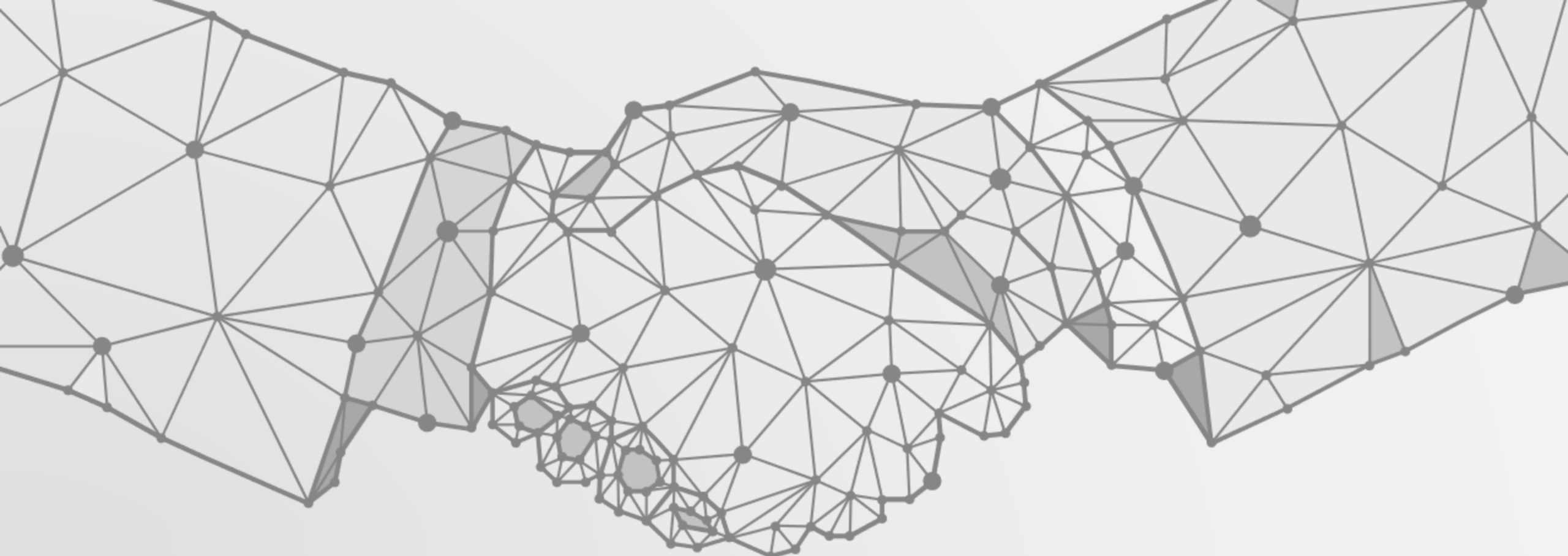


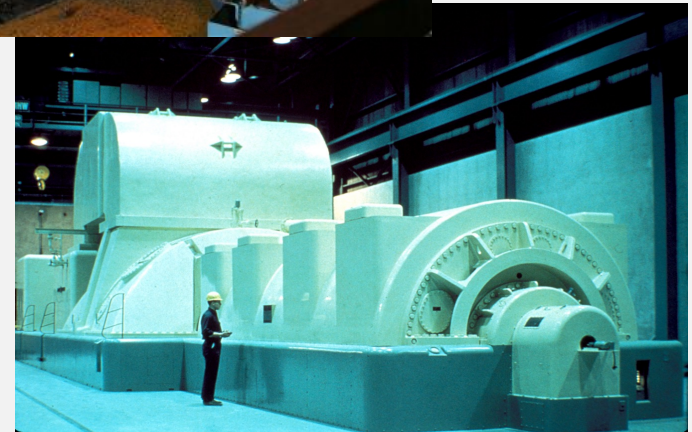
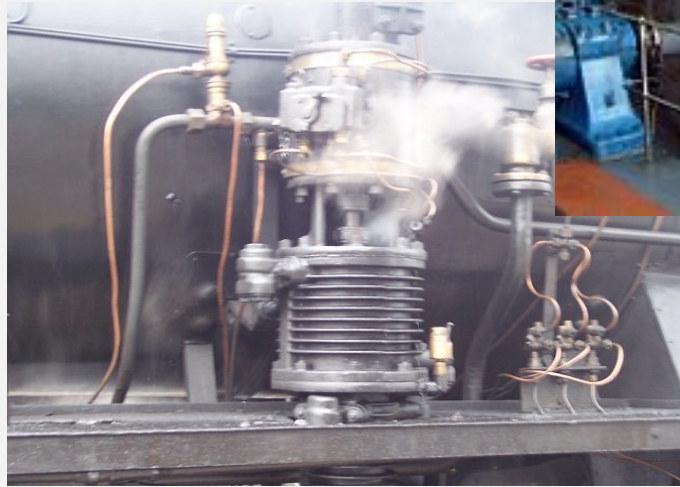
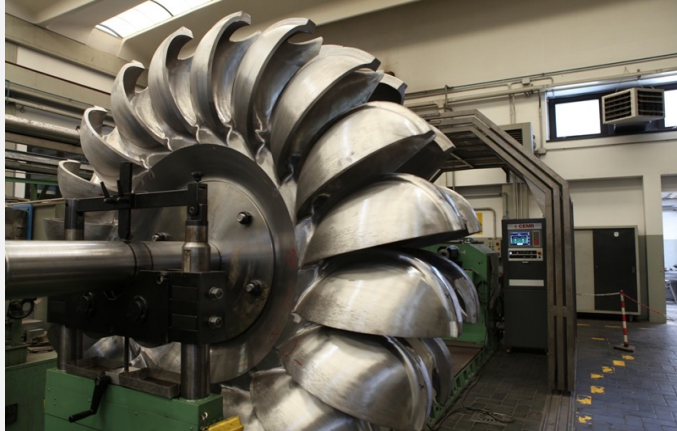


NIS2 és az ipari digitális környezetek

Budapest, 2023.11.14

Csinos Tamás, CISSP
country manager, Clico

Industrial machinery and equipment



Ki az, aki már most tudja, hogy a NIS2
vonatkozni fog rá?



Biztos?



Kategória	Főtevékenység	Teljes tevékenységi kör
Kiemelten kockázatos ágazatok	432	528
Kockázatos ágazatok	1247	339
Összesen	1679	867
	2546	

50  és 10M 

250  és 50M 

N
I
S
2

Több, mint 50  vagy 10M 

Érintett szektorok (és ezek esetleges beszállítói)



OT - Operational Technology

ICS - Industrial Control System = IACS - Industrial Automation and Control System



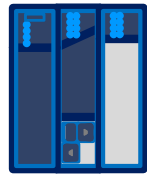
Advanced analytics and data storage

- MES – Manufacturing Execution System
- APC - Advanced Process Control
- Data Historian



Visualization, supervision and control

- SCADA - Supervisory Control and Data Acquisition
- DCS - Distributive Control System
- HMI - Human Machine Interface



Control devices

- PLC - Programmable Logic Controller
- PAC - Programmable Automation Controller
- RTU - Remote Terminal Unit

Industrial machinery and equipment

OT - Operational Technology

ICS - Industrial Control System = IACS - Industrial Automation and Control System



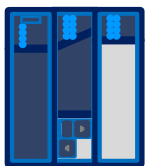
Advanced analytics and data storage

- MES – Manufacturing Execution System
- APC - Advanced Process Control
- Data Historian



Visualization, supervision and control

- SCADA - Supervisory Control and Data Acquisition
- DCS - Distributive Control System
- HMI - Human Machine Interface



Control devices

- PLC - Programmable Logic Controller
- PAC - Programmable Automation Controller
- RTU - Remote Terminal Unit

Nincs beépített biztonság

Industrial machinery and equipment

Adatbázisok

Exploits

Webes
felületek

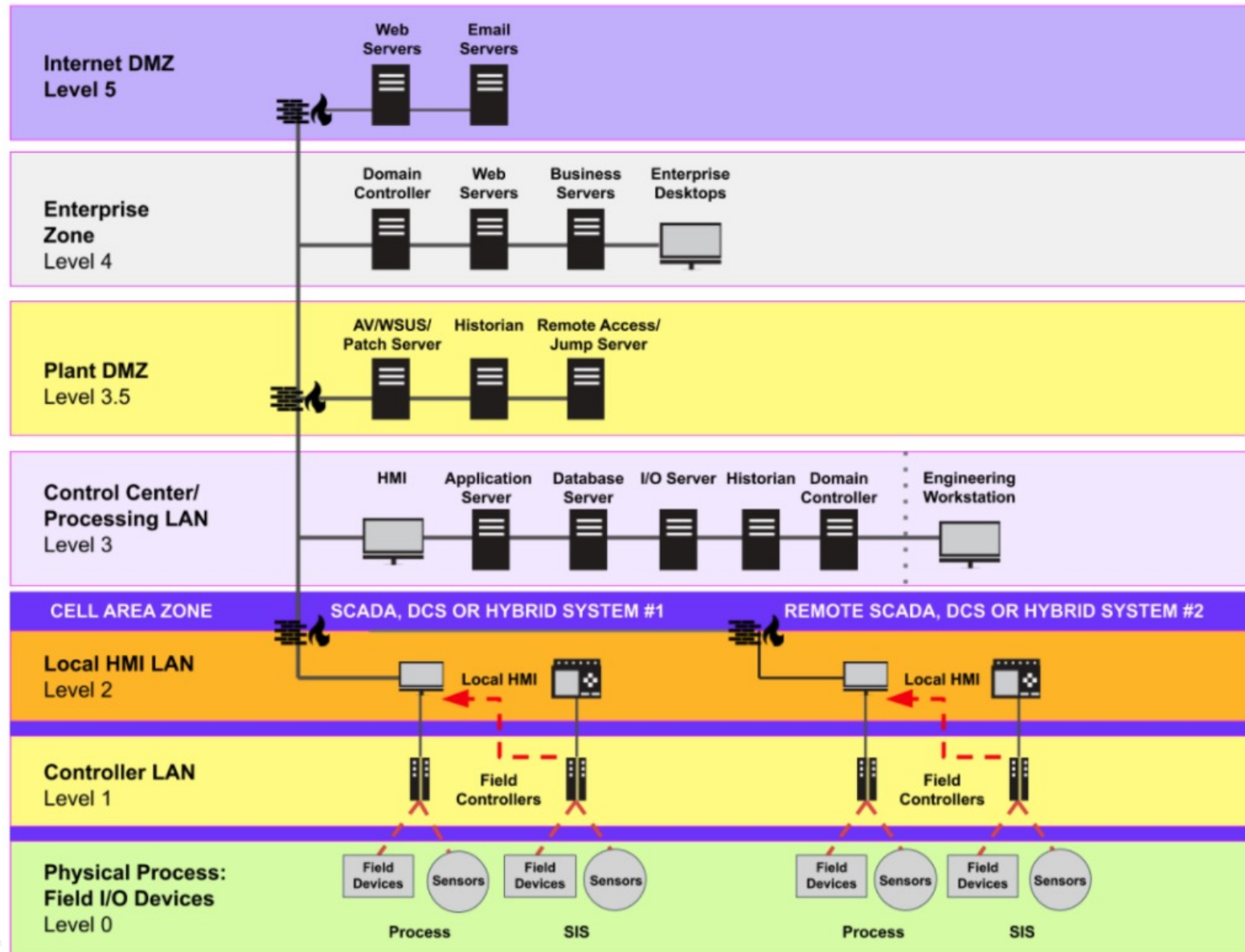
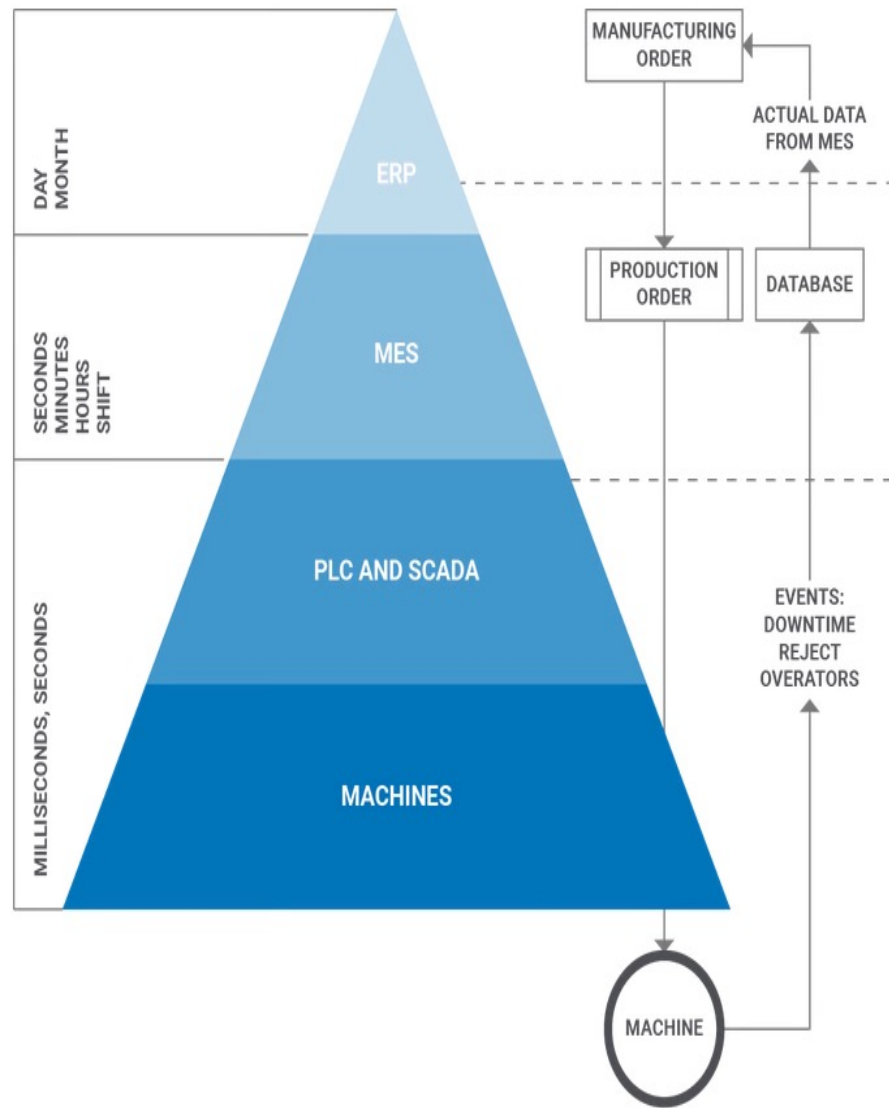
SQL-I, XSS

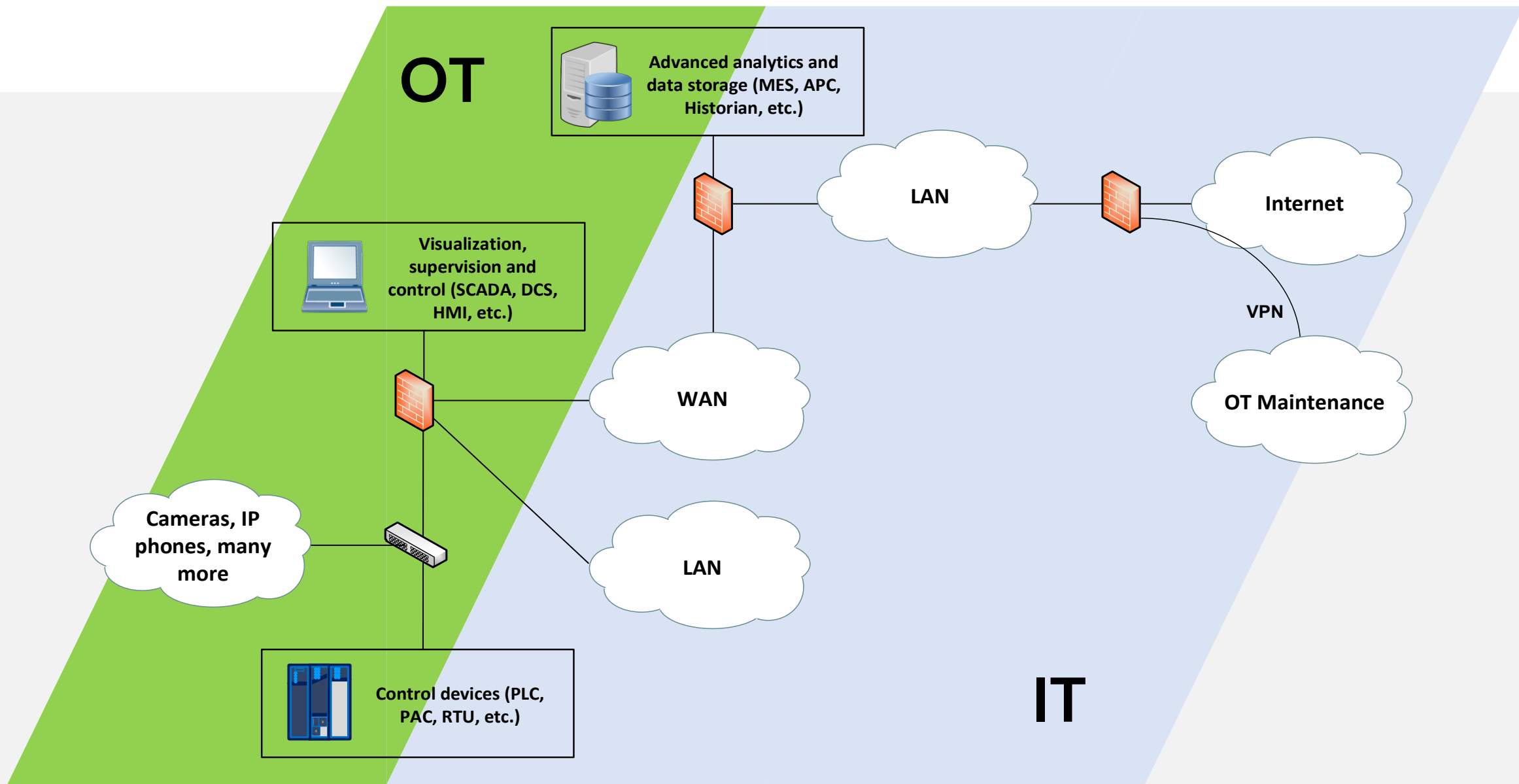
SSH / egyéb
távoli
hozzáférések

Misuse

Windows és
Linux alapú
rendszerek

Malware





Mit hallunk mindig az OT rendszer üzemeltetőktől?

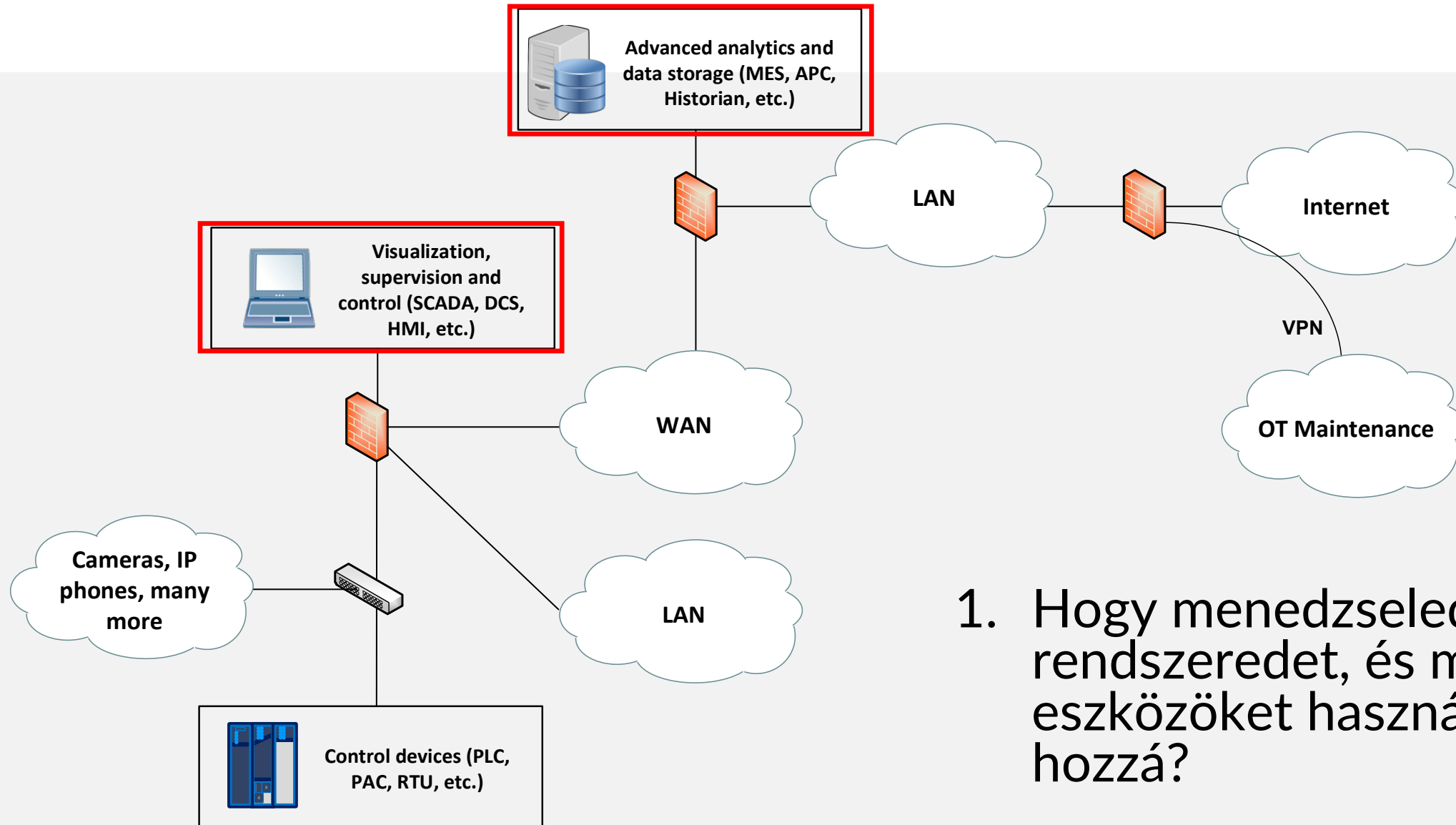
- 1# Ohh, nálunk nincs semmi SCADA...
de ha van, az is régi...

Biztonságosak vagyunk!

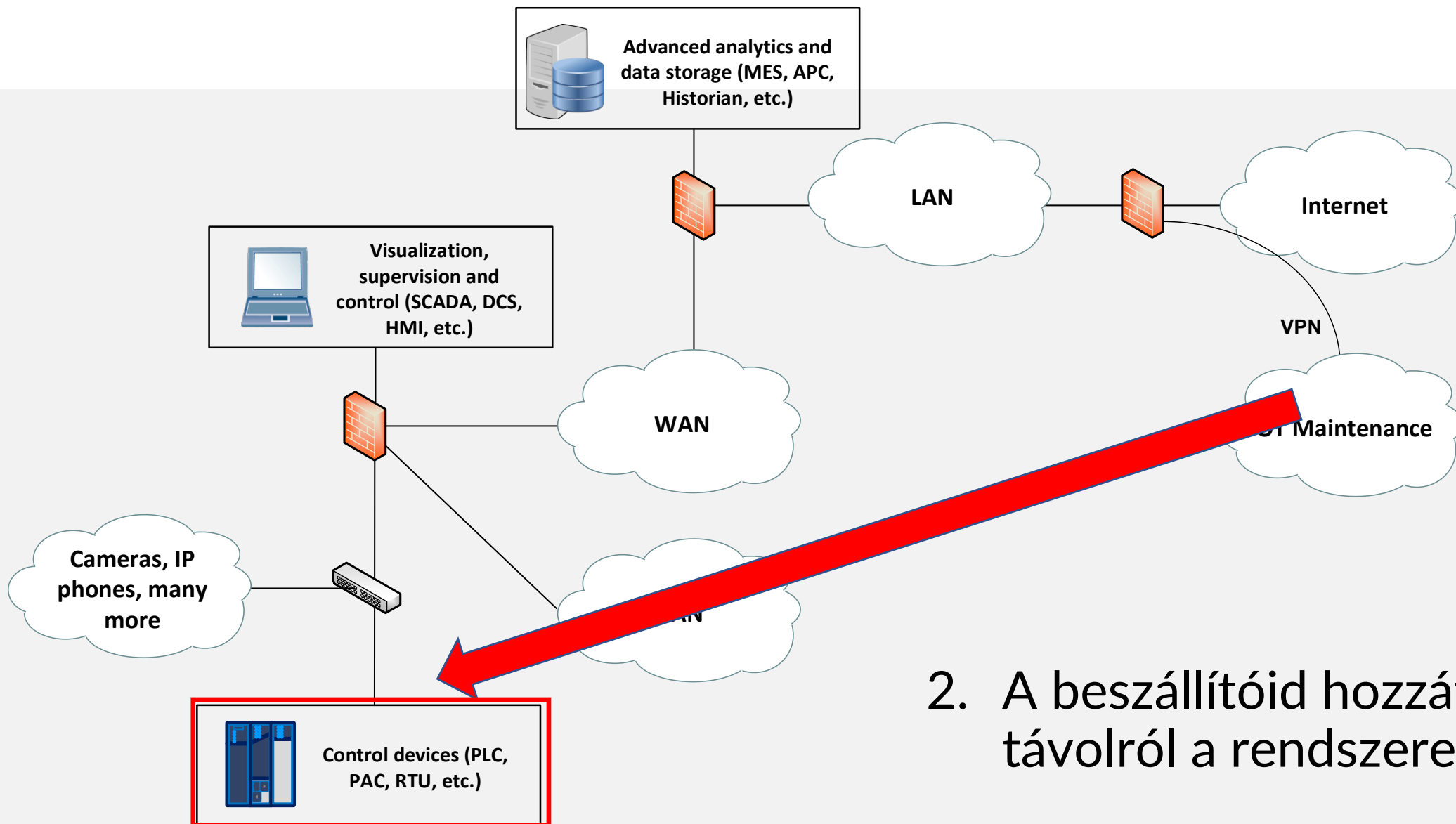
- 2# Az ipari rendszereink nem csatlakoznak
az irodaiakhoz, nincs internet hozzáférésük.

Biztonságban vagyunk!



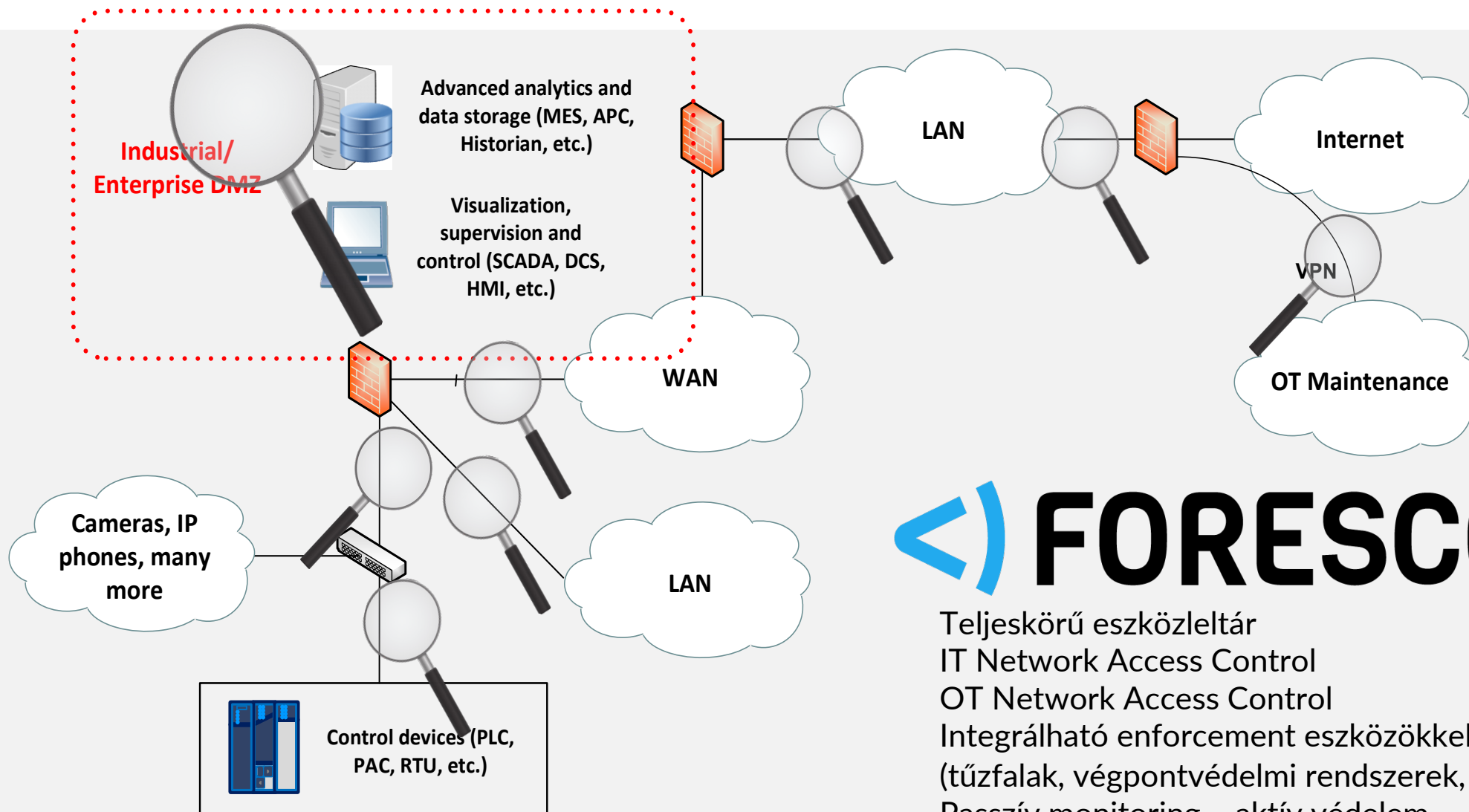


1. Hogy menedzseled az OT rendszeredet, és milyen eszközöket használsz hozzá?



2. A beszállítóid hozzáférnek távolról a rendszereidhez?

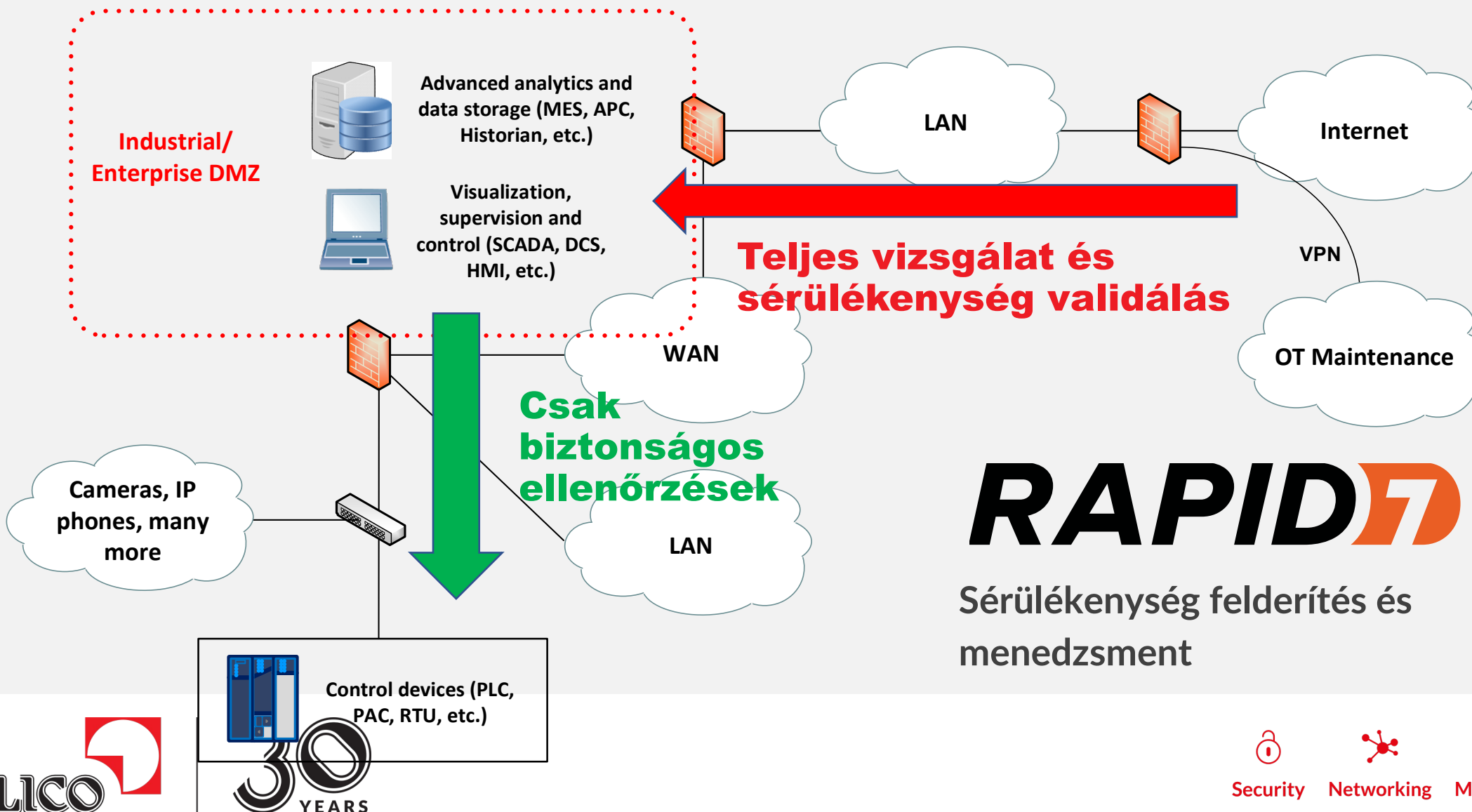
Láthatóság – fizikai eszközök



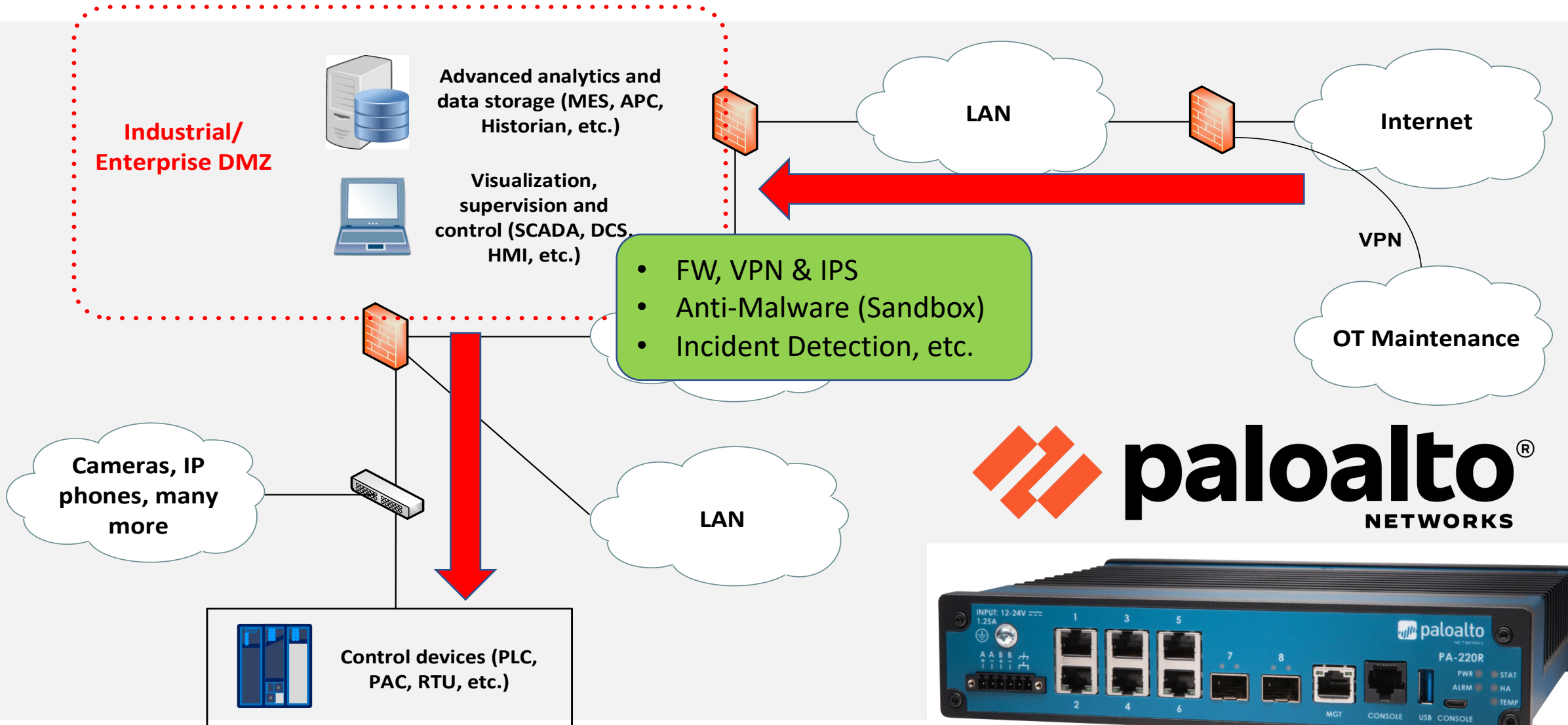
 **FORESCOUT®**

Teljeskörű eszközlétár
IT Network Access Control
OT Network Access Control
Integrálható enforcement eszközökkel
(tűzfalak, végpontvédelmi rendszerek, SIEM, stb)
Passzív monitoring – aktív védelem

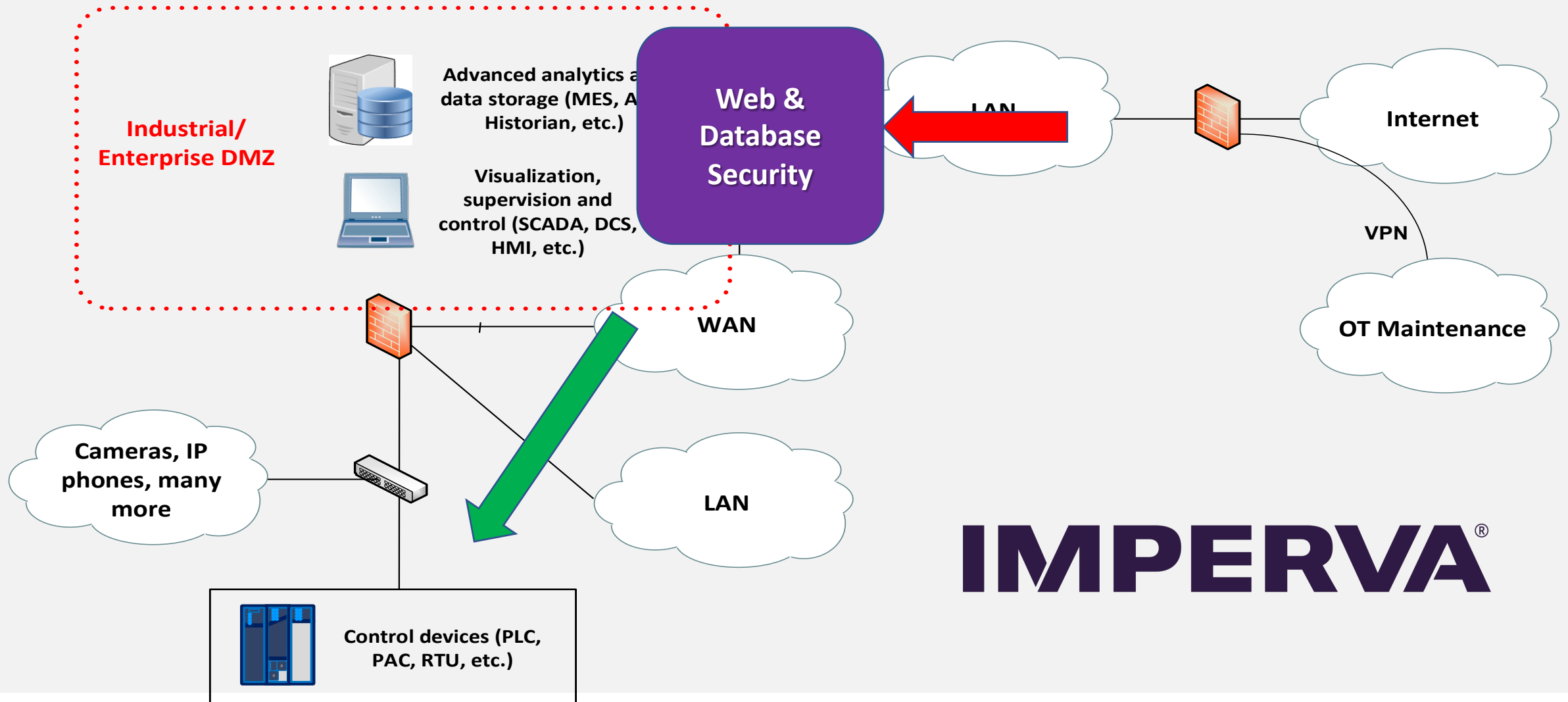
Láthatóság – software eszközök



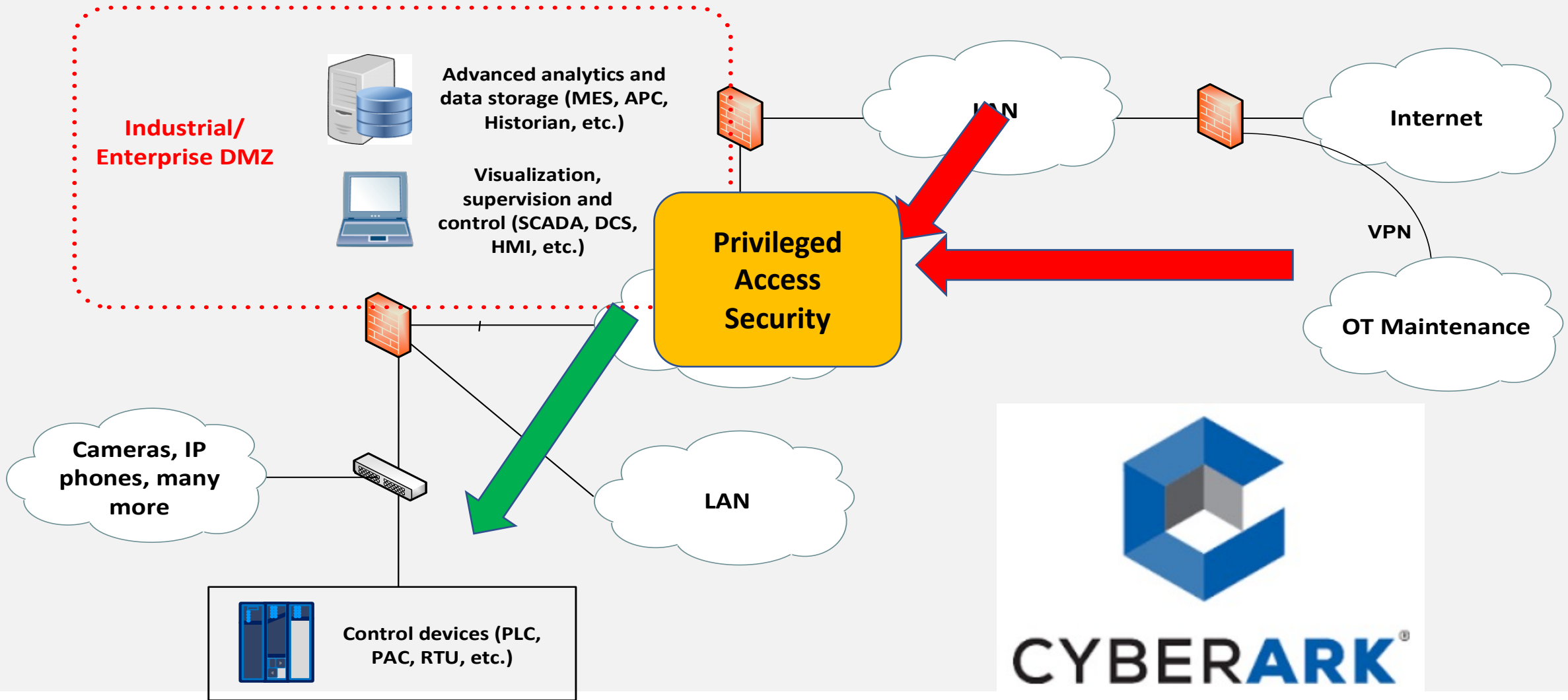
Szegmentáltság, forgalom kontroll – aka „tűzfalazás”



Adatbázisok és kezelőfelületek védelme



Üzemeltetők, rendszertámogatók felügyelete – kiemelt felhasználók kezelése



Palo Alto Networks - Palo-Usage Collector [< prev top next >](#)

Policy Package: Standard

Note: Rules displayed in the 'Rules that are not tracked' section may have hits in rule usage report.

It can happen when the log / track configuration is changed for this rule during the report's time period or, for Check Policy, when the complementary logging feature is used.

[Most-used rules](#)
[Least-used rules](#)
[Unused rules](#)
[Rules that are not tracked](#)
[Used rules containing unused objects](#)
[Unused objects in rules](#)

Most-used rules - 1 of 10 (top 50%)

	HITS	FIRST HIT	LAST HIT	Name	Rule Type	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application Identity	Service
4	264,529 (66%) Changed	Sun, 11 Oct 2015 00:00	Thu, 10 Mar 2016 03:00	rule_2	universal	any	any	172.200.10.10 264, 529 (100%)	Any	10.100.200.160 264, 529 (100%) 192.168.1.88 0 (0%)	Any	ANY

Least-used rules - 1 of 10 (bottom 50%)

TXOne Networking Solution Models

EdgeIPS Pro-1048 Gen2

- 10Gbps+ performance
- Virtual Patching(IPS) / Anvti-virus
- OT protocol inspection
- Rugged design and Commercial
- Up to 24 pairs hardware bypass
- OOB support

EdgeIPS Pro-216 R&C

- 1.8Gbps+ performance
- Virtual Patching(IPS) / Anti-virus
- OT protocol inspection
- Rugged design and Commercial
- 8 pairs hardware bypass
- OOB support

EdgeIPS Pro-2096 Gen2

- 10Gbps+ performance
- Virtual Patching(IPS) / Anvti-virus
- OT protocol inspection
- Rugged design and Commercial
- Up to 48 pairs hardware bypass
- OOB support



EdgeOne

- Available management all Edge product in one console
- Network visibility
- Centralized policy management
- SIEM and XDR integration
- Security posture and report
- Multi-hypervisor support (Vmware /KVM/Hyper-V)

EdgeIPS-103

- 850Mbps+ performance
- Virtual Patching(IPS)
- OT protocol inspection
- Rugged design
- 1 pairs hardware bypass
- OOB support

EdgeIPS-102

- 200Mbps+ performance
- Virtual Patching(IPS)
- OT protocol inspection
- Rugged design
- 1 pairs Hardware bypass

EdgeIPS LE-102

- 150Mbps+ performance
- Virtual Patching(IPS)
- 1 pairs Hardware bypass

EdgeFire-1012

- 200Mbps+ performance
- Virtual Patching(IPS)
- OT protocol inspection
- Rugged design
- NAT and Remote access protection(VPN)
- OOB support

New model

New model

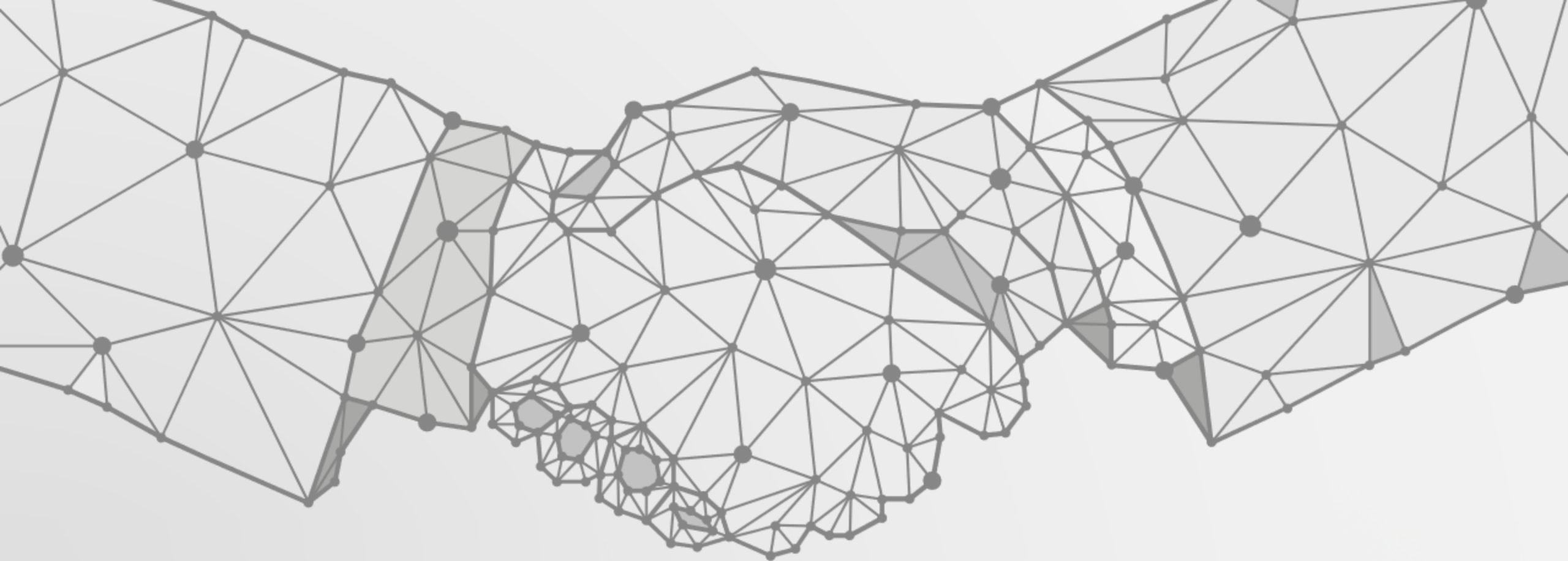
EdgeIPS Pro-2008

- 20Gbps+ performance
- Virtual Patching(IPS)
- 4 pairs 10G copper with Hardware bypass

New model

EdgeIPS Pro-2016F

- 20Gbps+
- 8-Pairs 10G Fiber Bypass (Gen3)



Köszönöm a figyelmet!

