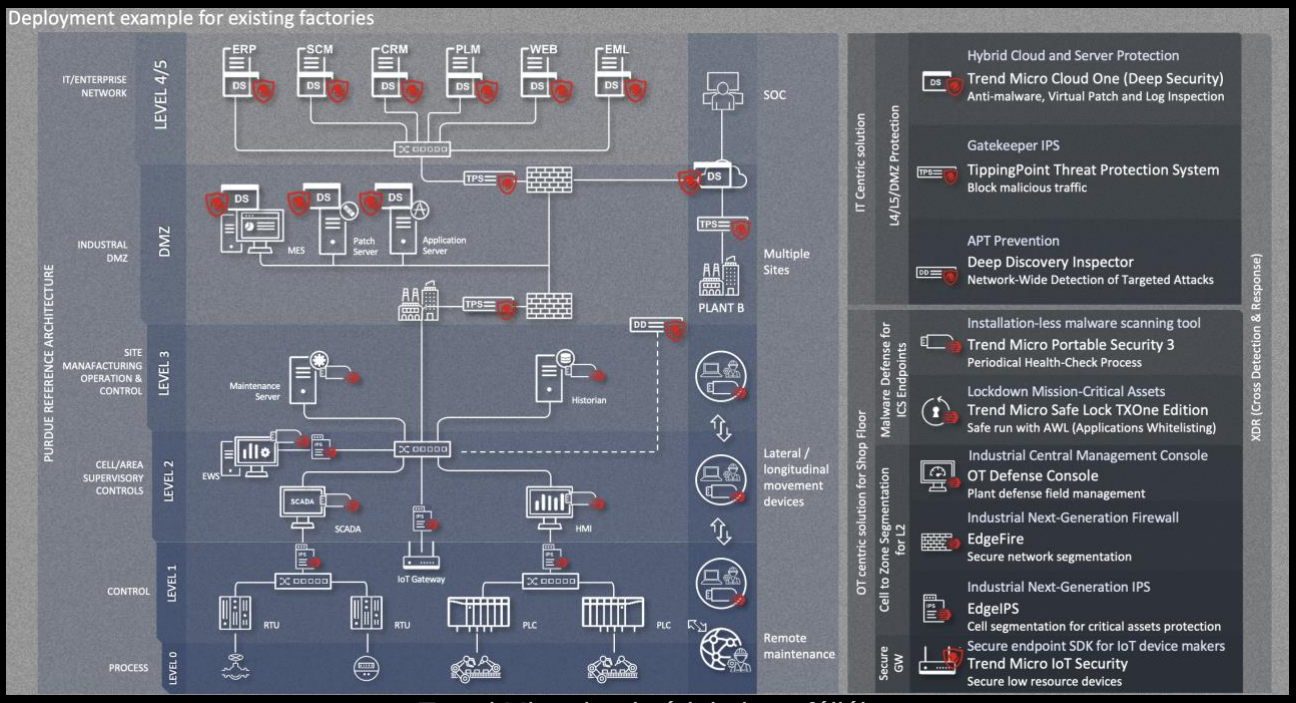
ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

ARLITECH IPARI BIZTONSÁG

Az OT (Operációs Technológia) eszközök a **gyártási folyamatok** nélkülözhetetlen eszközei, bármilyen kimaradás, leállás, hatalmas veszteséget okozhat.

A kritikus infrastruktúrák üzemeltetésénél szintén fontos az eszközök védelme: **elektromos, víz, olaj, gáz, egészségügyi szolgáltatás. Légi- vasúti közlekedés, szállítmányozás. Gyógyszergyártás. Élelmiszeripar.**

A Trend Micro OT-biztonsági termékei a kezdetektől fogva ipari környezetre lettek kifejlesztve. A hálózatvédelmi megoldások hardverét az ipari megoldásairól közismert Moxa gyártja a Trend Micro számára, így garantálva, hogy a Trend Micro TXOne eszközök maximálisan megfeleljenek az ipari szabványoknak. Az eszközök magas MTBF (Mean Time Between Failure) értékkel rendelkeznek, továbbá könnyedén illeszthetők gyártósorokon is, legyen szó akár rögzítésről (DIN-rail, wall mount), vagy akár tápellátásról (dual terminál block).

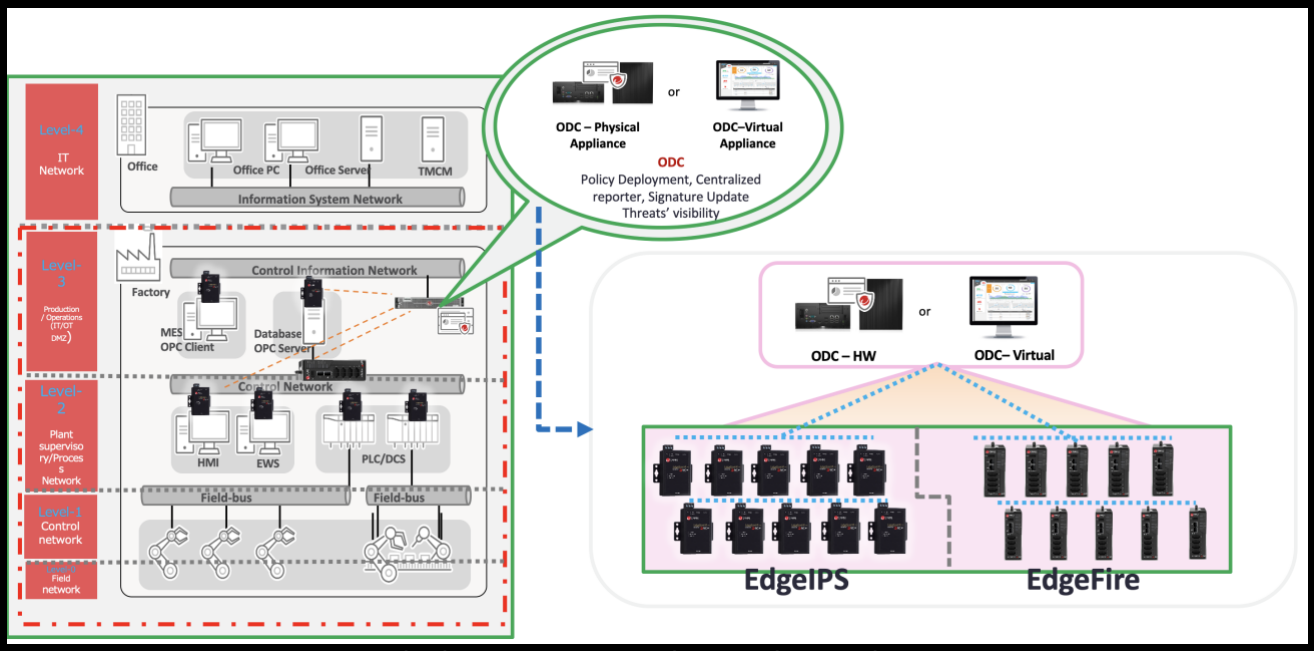


Trend Micro ipari védelmi portfóliója

Az IT (Információs Technológia) és OT (Operációs Technológia) technológiák általában külön működnek, mindegyik saját hálózattal, karbantartó csapattal, célokkal és igényekkel. A tipikus OT hálózat olyan hatalmas számú eszközt kapcsol össze, amelyek nem a modern vállalati hálózatokhoz lettek tervezve, és ennek következtében rendkívül nehéz időben elvégezni az aktualizálásokat és a javításokat, a kritikus eszközök védelmének fenntartása érdekében.

Ipari hálózatvédelem – Trend Micro TXOne ODC Központi menedzsment

A Trend Micro TXOne EdgeFire és EdgeIPS eszközei akár különálló eszközként is menedzselhetők, amennyiben nincs lehetőség központi menedzsmentbe bekötni őket. Amennyiben viszont ennek nincs akadálya, mindenképpen javasoljuk a TXOne ODC (OT Defense Console) használatát. A megoldás akár virtuális appliance változatban, akár hardveres változatban is elérhető.



Trend Micro TXOne ODC központi menedzsment

A központi menedzsment felületén keresztül az EdgeIPS eszközök szabályhalmaza egy helyről menedzselhető, összevont biztonsági jelentések, és asset reportok készíthetők az eszközökről. Továbbá az eszköz központi disztribúciós pontként szolgálhat IPS frissítések terítéséhez.

Ipari hálózatvédelem – Trend Micro TXOne EdgeIPS

A TXOne EdgeIPS eszközök ipari környezetek számára készültek, ahogy az alábbi specifikációban is látható a paraméterei tökéletesen megfelelnek akár gyártósori használatra is (hőmérséklet ingadozás vagy vibráció magasfokú tűrése, magas MTBF). Az eszközök hálózati interfészei alacsony késleltetésűek (<500 micromp.). Amennyiben az eszköznek megszűnik a tápellátása akkor bypass módban át tudja engedni a hálózati forgalmat.

Features	EdgeIPS 102-BP-TM
Supported IPS throughput	200Mbps+
Latency	<500 micro seconds
Concurrent Connection (TCP)	10,000
Supported ICS Protocol	Modbus / EtherNet/IP / CIP / FINS, with more being added regularly
Policy Enforcement Rules	64 Rules
ICS Protocol Filter Profiles	32 Profiles
Form Factor	DIN-rail mounting and Wall mounting (with optional kit)
Weight (Stand-Alone Device)	322g (0.7098 lb)
Dimensions (W x D x H)	42mm x 70mm x 83mm (1.65 x 2.76 x 3.27 in)
Network Interface Type	2 x Auto-sensing 10/100/1000 Mbps ports (RJ45 connector)
USB Interface	1 x USB v2.0 Type-A
Management Interface(Web Console)	With Uplink port shared
Hardware Fail-over	Hardware bypass
Management Console interface	USB Type-C Console
Input Voltage	12/24/48 VDC
Input Current	0.483/0.241/0.127 A
Power Supply	Dual-power input (4-pin terminal block, V+, V-)
Operating Temperature	-40 to 75 °C (-40 to 167 °F)(Wide Temperature)
Ambient Relative Humidity	5 to 95% non-condensing
Non-operating / Storage Temp.	-40 to 85 °C (-40 to 185 °F)
Non-operating / Storage Relative Humidity	5 to 95% non-condensing
Vibration	IEC60068-2-6 (without any USB devices attached)
Mean Time Between Failure (MTBF)	700,000 hours +
Safety Certification	CE ,UL,UL 60950-1
Electromagnetic Compatibility	EMI: CISPR 32, FCC Part 15B Class A EMC: EN 55032/35, VCCI Class A
Green Product	RoHS, RoHS2, CRoHS, WEEE

Virtuális patchelés – agent nélküli védelem

Az IDS/IPS virtuális patchelést is biztosít, elfedve a munkaállomásokon vagy egyéb ipari eszközön levő sebezhetőségeket. Az eszköz aktívan blokkolni vagy monitorozni tudja a különböző sebezhetőségek kihasználási próbálkozásait. Így kiváló agent nélküli védelmet tud nyújtani olyan eszközök előtt, ahova nem lehet végpontvédelmi megoldást telepíteni.

Protokoll fehérlistázás

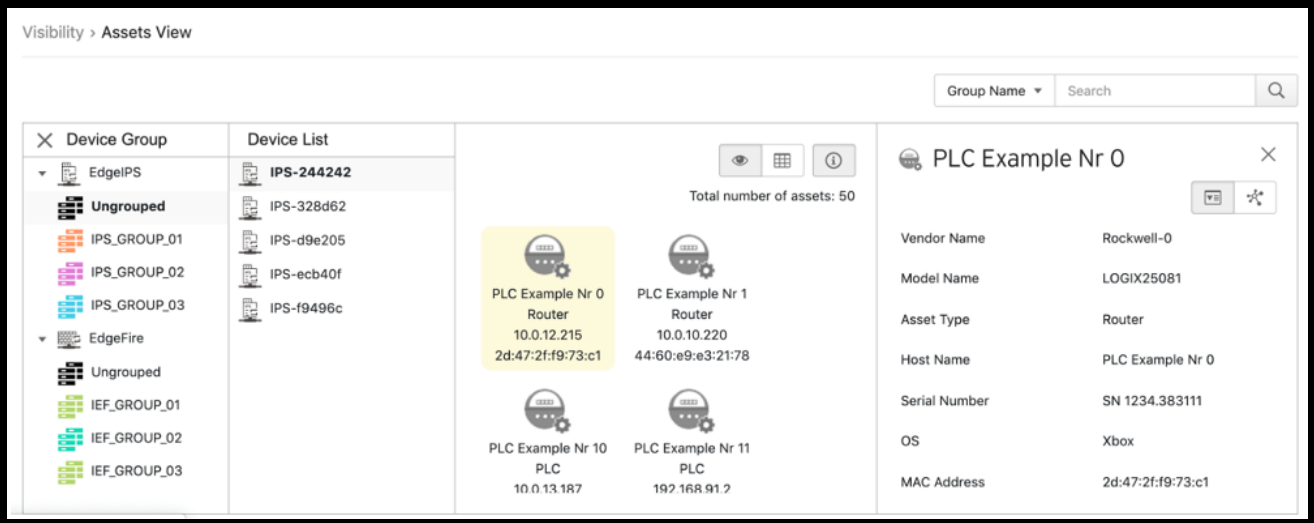
A leggyakoribb Modbus és Siemens S7 protokollok természetesen támogatottak és az EdgeIPS Deep Packet Inspectionnel tudja őket elemezni. Emellett rengeteg egyéb protokollt is támogatnak a TXOne eszközök, ahogyan az alábbi táblázatban látható:

2019		2020 1H	2020 2H
IT Protocols	OT Protocols		
	Factory Automation	Power & Electric	Oil / Gas
CDP	Modbus	OPC Classic(DA/AE/HAD)	DNP3
LLDP	EthernetIP/CIP	IEC 104	DCS protocols
DCE/RPC	Siemens S7COMM	GOOSE	OPC UA
DHCP V4	Siemens S7COMM Plus	MMS	FTE (Honeywell)
ARP	OMRON FINS	ICCP	Emerson Ovation DCS protocols
VNC	MITSUBISHI-SLMP	ABB Bailey	Emerson DeltaV DCS protocols
TFTP	SECS/GEM	ICCP TASE.2	Yokogawa VNet/IP
NTP	DNP3	GOOSE	GE Mark6e (SDI)
RDP	HART Protocol	IEC 62351	Schneider Foxboro
SSL	OMRON Fins	Bently Nevada	Triconex
NTLMSSP(Planning 2020)	Bechoff ADS	ANSI C12.18	
ATSVC	IEEE C37.118	Controll Area Network-CAN	
SMB-PIPE	IEC 61850-5		
TCP/IP	MITSUBISHI-SLMP		
SNMP	MELSOFT		
SSH	Modbus Schneider		
HTTP/HTTPS	CC-LINK IE		
Telnet	IEC 60870-5-104		
FTP	FATEK PLC		
SMB/CIFS	OPC UA		
ICMP	Niagara Fox		
IGMP	BACnet		
FTP			

A protokollokban használható parancsok részletesen testre szabhatók Modbus és S7 protokollok esetén is. Például készíthető olyan szabály, hogy egy munkaállomás csak read-only módon kommunikálhat Modbus felett a PLC eszközzel.

Asset információ gyűjtés

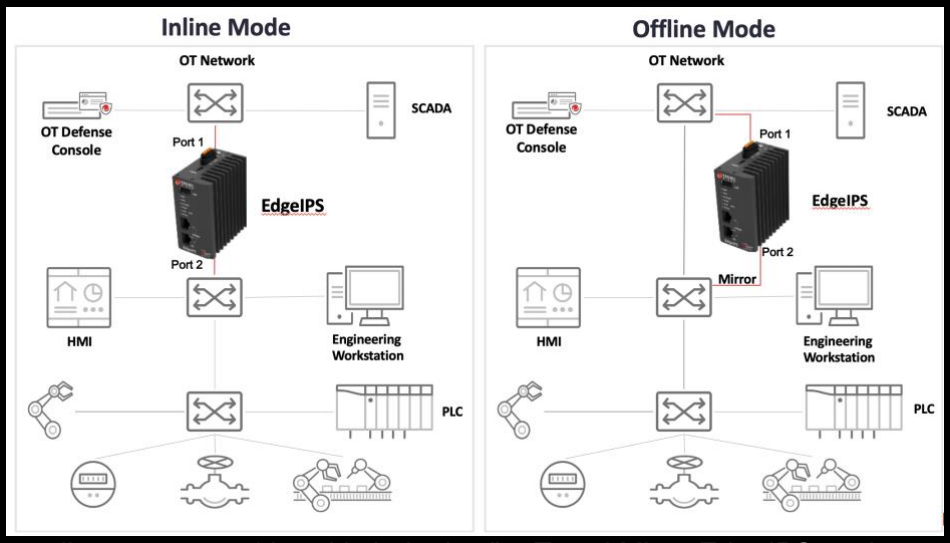
A TXOnne EdgeIPS és EdgeFire eszközök a hálózaton levő eszközökről asset információkat is gyűjthetünk. Ezen információk az eszközökön vagy a központi menedzsment felületén is megtekinthetők.



Példa asset információkra

IDS/IPS működési módok

Az EdgeIPS eszközök in-line, illetve out-of-band eszközként tükrözött forgalomra is beköthetők. A különböző illesztési módokat az alábbi ábra mutatja be. Inline módban is lehet választani IPS (detektál és blokkol) és IDS (csak detektál) módok között, illetve köszönhetően a bypass interfészeknek áramkimaradás esetén is folyamatos hálózati forgalmat biztosít az eszköz.



In-line vagy out-of-band is beköthető a Trend Micro EdgeIPS eszköze

Ipari hálózatvédelem – Trend Micro TXOne EdgeIPS Pro

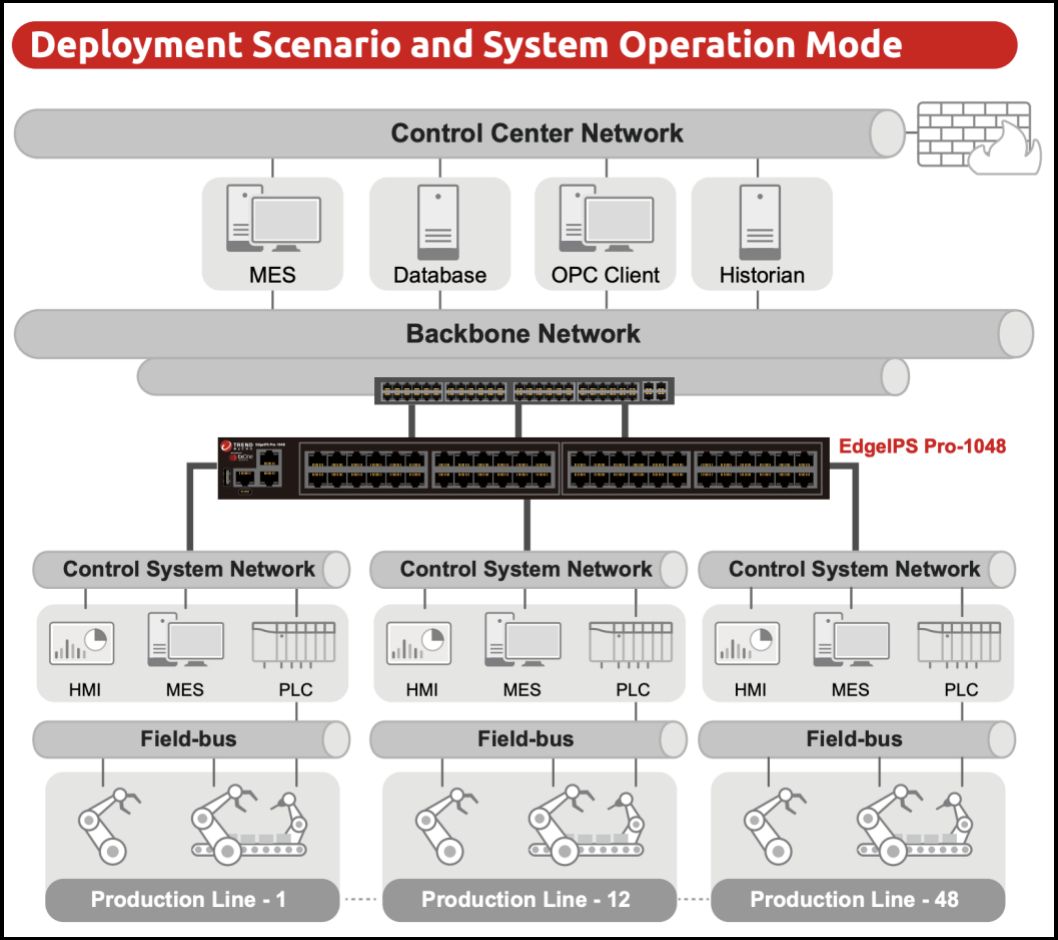
Az EdgeIPS Pro egy kiberbiztonsági eszköz, amelyet nagyméretű gyártósorokhoz terveztek. Az iparág vezetőitől származó visszajelzések alapján készült, és natívan támogatja az operatív technológia (OT) több szegmensét. Az EdgeIPS Pro-t alkalmazó gyárak és munkahelyek élvezhetik a központosított felügyelet, a működési folytonosság, a műhelyvédelem és a rugalmas telepítés előnyeit.

Nagy port sűrűségű IPS tömb az OT maghálózat védelméhez.

Az EdgeIPS Pro™ szabványos 1U rack-tartóval rendelkezik 48 porttal, vagy 2U-os rack-tartóval 96 port-tal a nagyüzemi gyártáshoz. A modulkártya rugalmas a különböző hálózati stratégiákhoz. Az EdgeIPS Pro a monitor és a megelőzési módok között vált a legjobb belső védelem vagy a zavartalan biztonsági tudatosság érdekében.

Nagy teljesítményű

A gyártósoron lévő eszközöknek késedelem nélkül kell kommunikálniuk. Az EdgeIPS Pro nagy teljesítményű kialakítása korlátozza a laterális mozgást, tehát egy esetlegesen fertőzött végpontról, másik végpontra való átlépést és megakadályozza a kibertámadást, miközben minimalizálja a késleltetést. Az 1U EdgeIPS Pro 1048 10 Gb/s-on, a 2U EdgeIPS Pro 2096 pedig 20 Gb/s-on teljesít, bekapcsolt fenyegetésmegelőzés mellett.



Syslog integráció SIEM/SOAR rendszer felé

Az EdgeIPS/IPS Pro eszközöknek fontos szerepe van az OT környezetben lévő forgalom szűrésében, az ott lévő adatforgalom analizálásában, gyanús hálózati forgalmak minta típusú detektálásában, korrelációjában és fenyegetettségi intelligencia vizsgálat meghatározásában, akár protokoll specifikus módon, a lehető legszélesebb körben támogatott OT protokollokon keresztül.

Az itt lévő gyanús események, támadási kísérletek vagy éppen konkrét incidensek monitorozása, naplózása vagy adott esetben blokkolása kritikus a termelésirányítási rendszerek megvédése szempontjából.

Napjainkban az erős IT-OT konvergencia következtében kulcskérdéssé vált az OT rendszereink átláthatósága és kontrollja. Ezért kiemelten fontos, hogy a keletkezett riasztásokat, eseményeket el tudjuk juttatni olyan SIEM/SOAR rendszerek irányába is, melyek elsősorban a vállalat belső infrastruktúrájából gyűjtenek és elemeznek logokat és riasztásokat, közvetlenül az OT környezetből nem, így azok úgynevezett vakfoltok (blind spot) lesznek. Így sem átláthatóság, sem pedig kontroll nem lesz esetleges gyanús vagy valós incidensekről, veszélyeztetve ezzel az üzembiztonságot.

Az Edge ISP megoldás természetesen rendelkezik Syslog alapú integrációval, ahol a különféle konfigurációs, működési, rendszer és biztonsági eseményeket tudja továbbítani.

Ipari hálózatvédelem – Trend Micro TXOne EdgeFire

Inline fenyegetés elleni védelem, gyártósorok, gépészeti rendszerek folyamatos működéshez, kulcsfontosságú eszközök védelmére, valós idejű reagálással az eseményekre.

Az EdgeFire következő generációs tűzfal lehetővé teszi a hálózati szegmentálást és szeparálást, hogy a hálózatot különböző vezérlési zónákra ossza, akár a cellák szintjéig is. A kritikus eszközök számára hálózati hozzáférés-ellenőrzést és hálózati támadás megelőzést kínáló EdgeFire a mélyreható kiberbiztonsági védelmet szolgálja, hogy egyszerűsítse az OT napi működését.

Fenyegetések detektálása és kivédése következő generációs tűzfaltechnológiával, különösen a férgek terjedésének megakadályozására:

- Azonnali és folyamatos fenyegetésvédelmet biztosít rugalmas telepítési lehetőségeken keresztül, amelyek lehetővé teszik az egyszerű telepítést és kezelést a központosított kezelőfelületen.
- Védelem a sebezhető, nem patch-elt eszközök és öröklött rendszerek számára.
- Védi az eszközöket az OT exploit-okkal szemben, szignatúra alapú virtuális patch-eléssel.
- Szegmentálást alkalmaz a gyártási zónák létrehozásához, hogy csökkentse a működési hibákat és kibertámadások okozta károkat.

EdgeFire™ Specifications

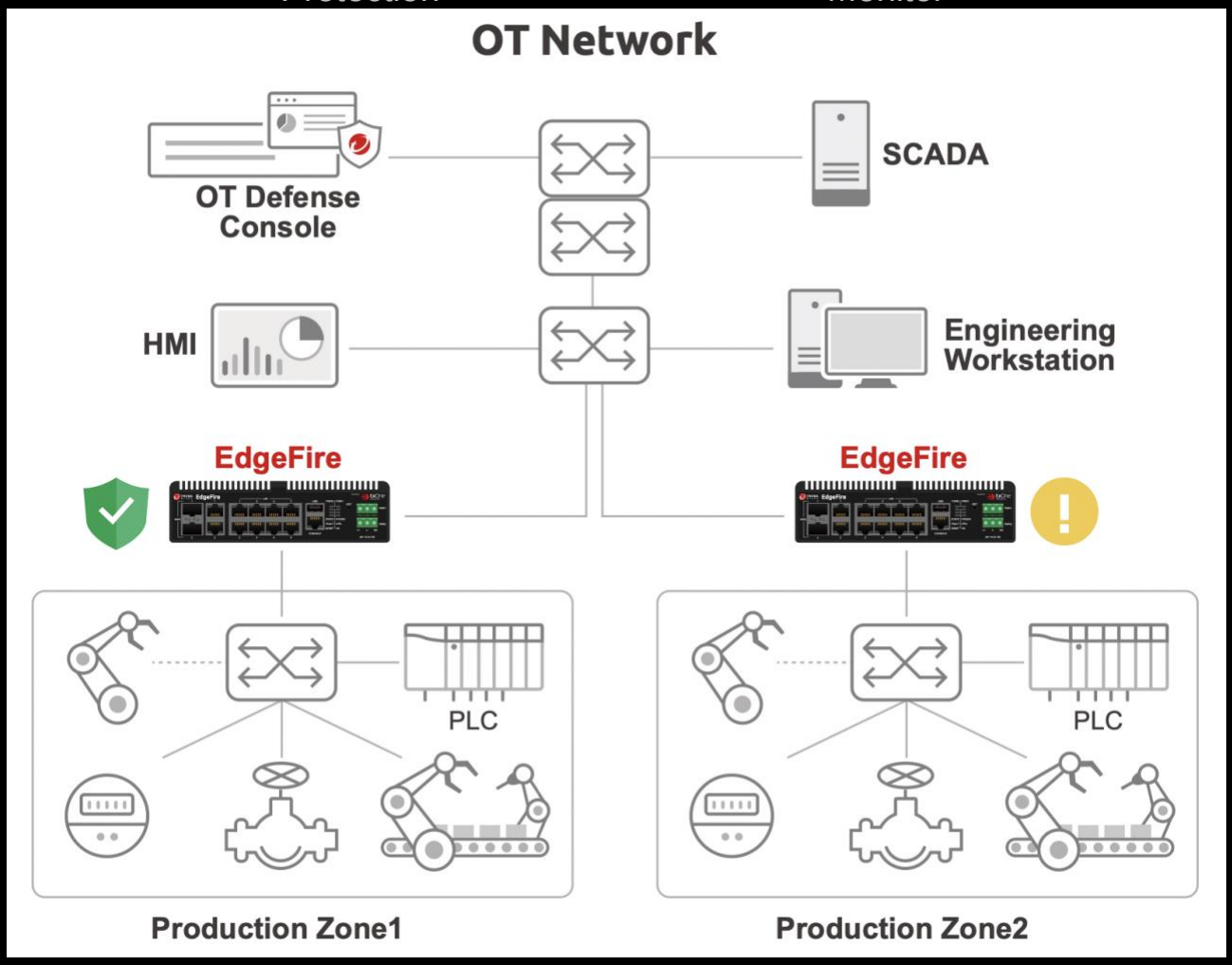
Feature	EdgeFire 1012
Supported IPS Throughput	200Mbps at least (IMIX) / 600Mbps (UDP 1518 bytes)
Latency	<500 microseconds
Concurrent Connection (TCP)	100,000
Supported ICS Protocol	Modbus / EtherNet IP / CIP / FINS / S7Comm/ S7comm+/ TOYOPUC, with more being added regularly
Policy Enforcement Rules	512 Rules (L3 Policy Enforcement Rules in gateway/bridge mode) 256 Rules (L2 Policy Enforcement Rules in bridge mode)
ICS Protocol Filter Profiles	64 Profiles
VPN	Max. concurrent IPSec VPN tunnels: 50 VPN Tunnels Site-to-Site VPN / Client-to-Site VPN Protocol: IPSec (IKEv1, IKEv2), L2TP over IPSec VPN Throughput: 50 Mbps
Form Factor	DIN-rail mounting and wall mounting (with optional kit)
Weight (Standalone Device)	1381g (3.044 lb)
Dimensions (W x D x H)	180mm x 120mm x 50mm (7.09 x 4.72 x 1.97 in)
Network Interface Type	8 x Auto-sensing 10/100/1000 Mbps ports (RJ45 connector) 2 x 100/1000 fiber optic ports and 2 x Auto-sensing 10/100/1000 Mbps Copper ports (Combo)
USB Interface	1 x USB v2.0 Type-A
Management Interface (Web Console)	LAN Interface
Management Console Interface	RJ-45 Console
Power Input	9/12/24/48 VDC, Dual Redundant Inputs (2 x 3 Pin Terminal Block, located in front panel); Reverse Polarity Protection Supported. (* 12V VDC Recommended)
Input Current (A)	1.8/1.35/0.68/0.35A
Power Supply	Dual Power input, total 6 pin terminal block
Operating Temperature	-40 to 75 °C (-40 to 167°F)(Wide Temperature)
Ambient Relative Humidity	5 to 95% non-condensing
Non-operating / Storage Temp.	-40 to 85 °C (-40 to 185 °F)
Non-operating / Storage Relative Humidity	5 to 95% non-condensing
Vibration	IEC 60068-2-6, IEC 60068-2-27, IEC 60068-2-64 (without any USB devices attached)
Mean Time Between Failure (MTBF)	700,000 hours +
Safety Certification	CE, UL, UL 60950-1
Electromagnetic Compatibility	EMI: CISPR 32, FCC Part 15B Class A EMC: EN 55032/35, VCCI Class A
Green Product	RoHS, RoHS2, CRoHS, WEEE

Protection/Monitor működési módok

Protection mód:
Az EdgeFire inline módban van telepítve (a forrás és a cél eszköz közvetlen kommunikációjában), ahol aktívan elemzi a forgalom áramlását, naplózza az eseményeket, és automatizált intézkedéseket hoz a rosszindulatú események megelőzésére.

Monitor mód:
Az EdgeFire inline módban van telepítve (a forrás és a cél eszköz közvetlen kommunikációjában), ahol aktívan elemzi a forgalom áramlását, és csak naplózza az eseményeket anélkül, hogy bármilyen intézkedést tenne, amikor rosszindulatú eseményeket észlel.

Protection Monitor



Az EdgeIPS eszközökhöz hasonlóan, szintén része a rendszernek a:

- Virtuális patch-elés – agent nélküli védelem
- Protokoll fehérlistázás
- Asset információ gyűjtés

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

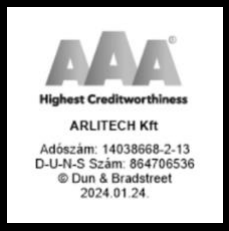
Az ARLITECH bemutatása

Az ARLITECH legfontosabb célja, hogy Ügyfelei a lehető legnagyobb biztonságban tudhassák információikat, adataikat. Ehhez nyújt high-end megoldásokat, a legkorszerűbb technikai háttérrel támogatva.

Csapata olyan IT szakemberekből áll, akik az eddig megszerzett tapasztalataikkal, szakmai tudásukkal a legmagasabb minőségű megvalósítást garantálják.

Az ARLITECH szolgáltatásainak portfoliója a technológiákkal együtt folyamatosan változik. Ezek a szolgáltatások tudatos tervezésen és az Ügyfelek igényein alapulnak. Az ARLITECH sikere azon gyakorlatias hozzáálláson alapul, hogy egyszerre kíván megoldást nyújtani ügyfelei azonnali és hosszú távú informatikai kihívásaira.

Az ARLITECH a magyarországi vállalkozások azon kivételes körébe tartozik, mely megfelelt a Dun & Bradstreet nemzetközi minősítési rendszere által támasztott legszigorúbb feltételeknek. AAA Silver.



Alapítva 2007-ben.

Szolgáltatások:

- IT biztonság
- IT/OT rendszerintegráció
- NIS2
- IT/OT üzemeltetés
- Audit
- SOC
- Oktatás

Elérhetőségek:

Web: www.arlitech.hu
Email: info@arlitech.hu
Facebook: https://www.facebook.com/arlitech.official
X: https://twitter.com/arlitech
Linkedin: https://hu.linkedin.com/company/arlitech
WhatsApp: https://whatsapp.com/channel/0029VaQKLxI0AgW9CfNXof2c
Instagram: arlitech.official
Telefon: +36 30 3119042

Referenciák:

MTE (Magyar Táncművészeti Egyetem),
NIF (Nemzeti Infrastruktúra Fejlesztő Zrt.),
MÜPA,
Korda filmstúdió,
OBH (Országos Bírósági Hivatal, az összes bíróság),
Országos Igazságszolgáltatási Tanács Hivatala, (OITH)
NNK (Nemzeti Népegészségügyi Központ, volt ÁNTSZ)
FÖMI (Földmérési és Távérzékelési Intézet, az összes földhivatal,
HMEI (Honvédelmi Minisztérium Elektronikai Igazgatóság),
MKEH (Magyar Kereskedelmi és Engedélyezési Hivatal),
SZTNH (Szellemi Tulajdon Nemzeti Hivatala),
MFB (Magyar Fejlesztési Bank),
Magyar Nemzeti Vagyonkezelő (MNV)
Állami Vagyonnyilvántartási Kft. (ÁVNY)
Magyar Bírósági Végrehajtói Kar (MBVK)
KNAUS,
TriGranit,
Westend,
Accenture,
Topin-hub,
Askance,
Szegedi Vízmű,
KÖBE Közép-európai Kölcsönös Biztosító Egyesület,
Emberbarát Alapítvány,
Gödöllői Polgármesteri Hivatal,
Gödöllő Város Önkormányzata,
Future Films Hungary,
Zalakerámia
Iskolák, ovodák, bölcsödék
Önkormányzatok
…