

Przemysłowy antywirus dla Energetyki – możliwości i zastosowanie

Mirosław Zwierzyński

Email: miroslaw.zwierzynski@elmark.com.pl



Elmark Automatyka w pigułce



Siedziba w Warszawie

Rok założenia **1983**



Jeden z największych
dystrybutorów w Europie:

Advantech, Getac, MOXA, Unitronics,
Universal Robots

Wieloletni sprawdzony
partner polskiego przemysłu



Zatrudnienie ponad **70**
wykwalifikowanych pracowników

Przeszkolonych osób **>1500**



Roczny obrót **140 M PLN**

Liczba zamówień rocznie ponad **25.000**

Wartość magazynu ponad **35 M PLN**

Stabilna sytuacja finansowa



Przemysłowa komunikacja i Cyberbezpieczeństwo



Obszary działania:

- **Kompletna infrastruktura komunikacyjna dla OT**
- **Rozwiązania do budowa przemysłowych sieci Ethernet**
- **Wykorzystanie IEC 62443 w budowie sieci**
- **Segmentacja sieci**
- **Ochrona assetów na poziomie sieciowym z wykorzystaniem systemów IPS**
- **Ochrona assetów końcowych opartych o systemy Windows**
- **Inspekcja assetów opartych o systemy Windows**



Przemysłowa komunikacja i Cyberbezpieczeństwo

Nasi partnerzy



MOXA[®]



txOne
networks



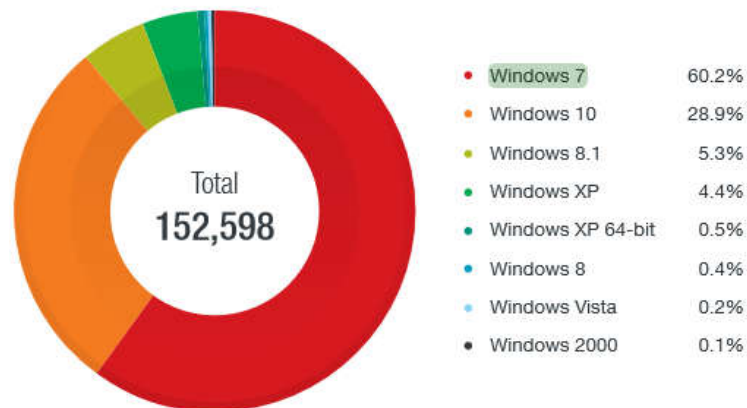
Systemy operacyjne w aplikacjach OT

Systemy Windows w środowiskach przemysłowych



Systemy operacyjne Windows w środowiskach przemysłowych (dane z 2020 roku)

Starsze wersje Windows dalej mają znaczący udział



Źródło:

Trend micro securing smart factories threats to manufacturing environments in the era of industry 4.0
https://documents.trendmicro.com/assets/white_papers/wp-threats-to-manufacturing-environments-in-the-era-of-industry-4.pdf

50% użytkowników ma zaimplementowany antywirus w środowisku OT

Na bazie odpowiedzi około 500 respondentów – właścicieli fabryk



Źródło

The State of Industrial Cybersecurity
Converging IT and OT with people, process, and technology
https://resources.trendmicro.com/rs/945-CXD-062/images/WP00_State_Industrial_Cybersecurity_White_Paper_210319US_web.pdf

Jakie widzimy potrzeby i wyzwania?



- Brak pełnej wiedzy o stanie, statusach oraz wykorzystaniu posiadanych komputerów w obszarze OT
- Brak pełnej kontroli nad działaniami użytkowników
- Ryzyko nieautoryzowanego wykorzystania fizycznych portów
- Nieświadoma ingerencja w pliki systemowe oraz aplikacji
- Ryzyko transferu niebezpiecznego oprogramowania przez „zewnętrznych” użytkowników
- Brak dedykowanych narzędzi do realizacji polityk bezpieczeństwa

Zabezpieczenie stacji inżynierskich i komputerów przemysłowych przed nieautoryzowanym oprogramowaniem oraz łatwe monitorowanie ich wykorzystania

Istniejące rozwiązania vs wymagania OT

Po prostu nie pasują -
rozwiązania IT nie biorą pod
uwagę trudnych warunków w
sieciach OT:

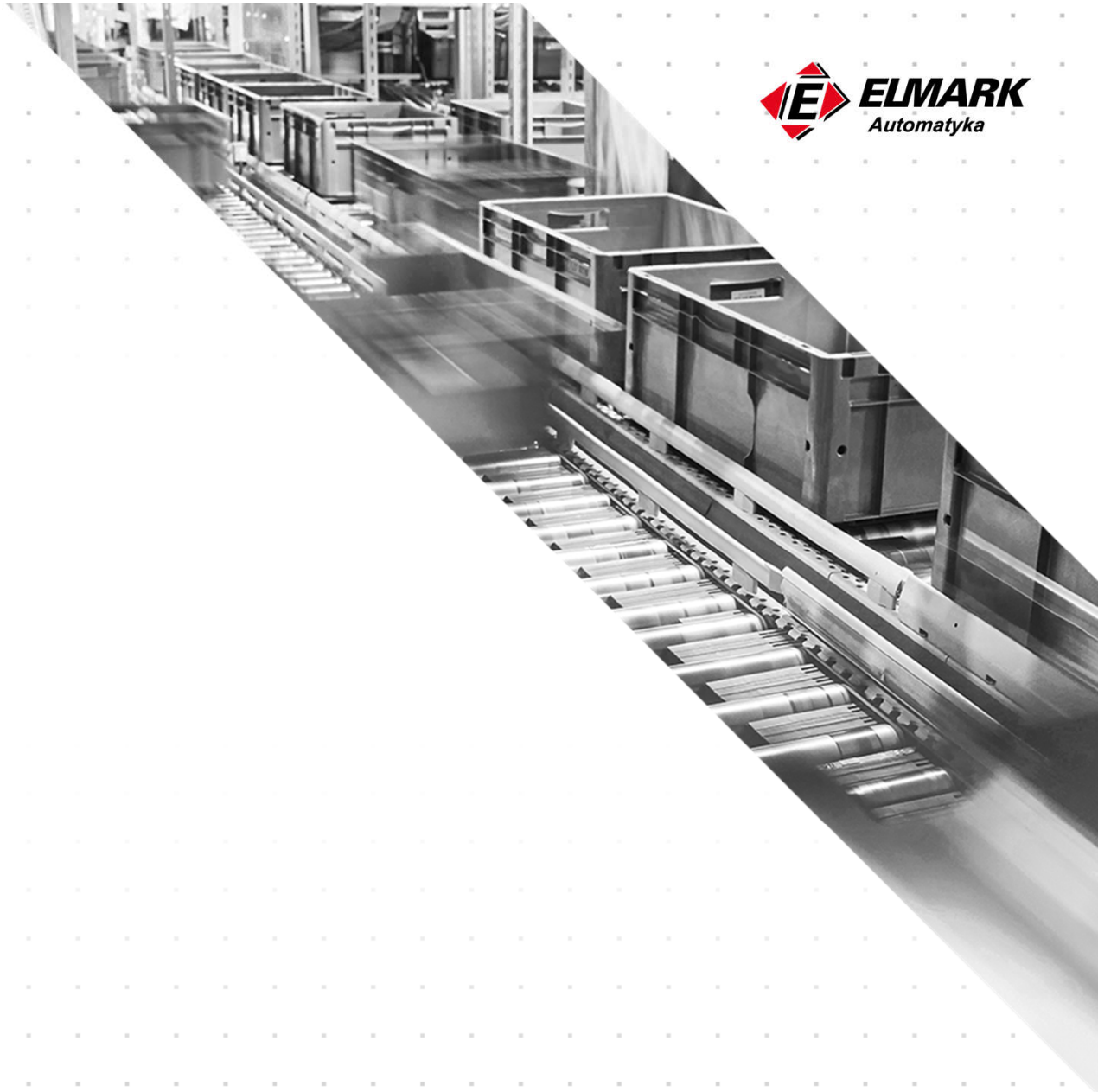
- Mała tolerancja na opóźnienia sieci
- Przeszarżałe systemy operacyjne (brak wsparcia dla starszego systemu niż Windows 7)
- Ograniczone zasoby obliczeniowe – min. Wymaganie na 1 GB RAM
- Brak internetu = nie da się pobrać aktualizacji sygnatur

Istotne ograniczenia – brak
informacji na temat środowisk
przemysłowych w rozwiązaniach
bezpieczeństwa IT

- Różne protokoły sieciowe
- Aplikacje od różnych dostawców
- Podatności specyficzne dla OT
- Taktyki i techniki atakujących stosowane w OT

Sama widoczność nie jest
wystarczająca – brak osób
odpowiedzialnych za
bezpieczeństwo OT

- Zmęczenie ilością zdarzeń
- Potrzeba technik blokujących 99% znanych zagrożeń



TXOne Stellar





TXOne Stellar



**Przemysłowy antywirus
nowej generacji**

**Ochrona aplikacji
przemysłowych**

**Inteligentne
wykrywanie anomalii**

**Blokowanie
niezauważanych procesów**

**Kontrola
portów USB**



**Zaawansowane
skanowanie w
poszukiwaniu zagrożeń
zabezpiecza zasoby OT bez
przerywania pracy**

**Wykrywanie i
rozpoznawanie aplikacji
ICS/OT oraz ich ochrona**

**Wykrywanie
nieprawidłowych
operacji, które nie pasują
do wzorca zachowania
użytkownika**

**Tylko zaufane i
zatwierdzone procesy
mogą być uruchamiane
przez użytkownika oraz
inne aplikacje**

**Zapobieganie
zagrożeniom
wewnętrznym i
szkodliwym działaniom**

Stellar Protect – lekki agent na systemy Windows



The screenshot displays the TXOne StellarProtect application window. The interface includes a sidebar with navigation options: Overview, OT Applications, OT Certificatee, Approved List, Scan Components, Password, Settings, and About. The main content area features a large green checkmark icon and the text "Your device is under protection." Below this, there are two status indicators: "Real-Time Malware Scan" and "Application Lockdown (Enforce)", both with active toggle switches and timestamps from 2022-05-11T12:29:21. An "Information" section provides details about the StellarOne registration, including the group name "Asia & Pacific", 4 OT Apps, and various update timestamps. A "Device Information" link is also present.

OT EDR+

Next-gen AV

Lockdown

Device control

Support legacy

Stellar Protect – systemy operacyjne



Wspierane systemy operacyjne

OS	Client OS	Server OS
	<ul style="list-style-type: none"> - Windows 2000 (SP4) [Professional] (32bit) - Windows XP (SP1/SP2/SP3) [Professional/Professional for Embedded Systems] (32bit) - Windows Vista (NoSP/SP1/SP2) [Business/Enterprise/Ultimate] (32bit) - Windows 7 (NoSP/SP1) [Professional/Enterprise/Ultimate/Professional for Embedded Systems/Ultimate for Embedded Systems] (32/64bit) - Windows 8 (NoSP) [Pro/Enterprise] (32/64bit) - Windows 8.1 (NoSP) [Pro/Enterprise/with Bing] (32/64bit) - Windows 10 [Pro/Enterprise/IoT Enterprise] (32/64bit) Anniversary Update, Creators Update, Fall Creators Update, April 2018 Update, October 2018 Update*, May 2019 Update, November 2019 Update, May 2020 Update, October 2020 Update, May 2021 Update, November 2021 Update, 2022 Update - Windows 11 (NoSP) [Pro/Enterprise] (64bit) 2022 Update - Windows XP Embedded (SP1/SP2) (32bit) - Windows Embedded Standard 2009 (NoSP) (32bit) - Windows Embedded POSReady 2009 (32bit) - Windows Vista for Embedded Systems (NoSP/SP1/SP2) (32bit) - Windows Embedded Standard 7 (NoSP/SP1) (32/64bit) - Windows Embedded POSReady 7 (NoSP) (32/64bit) - Windows Embedded 8 Standard (NoSP) (32/64bit) - Windows Embedded 8 Industry (NoSP) [Pro/Enterprise] (32/64bit) - Windows Embedded 8.1 Industry (NoSP) [Pro/Enterprise/Sideload] (32/64bit) - Windows Embedded POSReady (32bit) 	<ul style="list-style-type: none"> - Windows 2000 Server (SP4) (32bit) - Windows Server 2003 (SP1/SP2) [Standard/Enterprise/Storage] (32bit) - Windows Server 2003 R2 (NoSP/SP2) [Standard/Enterprise/Storage] (32bit) - Windows Server 2008 (SP1/SP2) [Standard/Enterprise/Storage] (32/64bit) - Windows Server 2008 R2 (NoSP/SP1) [Standard/Enterprise/Storage] (64bit) - Windows Server 2012 (NoSP) [Essentials/Standard] (64bit) - Windows Server 2012 R2 (NoSP) [Essentials/Standard] (64bit) - Windows Server 2016 (NoSP) [Standard] (64bit) - Windows Server 2019 (NoSP) [Standard] (64bit) - Windows Server 2022 (NoSP) [Standard] (64bit) - Windows Storage Server 2012 (NoSP) [Standard] (64-bit) - Windows Storage Server 2012 R2 (NoSP) [Standard] (64-bit) - Windows Storage Server 2016 (NoSP) (64bit) - Windows Server 2003 for Embedded Systems (SP1/SP2) (32bit) - Windows Server 2003 R2 for Embedded Systems (NoSP/SP2) (32bit) - Windows Server 2008 for Embedded Systems (SP1/SP2) (32/64bit) - Windows Server 2008 R2 for Embedded Systems (NoSP/SP1) (64bit) - Windows Server 2012 for Embedded Systems (NoSP) (64bit) - Windows Server 2012 R2 for Embedded Systems (NoSP) (64bit)
CPU	Equivalent to minimum system requirements of operating system (only Intel 64 and IA-32 Architectures supported)	
Memory	Equivalent to minimum system requirements of operating system	
Free HDD space	Minimum 300MB	

StellarOne - Wykrywanie i rozpoznawanie aplikacji ICS/OT



stellarOne zen (Admin) Secured by txOne networks

Dashboard Agents Logs Administration About

Agents > StellarProtect

+ Add Group

Endpoint Search

All Agents

Policy

ICS items

All Agents (2)

Edit Policy

View ICS Items

ICS Applications (12)

Software	Vendor	Version
Rockwell Windows Firewall Configuration Utility 1.00.13	Rockwell Automation, Inc.	1.00.13.0004
FactoryTalk Linx 6.20.00 (CPR 9 SR 12.0)	Rockwell Automation, Inc.	6.20.00
Rockwell Automation USBCIP Driver Package	Rockwell Automation	3.18.06
TF5210-CNC-Export	Beckhoff Automation	3.1.3070.0
FactoryTalk Activation Manager 4.05.03	Rockwell Automation, Inc.	4.05.03
BootP-DHCP Tool	Rockwell Automation, Inc.	3.05.00
FactoryTalk Diagnostics 6.20.00 (CPR 9 SR 12)	Rockwell Automation, Inc.	6.20.00
Electronic Data Sheets Reader	Rockwell Automation, Inc.	33.00.20

ICS Certificates (23)

Issued To	Issued By	Hash
Rockwell Automation I...	DigiCert SHA2 Assure...	9F4D88C940ECF1B4115B18BD188F7BFECF266752
Rockwell Automation	Symantec Class 3 SHA...	2BC72F0C96CAFDE64AC3B5A2D6607D1156D383...
Rockwell Automation	Symantec Class 3 SHA...	28AE0D73930CD4CABA8EB7CB44DEC80737BC6F50
Rockwell Automation I...	DigiCert SHA2 Assure...	E8C8D45AED233430AAE06241BEB14BC5D63C7B2F
Rockwell Automation	Symantec Class 3 SHA...	78BACC8E53A96F250535ECEDDE12FB5E9728EB43
Rockwell Automation	Symantec Class 3 SHA...	9108F27107A8577610F685E627647B09B7215C48
Rockwell Automation	Symantec Class 3 SHA...	09E9908AE0904410C2BB530A0E6197AC8FC13952
Rockwell Automation	VeriSign Class 3 Code ...	7A31F9698DDED84EB610A731C7057BD3FB923F91



StellarOne - Wykrywanie i rozpoznawanie aplikacji ICS/OT





- ABB
- Acronis
- Autonics
- Baker Hughes
- Bürkert
- Codesys
- Delta electronics
- Druck limited
- Emerson
- Epson Robots
- Fanuc
- Fisher controls
- Fuji
- GE
- Idec
- Keyence
- Hitachi
- Honeywell
- Lovato electric
- Micromeritics
- Mitsubishi
- Motorola
- National instruments
- Omron
- Pactware
- Phoenix contact
- Red lion
- Roboticsware
- Rockwell
- Seiko Epson
- Schneider
- Siemens
- Verif-I
- YASKAWA
- Yokogawa
- Yamaha

StellarOne – ochrona aplikacji ICS oraz ich zasobów




Ochrona aplikacji ICS

Group
▶ Nagoya Horita (5)   Policy
▼ Edit Policy

ICS Application Safeguard

Protect files and folders from unauthorized changes.
 Protect the ICS Applications

▼ K-254-A23 10.1.192.36 ▶  South Area Omron S7-400 Metec











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

Ochrona krytycznych plików/folderów

ICS Application Safeguard

[+ Add](#)

Protection Path	Type	Exception Process	Actions
All ICS Applications	All ICS Applications	C:\Windows\explorer.exe	 
HKEY_LOCAL_MACHINE\SOFTWA	Registry Key	C:\Windows\explorer.exe	 
C:\MyFolder	Folder	No Process can write	 
C:\MyFolder\MyFile.exe	File	-	 
HKEY_LOCAL_MACHINE\SOFTWA	Registry Key	-	 

StellarOne – zarządzanie aplikacjami/certyfikatami



Group
▼ **Nagoya Horita (5)**

Policy
▶ Edit Policy

<input type="checkbox"/>	Endpoint	IP Address	Protected	Location	Vendor	Model	Description	Operation System	Last Connection
<input type="checkbox"/>	▶ 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
<input type="checkbox"/>	▶ K-101	10.1.192.33	▶ ✔	North Area	SIEMENS	Sinumerk	Consulting	Windows 7 Starter Edition build 7601	2020-08-13T11:31:15+08:00
<input type="checkbox"/>	▼ 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

StellarOne - Wykrywanie anomalii



Monitorowanie wrażliwych procesów – np. PowerShell

Operations Behavior Anomaly Detection

- Learning: Add the unrecognized call of monitored process to approved operation.
- Detection: Write a log on unrecognized call of monitored process.
- Prevention: Block the unrecognized call of monitored process.
- Disable

Aggressive Mode

Approved Operation(s)

Operations Behavior Anomaly Detection

+ Add

Monitored Process	Actions
PowerShell.exe	
C:\WINDOWS\system32\wscript.exe	
C:\WINDOWS\system32\wscript.exe	
MAHTA.exe	
C:\WINDOWS\system32\wscript.exe	

Nauka i akceptowanie prawidłowego zachowania użytkownika

Operations Behavior Anomaly Detection Approved Operation(s)

command arguments

process sequence

Monitored Process	Approved Operation	Created Time	Actions
"powershell.exe"-NoNiNt	"C:\Windows\System32\cmd.exe"-NoprOrFile	2020-08-13T15:00:00	
"powershell.exe"-NoNiNt	"C:\Windows\System32\cmd.exe"-NoprOrFile	2020-08-13T15:00:00	

<https://www.txone.com/blog/how-flax-typhoon-hack-weaponized-legitimate-software/>

StellarOne - Wykrywanie anomalii



Nauka i akceptowanie prawidłowych aplikacji

stellarOne szkolenie (szkolenie) txOne networks

Dashboard Agents Logs Administration About

← TEST-KOMPUTER

StellarProtect Policy Inheritance: Inherit from parent group: Elmark | Self-management:

General Info Policy **Situational Awareness**

OT Applications: 18 | OT Certificates: 2 | Approved Script Behaviors: 2 | Approved Login Accounts: 2 | **Approved Applications: 49**

The baseline below shows the approved applications for the agent. You can also manually add more approved applications to the [Policy-based Approved Applications](#) on the Policy page.

[Export](#) Baseline Toggle

Application ↑	Size	SHA-1	SHA-256	Path	Version	Added From	Time Added
<input checked="" type="checkbox"/> Automation License...	3 MB	041c358bb83c32ca...	25f7a795fd73eb0a...	c:\program files\common files\siemens\sws\...	600.100.201.2	Learn mode	2023-11-14T17:59:...
<input checked="" type="checkbox"/> Instalator Windows ...	125 KB	443aac22d57edd4...	5ae0bf71e770c295...	c:\windows\system32\msiexec.exe	5.0.7600.16385 (wi...	Learn mode	2023-11-14T17:59:...
<input checked="" type="checkbox"/> Instalator Windows ...	72 KB	bd9bbb448dec04b...	78617ddf9a0067a3...	c:\windows\syswow64\msiexec.exe	5.0.7600.16385 (wi...	Learn mode	2023-11-14T17:59:...
<input checked="" type="checkbox"/> Java(TM) Platform ...	146 KB	77db74837435b2a...	9809ddb5a3b5cc20...	c:\program files (x86)\java\jre6\bin\java.exe	6.0.300.12	Learn mode	2023-11-14T18:09:...
<input checked="" type="checkbox"/> Java(TM) Platform ...	249 KB	45a3907feaa8503c...	e253ce5b347470cc...	c:\program files (x86)\common files\java\jav...	2.0.6.1	Learn mode	2023-11-14T17:59:...
<input checked="" type="checkbox"/> LoggingService Mo...	2 MB	8229a2e57a635f94...	ed320ac6e92cd291...	c:\program files (x86)\emerson\pac machin...	1, 0, 0, 1	Learn mode	2023-11-14T17:59:...

StellarOne - Wykrywanie anomalii



Nauka i akceptowanie logowania użytkowników

stellarOne szkolenie (szkolenie) txOne NETWORKS

Dashboard Agents Logs Administration About

← TEST-KOMPUTER

StellarProtect Policy Inheritance: Inherit from parent group: Elmark | Self-management:

General Info Policy **Situational Awareness**

OT Applications: 18 | OT Certificates: 2 | Approved Script Behaviors: 2 | **Approved Login Accounts: 2** | Approved Applications: 49

The baseline below shows the approved user accounts for the agent. You can also manually add more approved user accounts to the [Policy-based Approved Login Accounts](#) on the Policy page.

[Export](#) Baseline Toggle

Domain ↑	Username	Source IP	Login Type	Added From	Time Added	
<input type="checkbox"/>	.	administrator	-	Network (Logon Type 3)	Learn mode	2023-11-14T17:59:55+01:00
<input type="checkbox"/>	.	administrator	192.168.99.254	Remote Interactive (Logon Type...	Learn mode	2023-11-14T17:59:57+01:00

StellarOne – kontrola portów USB



Predefiniowane zaufane urządzenia USB

The screenshot shows the StellarOne web interface. The top navigation bar includes Dashboard, Agents, Logs, Administration, and About. The main content area is titled 'StellarProtect' and features a '+ Add Group' button. Below this, there are tabs for 'Agents' (All Agents (60)) and 'Policy' (Edit Policy). The 'USB Vector Control' section is active, showing a toggle switch for 'USB Vector Control' which is turned on. Below the toggle is a 'Trusted USB Device List' with a '+ Add' button and a table of devices.

Vendor ID	Product ID	Serial Number	Actions
07AB	FCFD	1100	
07AB	FCFD	1101	

Pozwolenie na jednorazowe użycie



StellarOne – Tryb maintenance



Łatwe przejście w tryb serwisowy pozwalający na zmiany, dodanie aplikacji i procesów

The screenshot displays the TXOne StellarProtect web interface. The top navigation bar includes the 'stellarProtect' logo and the 'txOne networks' logo. A left sidebar contains menu items: Overview, OT Applications, OT Certificates, Approved List, Password, Operations, Settings, and About. The main content area features a large green checkmark icon with a wrench, indicating 'Protection Enabled'. Below this, it states 'Maintenance Mode enabled since 2023-11-14T13:04:07' and 'It will be ended at 2023-11-14T14:04:07'. Two status cards are visible: 'Real-Time Scan' (enabled since 2023-11-13T16:18:51) and 'Application Lockdown (Enforce)' (enabled since 2023-11-08T12:24:28). An 'Information' section provides system details:

StellarOne registration:	✓
StellarOne group name:	Elmark
Last connection to StellarOne:	2023-10-20T13:42:36
Application vault last updated on:	2023-10-19T17:02:31
Approved List last updated on:	2023-10-19T17:04:01
Components last updated on:	2023-10-20T00:00:01
Last blocked event:	2023-11-13T09:17:52
License expires on:	2023-12-31

[Device Information](#)

StellarOne – centralne zarządzanie



Preview

winfred (winfred) ▾



Dashboard Agents Logs ▾ Administration ▾ About

Agents All (6) > America (6) > Canada (6) > Montréal (6) ▾



+ Add Group

Organize ▾

1 / 1 < > [Grid Icon]

<input type="checkbox"/>	Agent	IP Address	Protection	Policy	Agent Version	Last Connection	Product	Actions
<input type="checkbox"/>	ZION-WIN7X86-1	172.17.1.92		● Inherited	1.2.1065	2022-02-24T13:22:...	← StellarProtect	⋮
<input type="checkbox"/>	ZION-WIN2K16...	172.17.1.87		● Inherited	1.2.1065	2022-02-24T13:02:...	← StellarProtect	⋮
<input type="checkbox"/>	PROTETAGEN...	172.17.1.193		● Inherited	1.2.1065	2022-02-24T13:24:...	← StellarProtect	⋮
<input type="checkbox"/>	PROTECTAGE...	172.17.1.194		● Inherited	1.2.1065	2022-02-24T13:25:...	← StellarProtect	⋮
<input type="checkbox"/>	ZION-WIN7-EN...	172.17.1.175		● Customized	1.2.1014	2022-02-25T10:35:...	← StellarEnforce	⋮
<input type="checkbox"/>	ZION-W7ENTX...	172.17.1.187		● Inherited	1.2.1014	2022-02-24T16:48:...	← StellarEnforce	⋮



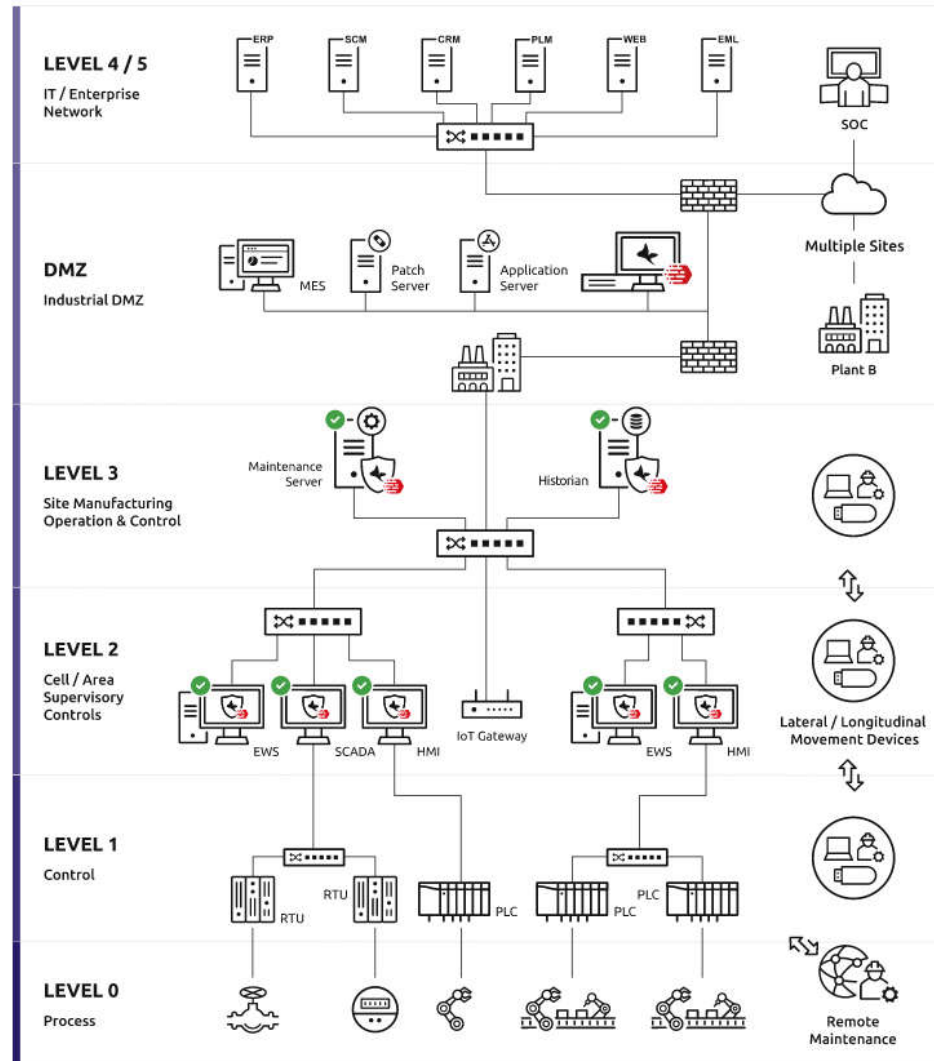
TXone Stellar vs standardowy antywirus



- **Wsparcie dla starych systemów operacyjnych (Windows XP, Windows 7, Windows 2000)**
- **Bardzo lekki agent (niskie zapotrzebowanie na CPU i RAM)**
- **Długoletnie wsparcie**
- **Tryb serwisowy w którym działa ochrona antymalware**
- **Automatyczne rozpoznawanie aplikacji OT**
- **Możliwość nauczania się zachowania użytkownika**
- **Wsparcie on-premise**
- **Łatwe masowe zarządzanie z podziałem na lokalizacje/grupy**

Możliwości zastosowania

**Ochrona wszelkiego typu
maszyn i komputerów
przemysłowych opartych o
systemy Windows**





TXOne Portable Inspector



Szybka weryfikacja assetów



PORTABLE SECURITY

Narzędzie do skanowania malware. Dla systemów odizolowanych.

- Nie trzeba niczego instalować
- Łatwa obsługa
- Widoczność zasobów (aplikacji OT) oraz centralne zarządzanie
- Możliwość kwarantanny lub usuwania zainfekowanego pliku
- Diody LED – wynik skanowania
- Windows oraz Linux
- Nie można go zainfekować – pliki są przechowywane na osobnych partycjach
- W wersji PRO bezpieczne przenoszenie plików (malware-free storage)

Scan status and
result notification with LED



No malware is detected. System is safe

Portable Inspector – scenariusze wykorzystania



Inspekcja przyjęcia

- Skanowanie systemów odbieranych od dostawców pod kątem infekcji

Inspekcja wysyłki

- Skanowanie produktu przed wysyłką

Regularna kontrola

- Regularne skanowanie niezależnych systemów na obiektach
- Skanowanie maszyn gdzie instalowanie trzeciego oprogramowania nie jest możliwe (maszyny krytyczne, urządzenie objęte gwarancją)
- Skanowanie maszyn gdzie jedynie fizyczny i rejestrowany dostęp jest możliwy

Kontrola firm zewnętrznych

- Weryfikacja osób odwiedzających obiekt w celu prac serwisowych



Kompletne i unikatowe podejście do ochrony systemów OT



Deployment Model

Security Inspection

Installation-less malware scanning tool
Portable Inspector
Periodical health-check processes

Installation-less malware scanning tool with encryption
Portable Inspector Pro Edition
Periodical health-check processes with secure transporter

Management Console
ElementOne
Manage Portable Inspector and Portable Inspector Pro edition

Endpoint Protection

All-terrain digital safety for OT endpoints
Stellar
Recognize and preserve thousands of critical ICS and OT applications

Management Console
StellarOne
Manage Stellar

Network Defense

Industrial next-generation IPS
EdgeIPS
Micro segmentation for critical assets protection

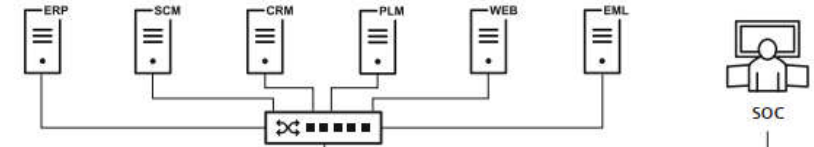
Industrial next-generation firewall
EdgeFire
Enables secure network segmentation

Industrial next-generation IPS Array
EdgeIPS Pro (For large-scale networks)
Internal segmentation for critical assets protection

Industrial central management console
EdgeOne / OT Defense Console
Plant defense field management

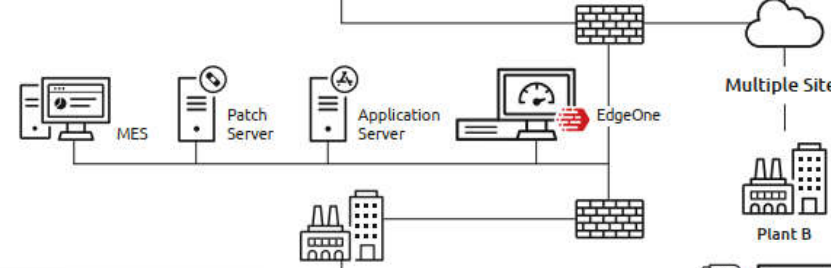
LEVEL 4 / 5

IT / Enterprise Network



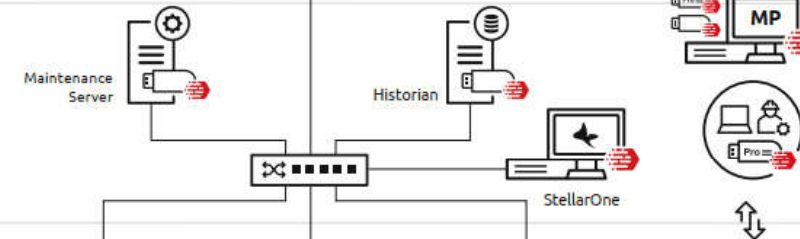
DMZ

Industrial DMZ



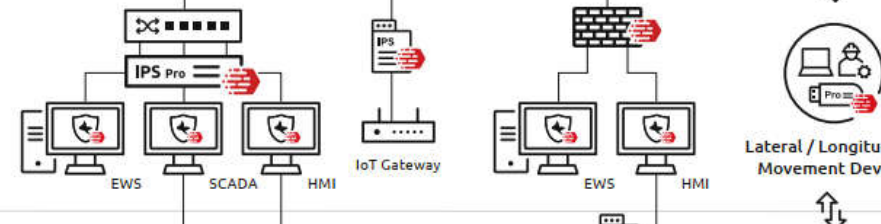
LEVEL 3

Site Manufacturing Operation & Control



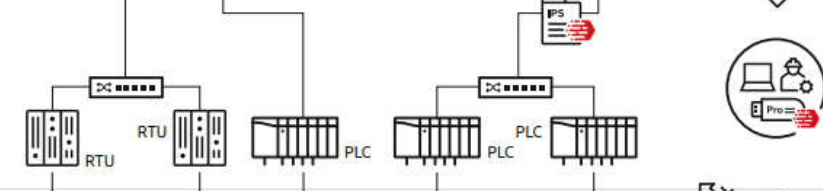
LEVEL 2

Cell / Area Supervisory Controls



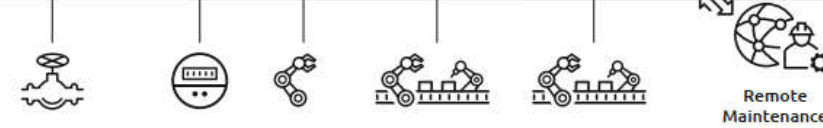
LEVEL 1

Control



LEVEL 0

Process



A photograph of two business people in suits shaking hands, symbolizing agreement or partnership. The image is overlaid with a white dotted grid pattern.

Dziękujemy za uwagę

Sprawdź:

www.elmark.com.pl

www.elmark-automation.com

www.elmark.com.ro