| NTP | RDP | SSL | NTLMSSP | ATSVC | SMB-PIPE |
| SNMP | SSH | HTTP / HTTPS | FTP | Telnet | SMB / CIFS |
| ICMP | IGMP | Browser | DNS | TFTP | TCP/IP |

# Center of TXODI™

## Наблюдаемость

- Обеспечение видимости устройства и протокола для сетевых администраторов

## Whitelisting Контроль

- Полный белый список на устройстве, протоколе и операции. Например, «PLC1 может взаимодействовать с ПК1 по протоколу Modbus **ТОЛЬКО** для операции чтения»

## Защита

- Обнаружение аномалий в протоколах, использование уязвимостей и соответствующих угроз

## IPS
- Easy to apply relevant rules by searching for CVEs/Keywords
- Virtual IPS: up to 256 Profiles

## Visibility
- Asset identification
- IT and OT network protocols (including SECS/GEM and Interface-A)

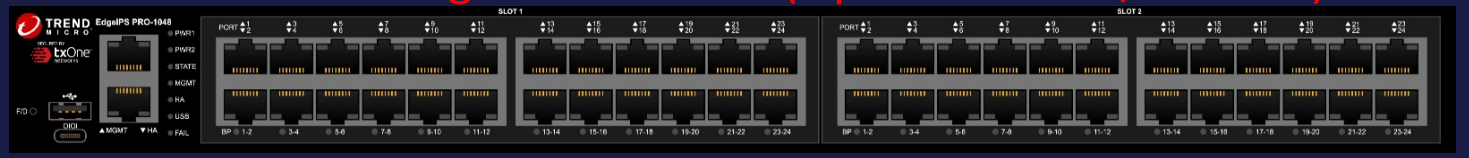
## Firewall
- Support 50, 000/100,000 Stateful ACL Rules

## Anti-Virus
- Detect and Block worm attack
- PE file and Fie extension filter
- Integration with Trend Micro DDAN to detect unknown malwares

## Others
- Xflow (Netflow) export
- API integration with existed system

## Hardware
- Flexible Port Configuration
  (by 24-port Expansion Cards)
- Gen3 hardware bypass

# SKU-1 : EdgeIPS Pro 1048 (Up to 48 Ports /24 Pairs)




# SKU-2 : EdgeIPS Pro 2096 (Up to 96 Ports /48 Pairs)


## Hardware

1. 2U Rack mount(EdgeIPS Pro-2096)
2. 1U Rack mount(EdgeIPS Pro-1048)

2. Redundant PSU

3. Up to 48 Ports 10/100/1G Interfaces (EdgeIPS Pro-1048)

4. Up to 96 Ports 10/100/1G interfaces (EdgeIPS Pro-2096)

5. 1x USB ports, 1*Serial Console(USB Type-C), 1*MGMT port, and 1* HA port

6. High flexibility interface slot exchange (Expansion Card slot)

## Performance

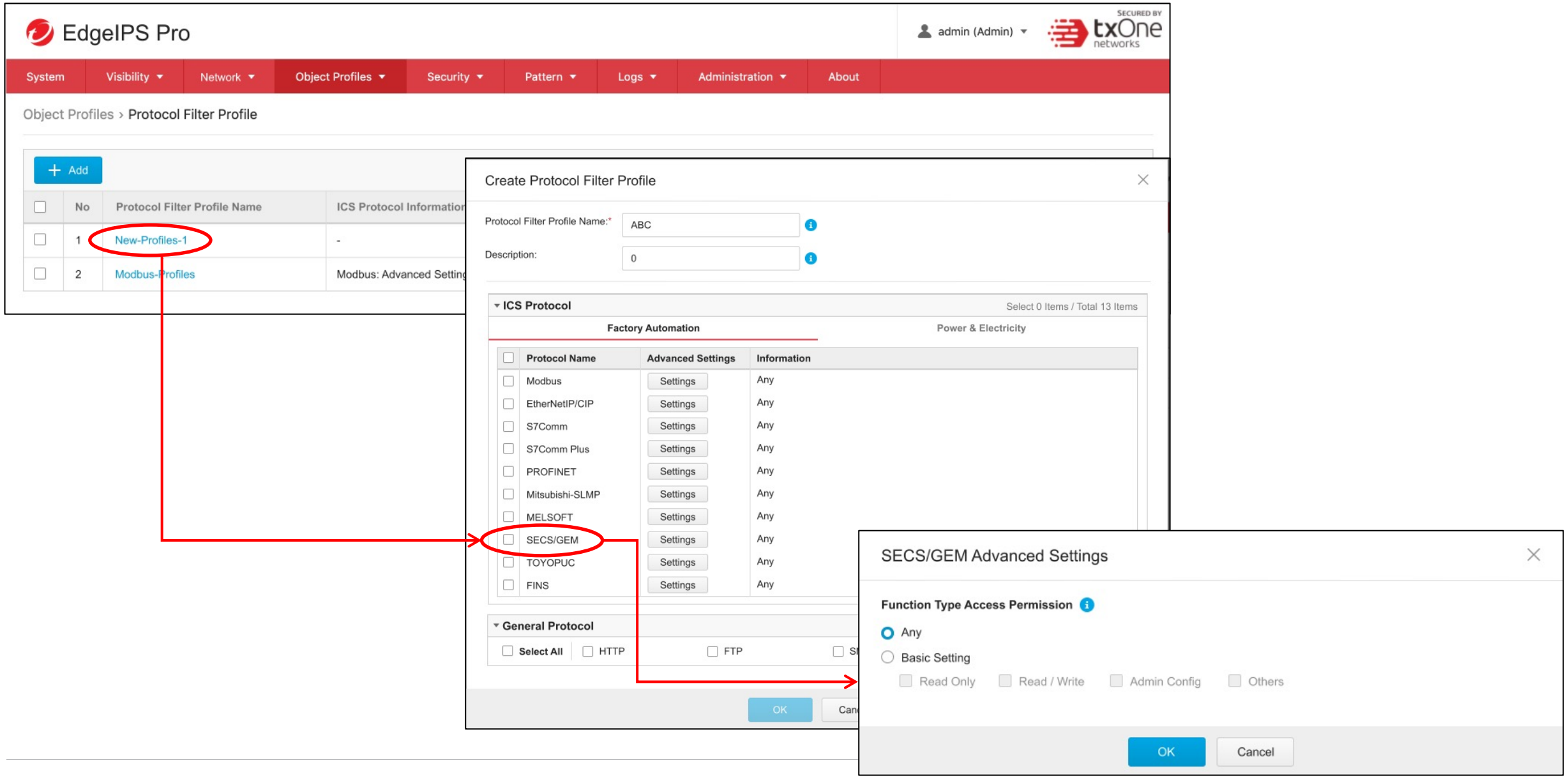
1. High throughput :
   - 10Gbps+ IPS throughput (EdgeIPS Pro-1048)
   - 20Gbps+ IPS throughput (EdgeIPS Pro-2096)

2. Low Latency : <200 microsecond

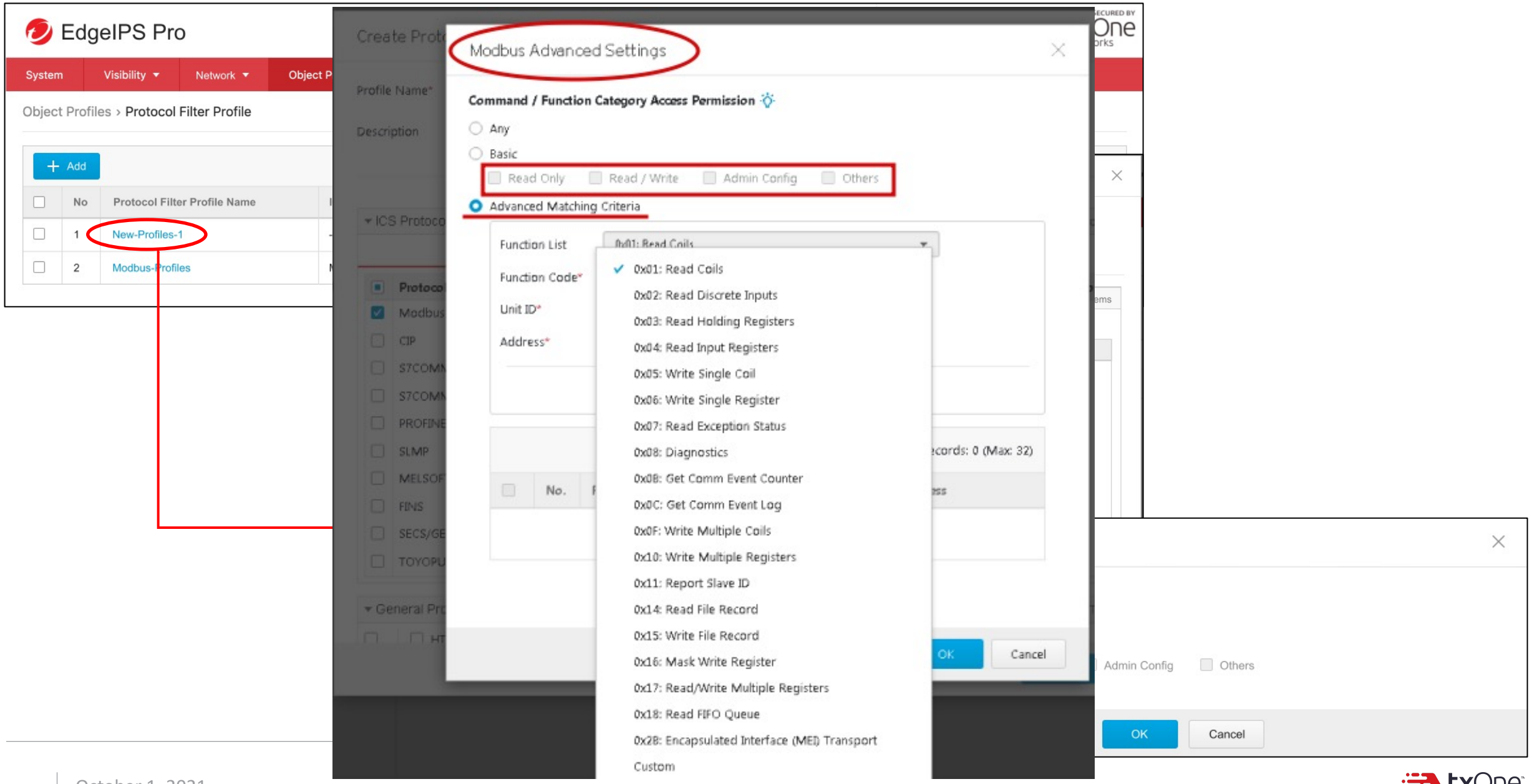
3. Concurrent connection
   support 2M+ sessions (EdgeIPS Pro-1048)
   support 4M+ sessions (EdgeIPS Pro-2096)

TREND MICRO
txOne networks

# EdgeIPS Pro-1048 – Protocol Filter Profile(SECS/GEM Setting)

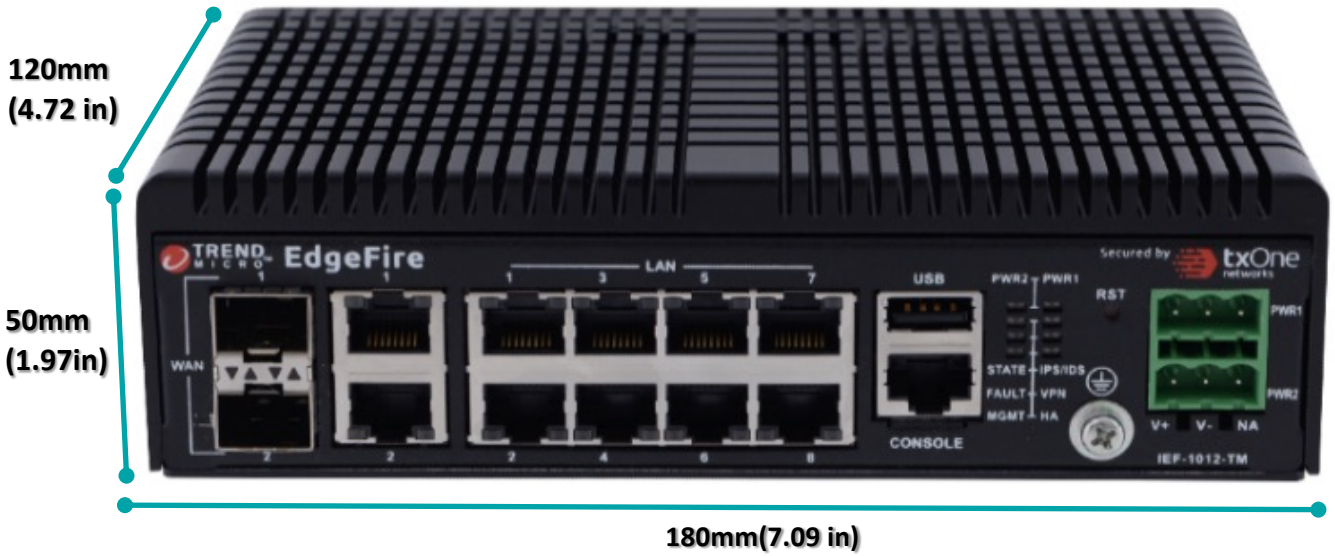


# EdgeIPS Pro-1048 – Protocol Filter Profile(SECS/GEM Setting)



# EdgeFire Series: Industrial Next-Generation Firewall

***L2-L7 Visibility and Protection***




Network visibility

Network Segmentation

OT Protocol Filter

NAT-Firewall

Virtual Patch

TXODI inside

Product name : EdgeFire
Short name : IEF
Model name : IEF-1012-TM

*Wide Temperature (−40℃ to 75℃)
(2Fiber + 8 Copper + USB)

## Интегрированный NAT и коммутатор

- Позволяет сегментировать сеть и защищать устройства в подсетях
  - Настраиваемая маршрутизация и проброс портов

## Обеспечивает интеграцию IT-OT

- Обеспечивает видимость и контроль OT процессов, а также применяет правила взаимодействия на уровнях IT и OT
  - Правила фильтрации настраиваются на основе профилей

## Прост в управлении

- Централизированное управление через OT Defense Console (ODC)
- Управление отдельным устройством через веб-консоль

## Высокая надежность

- High MTBF
- -40 to 75°C wide temperature operation
- 5-year warranty
- Industrial grade hardware design

# Защита конечных точек в средах OT с помощью TxOne Stellar

## StellarProtect

- Видимость OT активов
- Безопасность ICS приложений
- OT Zero Trust и детектирование аномалий

- Фиксация 4 в 1
- Сканирование по запросу

## StellarEnforce

**Современные хосты**

- Более мощное
- Ограниченные обновления
- Использует интеллектуальные функции

**Устаревшие хосты**

- Менее мощное
- Устаревшие ОС
- Предпочтителен режим фиксации состояния

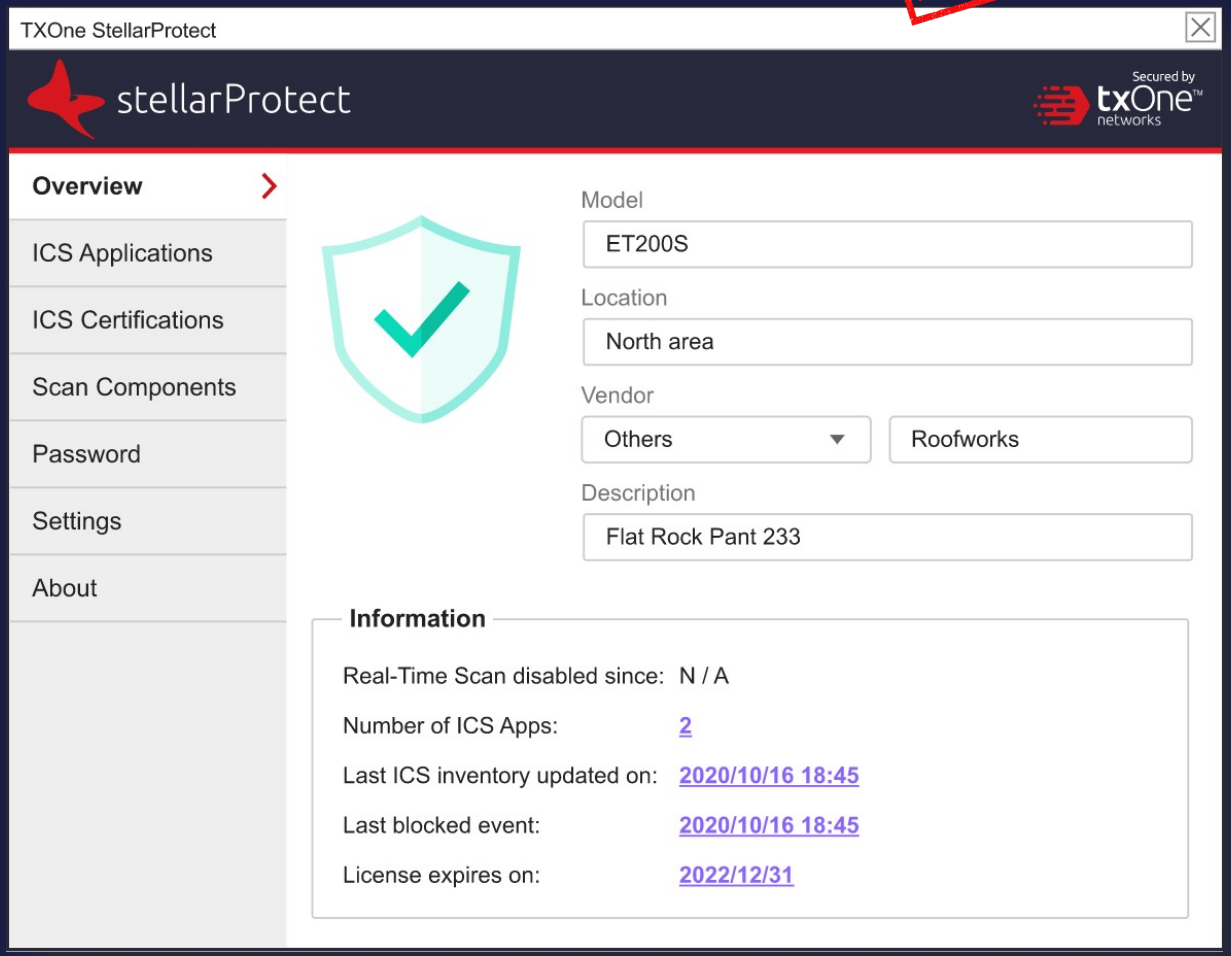
- **Pattern-Less**
- **Lightweight**
- **Patch-Free**
- **Support XP/2000**

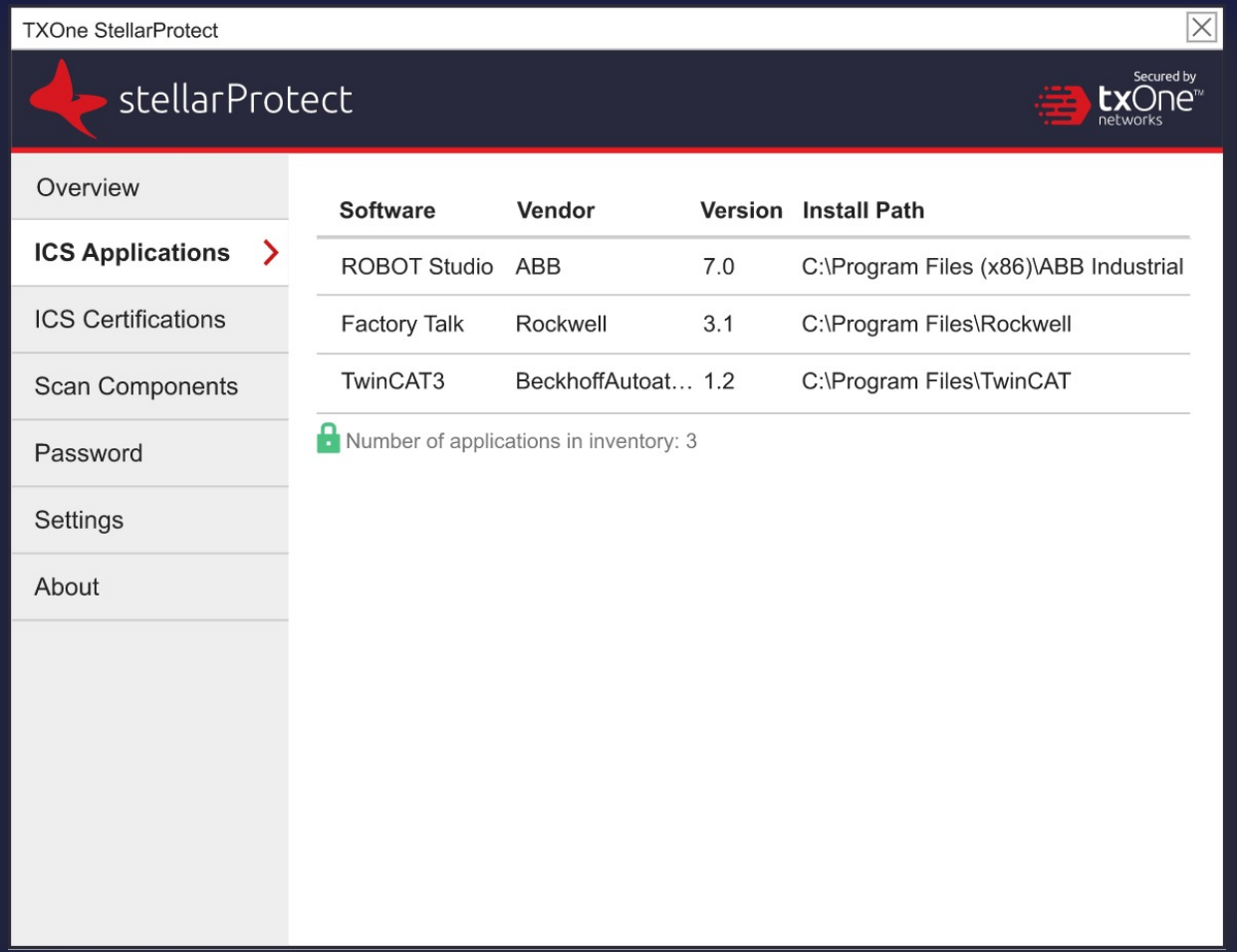

stellarProtect

# StellarProtect – Инвентаризация АСУ ТП (приложения/сертификаты)

PRIORITY

## “Обеспечение беспрерывной работы”

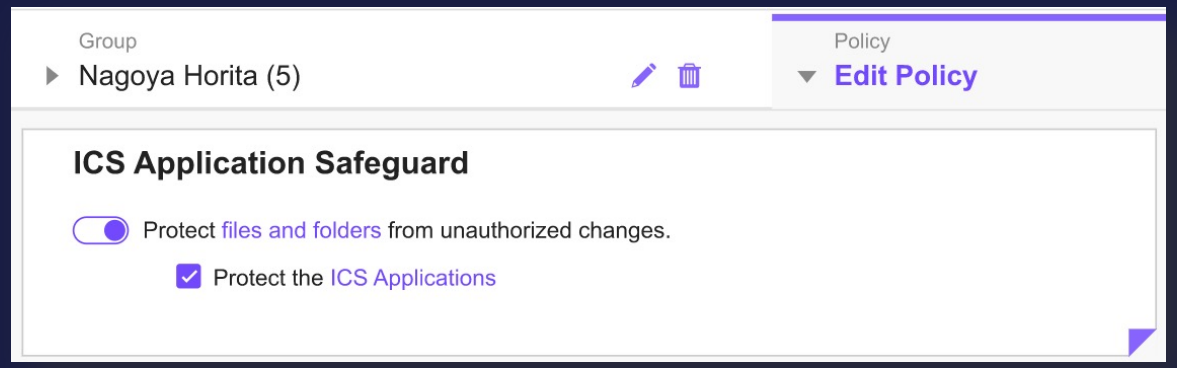


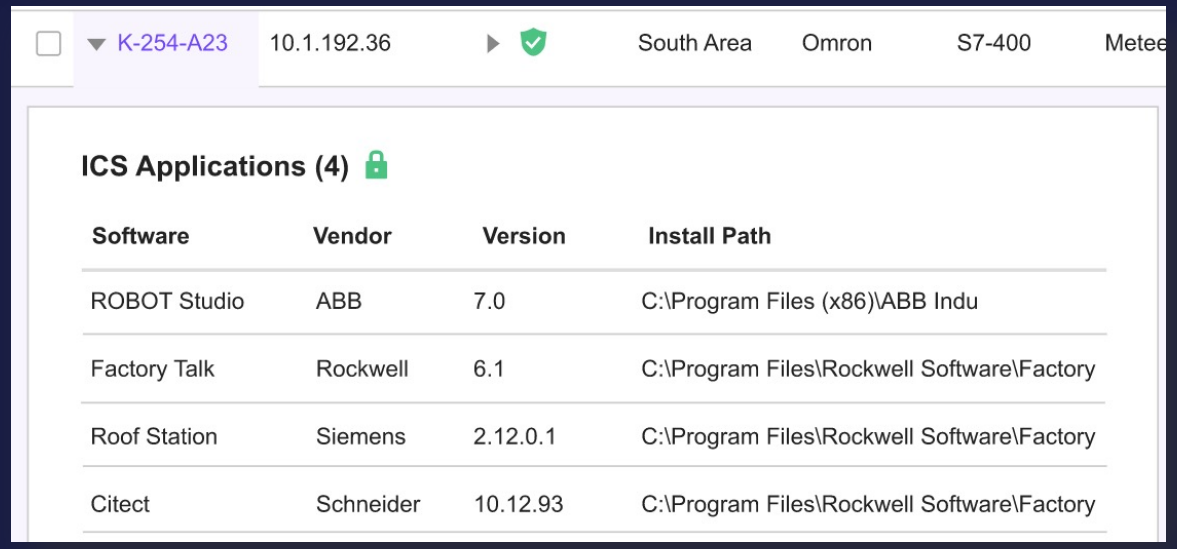




TREND MICRO txOne networks

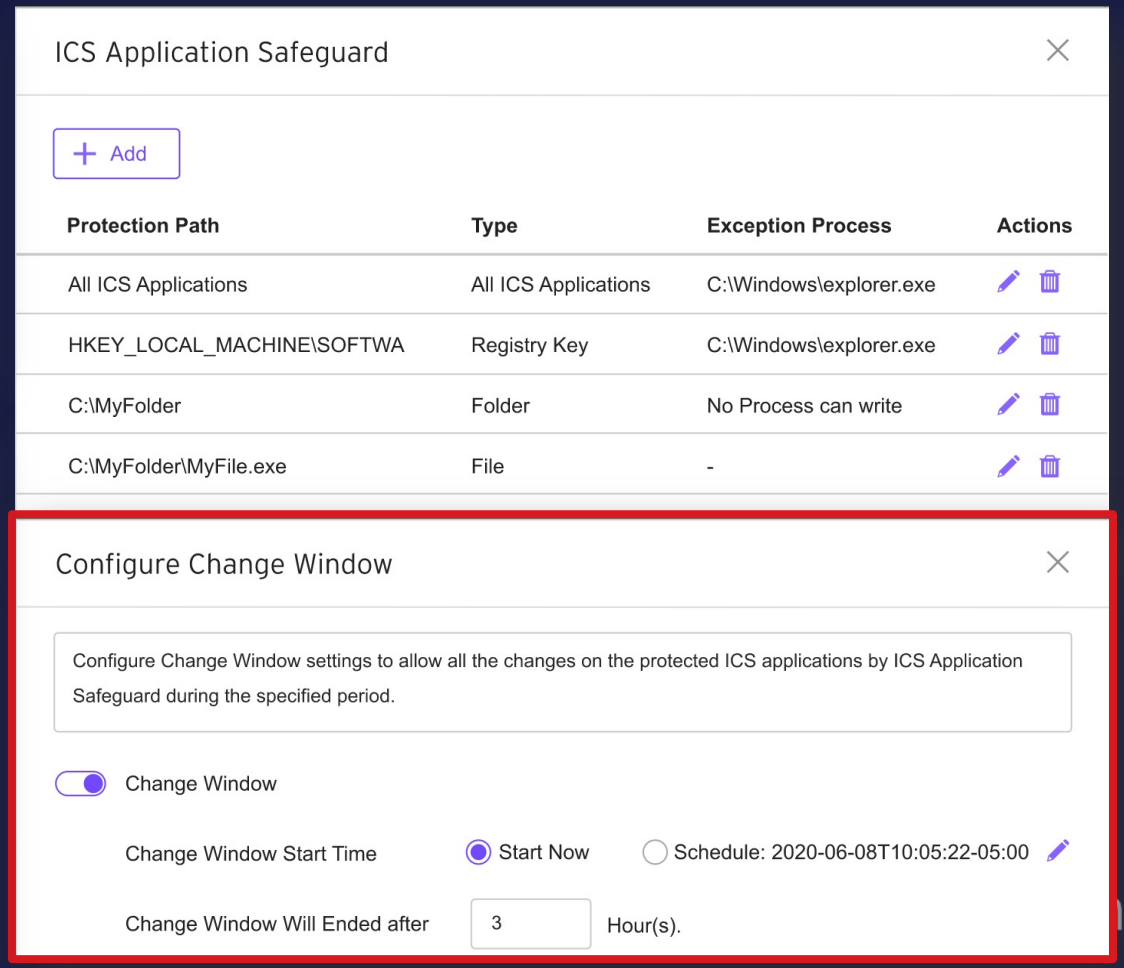
# Безопасность приложений АСУ ТП

## Защита приложений




## Защита файлов и папок



# АСУ ТП Управление приложениями/сертификатами

Group
Nagoya Horita (5)

Policy
Edit Policy

| Endpoint | IP Address | Protected | Location | Vendor | Model | Description | Operation System | Last Connection |
|---|---|---|---|---|---|---|---|---|
| K-100 | 10.1.193.192 | | North Area | SIEMENS | ET200S | Flat Rock Plant | Windows XP Professional Service Pack 3 build 26e… | 2020-08-13T11:31:15+08:00 |
| K-101 | 10.1.192.33 | | North Area | SIEMENS | Sinumerk | Consulting | Windows 7 Starter Edition build 7601 | 2020-08-13T11:31:15+08:00 |
| K-254-A23 | 10.1.192.36 | | South Area | Omron | S7-400 | Meteer | Windows 7 Starter Edition build 7601 | 2020-08-13T11:31:15+08:00 |

### ICS Applications (4)

| Software | Vendor | Version | Install Path |
|---|---|---|---|
| ROBOT Studio | ABB | 7.0 | C:\Program Files (x86)\ABB Indu |
| Factory Talk | Rockwell | 6.1 | C:\Program Files\Rockwell Software\Factory |
| Roof Station | Siemens | 2.12.0.1 | C:\Program Files\Rockwell Software\Factory |
| Citect | Schneider | 10.12.93 | C:\Program Files\Rockwell Software\Factory |

### ICS Certifications (20)

| Issued To | Issued By | Type | Hash |
|---|---|---|---|
| Schneider Electric | DigiCert SHA2 Secure | EE | 564e01066387f26c9120d78d37 |
| SIEMENS AG | Symantec Class 3 SHA256 | EE | Da39a3ee5e6b4b0d325501890 |
| DigiCert Glocal | DigiCert Glocal Root CA | CA | E0c9035898dd52fc65c49c4d20 |
| Schneider Electric | DigiCert SHA2 Secure | CA | 564e01066387f26c9120d78d37 |
| SIEMENS AG | Symantec Class 3 SHA256 | EE | Da39a3ee5e6b4b0d325501890 |

› Show All and Edit

### System Info

| | |
|---|---|
| Operating System | Microsoft Windows 7 Professional Service Pack 1 build 7601, 64-bit |
| Group | Root group\testTC |
| License Status | VALID |

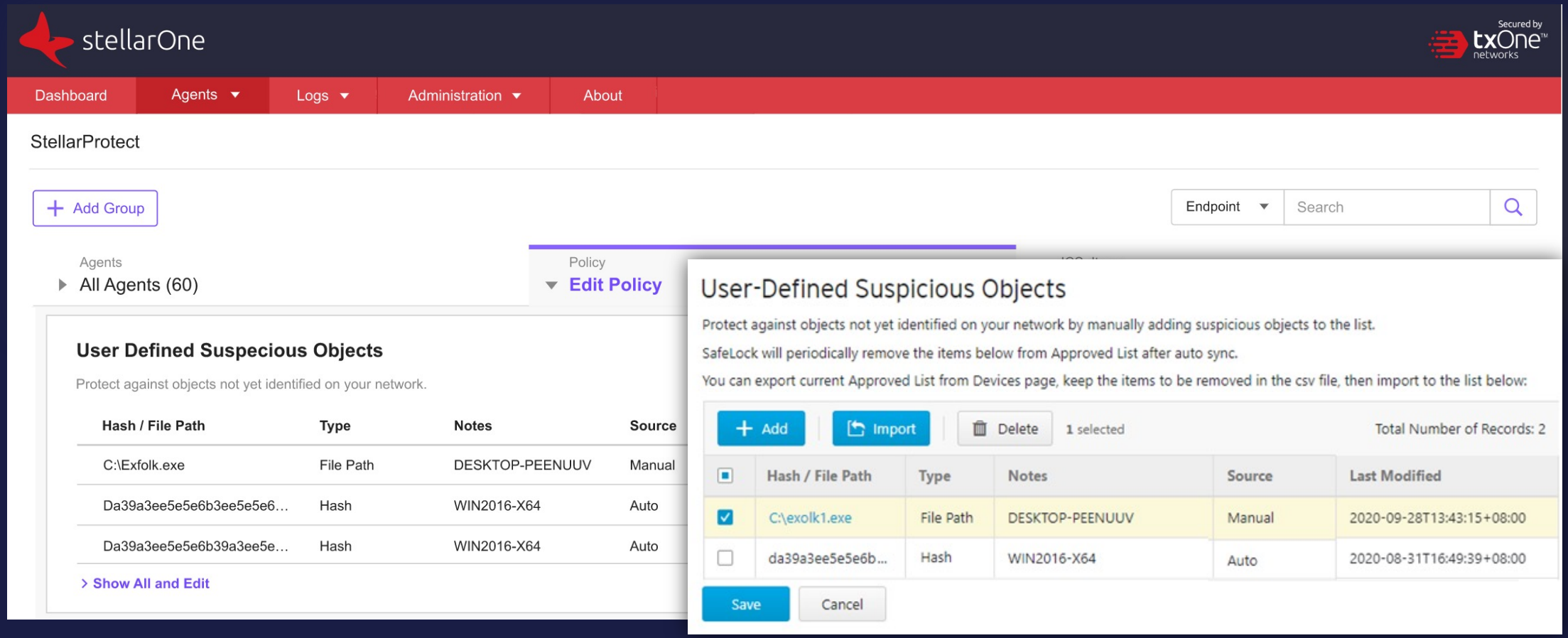
### Scan Components

⚠ Scan Components are older than OT Defense Console.

| | |
|---|---|
| Virus Pattern | 16.219.00 |
| Spyware Pattern | 2.333.00 |
| Digital Signature Pattern | 1.780.00 |

TREND MICRO
txOne networks

# Industrial-Grade NGAV – Обмен данными об IoC

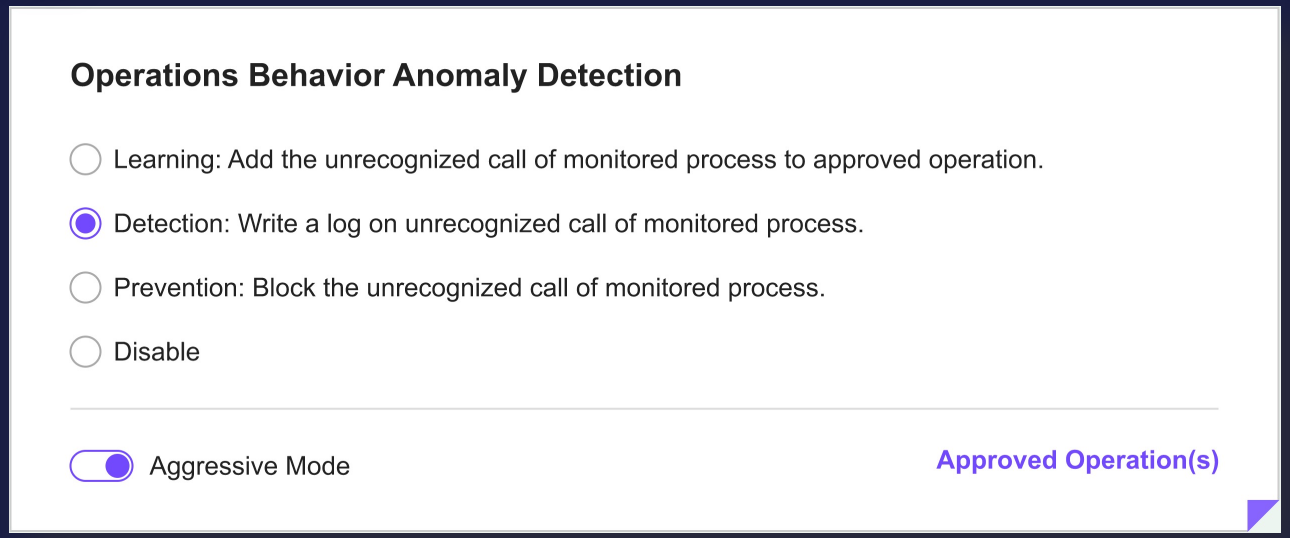


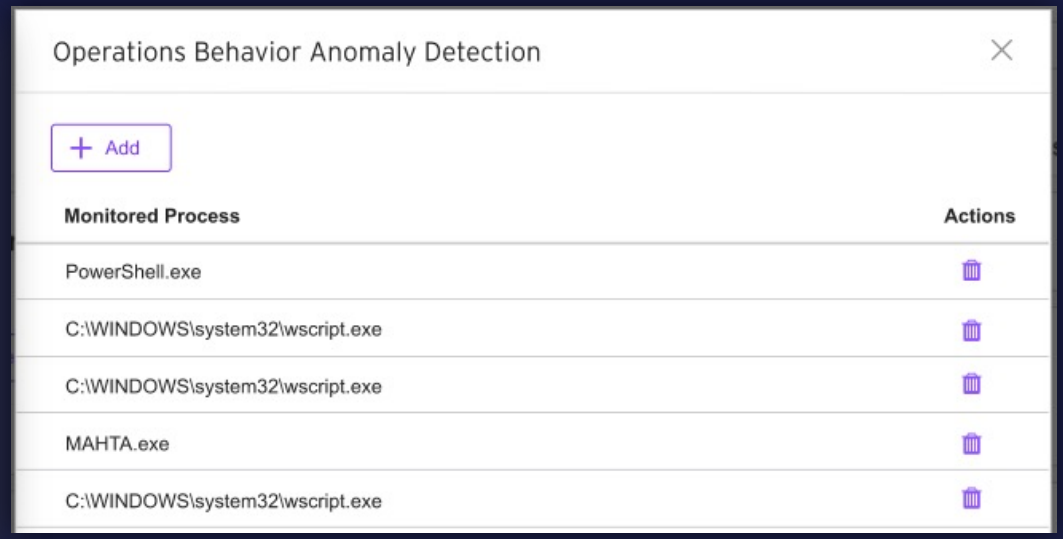

## Интеграция со сторонними решениями по обмену IoC

TREND MICRO
txOne networks

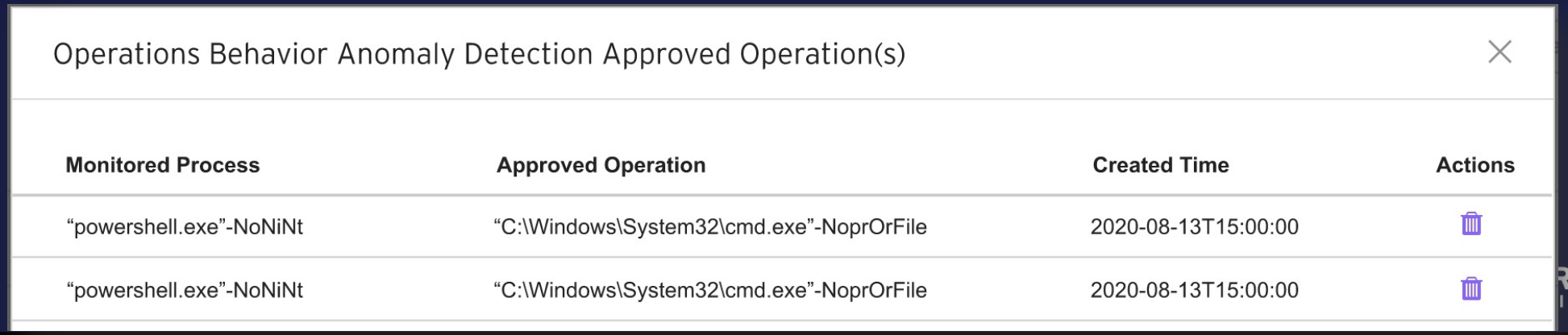
# Определение аномального поведения – OT Zero Trust

## Мониторинг уязвимого легитимного процесса с минимальным контролем привилегий



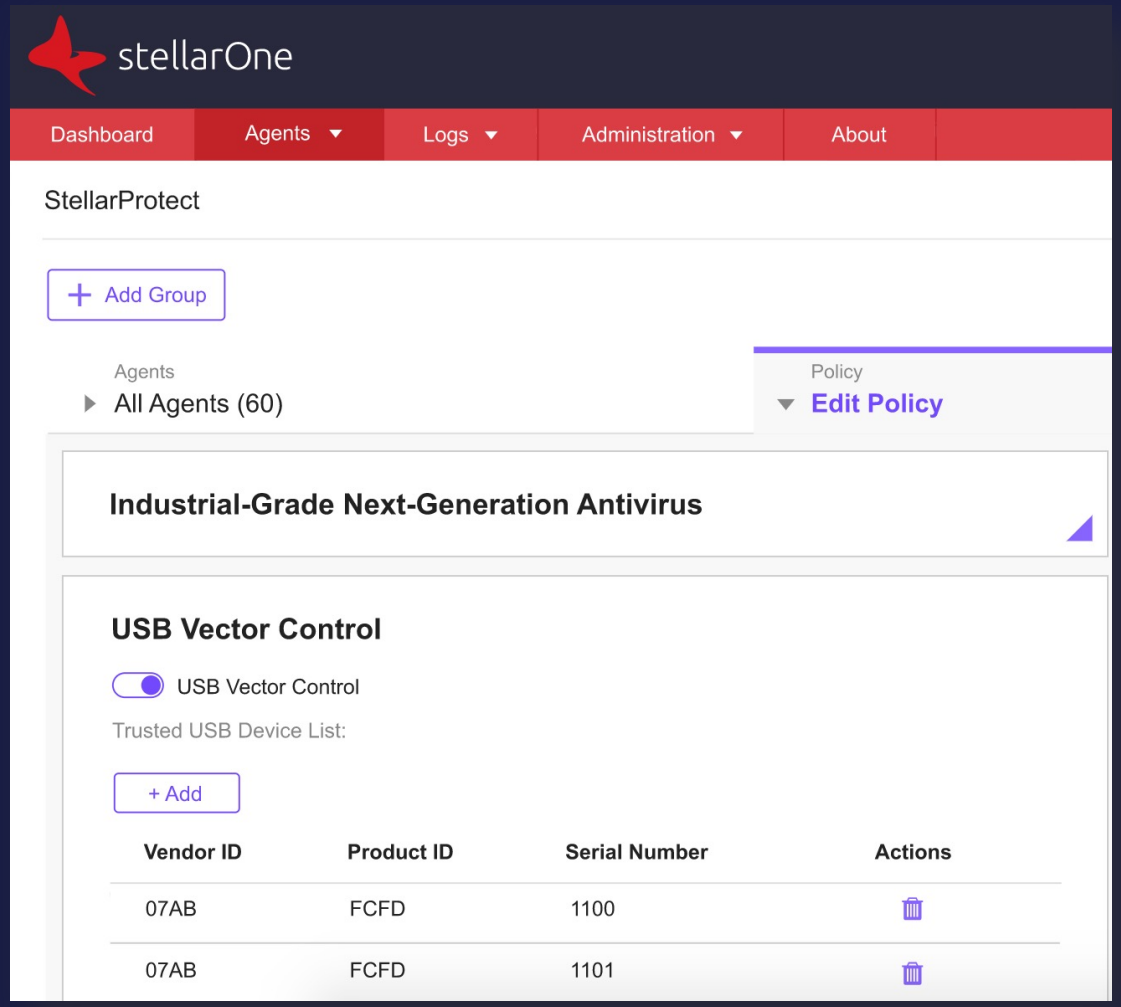




## Изучение и авторизация операционного поведения

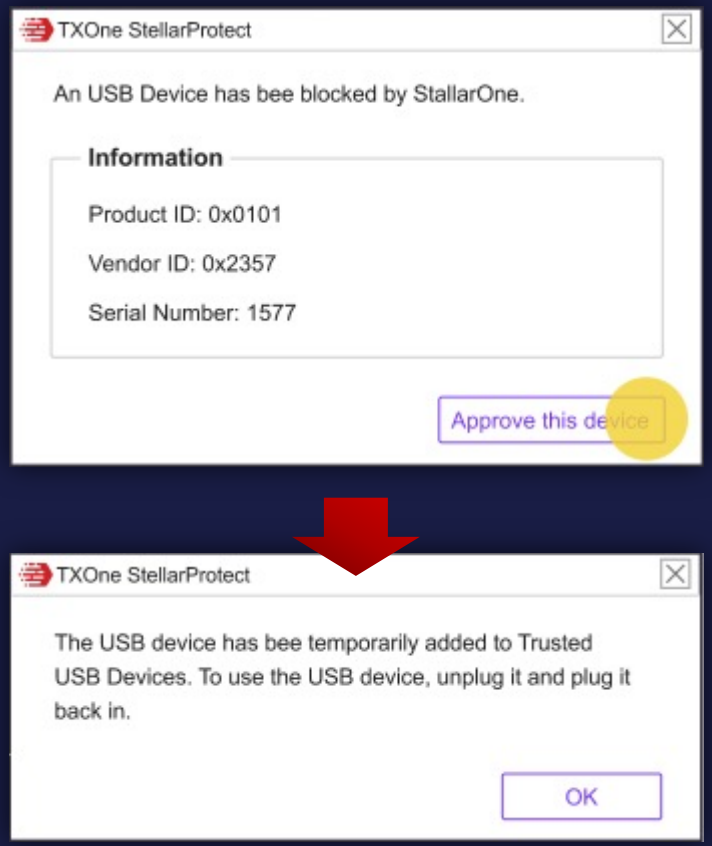


# Контроль USB устройств

## Разрешенный список




## Единоразовое использование



stellarEnforce

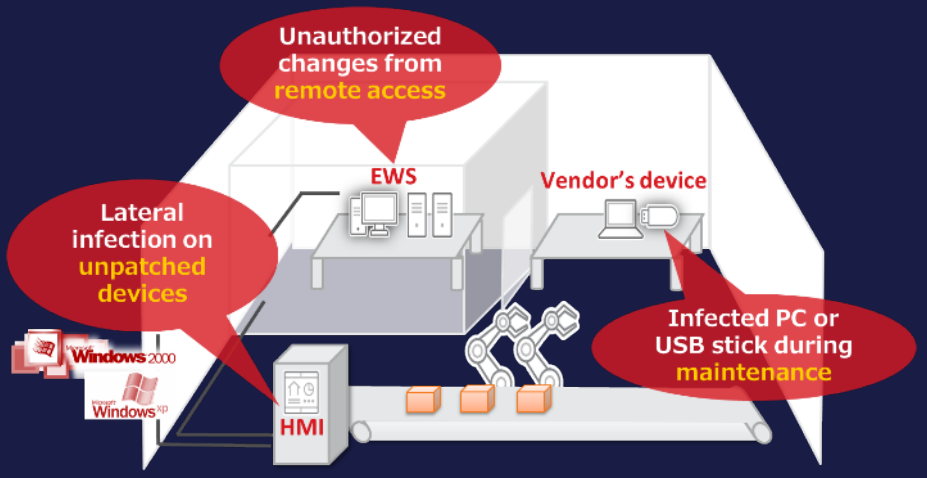
txOne networks

# StellarEnforce

Обеспечивает операционную целостность устаревших платформ с помощью блокировки и контроля изменений

*Реальность в устаревшем OT*

Практически нет окон обслуживания




Антивирусные системы не применимы

## Режим фиксации (Lockdown) 4 в 1

**Обеспечивает эксплуатационную целостность критически важных устройств**

| Operations Lockdown | USB Device Lockdown | Data Lockdown | Configuration Lockdown |
|---|---|---|---|

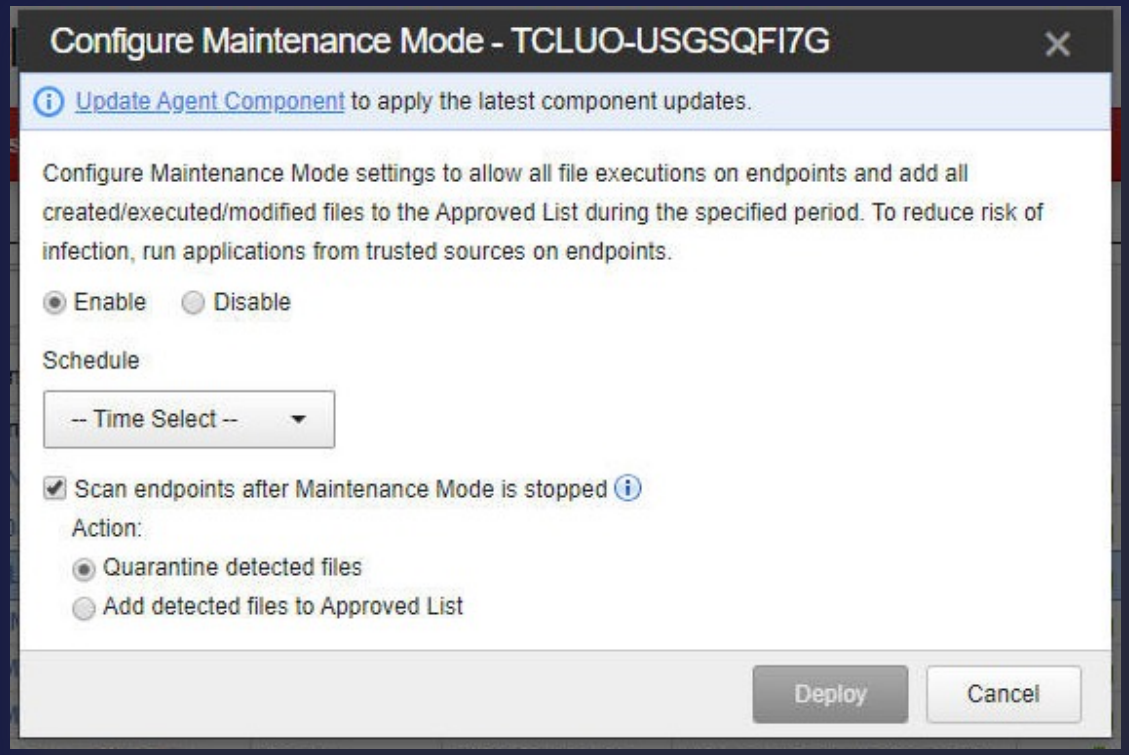
- **Patch-Free**
- **Support XP/2000**
- **Pattern-Less**
- **Lightweight**

TREND MICRO™ txOne networks™

# StellarEnforce – Простота обслуживания хостов

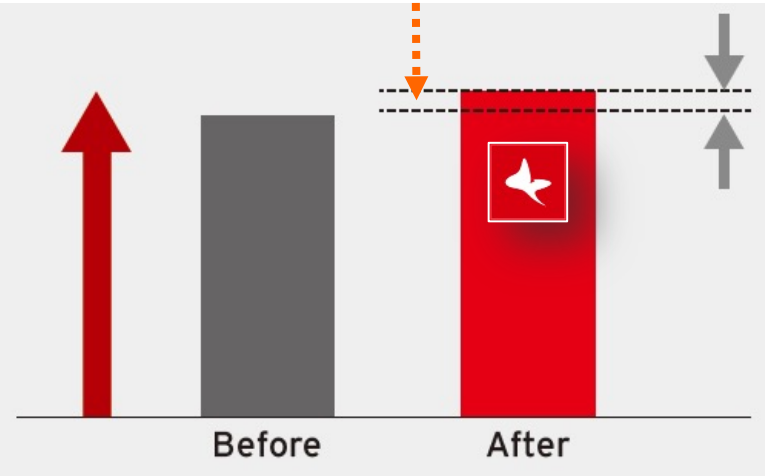
Пользователи могут запланировать окно изменения для автоматического обновления утвержденного списка.

- Начало / конец окна обслуживания
- Сканирование вредоносных программ во время обслуживания
- Отправка в карантин обнаруженных объектов



# StellarEnforce – Минимальное влияние на производительность

**Нагрузка на CPU < 1%**
**Усредненное использование ОЗУ < 10MB**



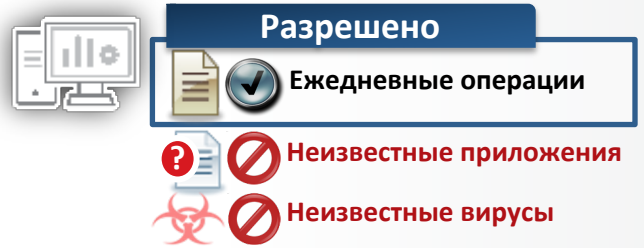

Реальный пример: заказчику необходимо выполнить 40 000+ операций ввода-вывода в течение 10 секунд на своем производственном компьютере, и StellarEnforce практически не добавил задержки для этой важной задачи

# Фиксация целостности

## Операции Lockdown

Process

- Обеспечивает целостность выполнения процесса
- Поддержка устаревших ОС
- Простой режим обслуживания




## Данные Lockdown

- Защита БД / SCADA
- Предупреждение о неавторизованных изменениях и аудит целостности данных

Защита критических данных

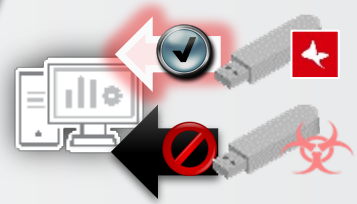
## Конфигурации Lockdown

- Повышение безопасности настроек чувствительной среды


Защита конфигураций

## USB/ приложения Lockdown

- Разрешенные устройства
- Контроль разрешенных приложений/ сертификатов



txOne networks

# Поддерживаемые ОС – StellarProtect

| | Client OS | Server OS |
|---|---|---|
| OS | Windows 7 (No SP/SP1) [Professional / Enterprise / Ultimate] (32/64bit)<br>Windows 8 (No SP) [Pro / Enterprise] (32/64bit)<br>Windows 8.1 (No SP) [Pro / Enterprise / with Bing] (32/64bit)<br>Windows 10 [Pro/Enterprise/IoT Enterprise] (32/64bit)<br>Windows Embedded Standard 7 (No SP/SP1) (32/64bit)<br>Windows Embedded 8 Standard (No SP) (32/64bit)<br>Windows Embedded 8.1 (No SP) [Pro / Industry Pro] (32/64bit)<br>Windows 7 for Embedded Systems (No SP/SP1) (32/64bit)<br>Windows Embedded POSReady 7 (32/64bit) | Windows Server 2008 (SP1/SP2) [Standard / Enterprise / Storage] (32/64bit)<br>Windows Server 2008 R2 (No SP/SP1) [Standard / Enterprise / Storage] (64bit)<br>Windows Server 2012 (No SP) [Essentials/Standard] (64bit)<br>Windows Server 2012 R2 (No SP) [Essentials/Standard] (64bit)<br>Windows Server 2008 for Embedded Systems (SP1/SP2) (32/64bit)<br>Windows Server 2008 R2 for Embedded Systems (No SP/SP1) (64bit)<br>Windows Server 2012 for Embedded Systems (No SP) (64bit)<br>Windows Server 2012 R2 for Embedded Systems (No SP) (64bit)<br>Windows Server 2016 (No SP) [Standard] (No SP) (64bit)<br>Windows Storage Server 2016 (64bit)<br>Windows Server 2019 Standard (64bit) |

TREND MICRO™ txOne networks™

# Поддерживаемые ОС – StellarEnforce

| | Client OS | Server OS |
|---|---|---|
| OS | Windows 2000 (SP4) [Professional] (32bit)<br>Windows XP (SP1/SP2/SP3) [Professional] (32bit)<br>Windows Vista (No SP/SP1/SP2) [Business / Enterprise / Ultimate] (32bit)<br>Windows 7 (No SP/SP1) [Professional / Enterprise / Ultimate] (32/64bit)<br>Windows 8 (No SP) [Pro / Enterprise] (32/64bit)<br>Windows 8.1 (No SP) [Pro / Enterprise / with Bing] (32/64bit)<br>Windows 10 (RS1/RS2/RS3/RS4/RS5) [Pro/Enterprise/IoT Enterprise] (32/64bit)<br>Windows XP Embedded (SP1/SP2) (32bit)<br>Windows Embedded Standard 2009 (No SP) (32bit)<br>Windows Embedded Standard 7 (No SP/SP1) (32/64bit)<br>Windows Embedded 8 Standard (No SP) (32/64bit)<br>Windows Embedded 8.1 (No SP) [Pro / Industry Pro] (32/64bit)<br>Windows XP Professional for Embedded Systems (SP1/SP2/SP3) (32bit)<br>Windows Vista for Embedded Systems (No SP/SP1/SP2) (32bit)<br>Windows 7 for Embedded Systems (No SP/SP1) (32/64bit)<br>Windows Embedded POSReady (32bit)<br>Windows Embedded POSReady 2009 (32bit)<br>Windows Embedded POSReady 7 (32/64bit) | Windows 2000 Server (SP4) (32bit)<br>Windows Server 2003 (SP1/SP2) [Standard / Enterprise / Storage] (32bit)<br>Windows Server 2003 R2 (No SP/SP1/SP2) [Standard / Enterprise / Storage] (32bit)<br>Windows Server 2008 (SP1/SP2) [Standard / Enterprise / Storage] (32/64bit)<br>Windows Server 2008 R2 (No SP/SP1) [Standard / Enterprise / Storage] (64bit)<br>Windows Server 2012 (No SP) [Essentials/Standard] (64bit)<br>Windows Server 2012 R2 (No SP) [Essentials/Standard] (64bit)<br>Windows Server 2003 for Embedded Systems (SP1/SP2) (32bit)<br>Windows Server 2003 R2 for Embedded Systems (No SP/SP1/SP2) (32bit)<br>Windows Server 2008 for Embedded Systems (SP1/SP2) (32/64bit)<br>Windows Server 2008 R2 for Embedded Systems (No SP/SP1) (64bit)<br>Windows Server 2012 for Embedded Systems (No SP) (64bit)<br>Windows Server 2012 R2 for Embedded Systems (No SP) (64bit)<br>Windows Server 2016 (No SP) [Standard] (No SP) (64bit)<br>Windows Storage Server 2016 (64bit)<br>Windows Server 2019 Standard (64bit) |
| CPU | Equivalent to minimum system requirements of operating system (only Intel 64 and 32 Architectures supported) | |
| Memory | Equivalent to minimum system requirements of operating system | |
| Free HDD space | Minimum 300MB | |

TREND MICRO™ txOne networks™