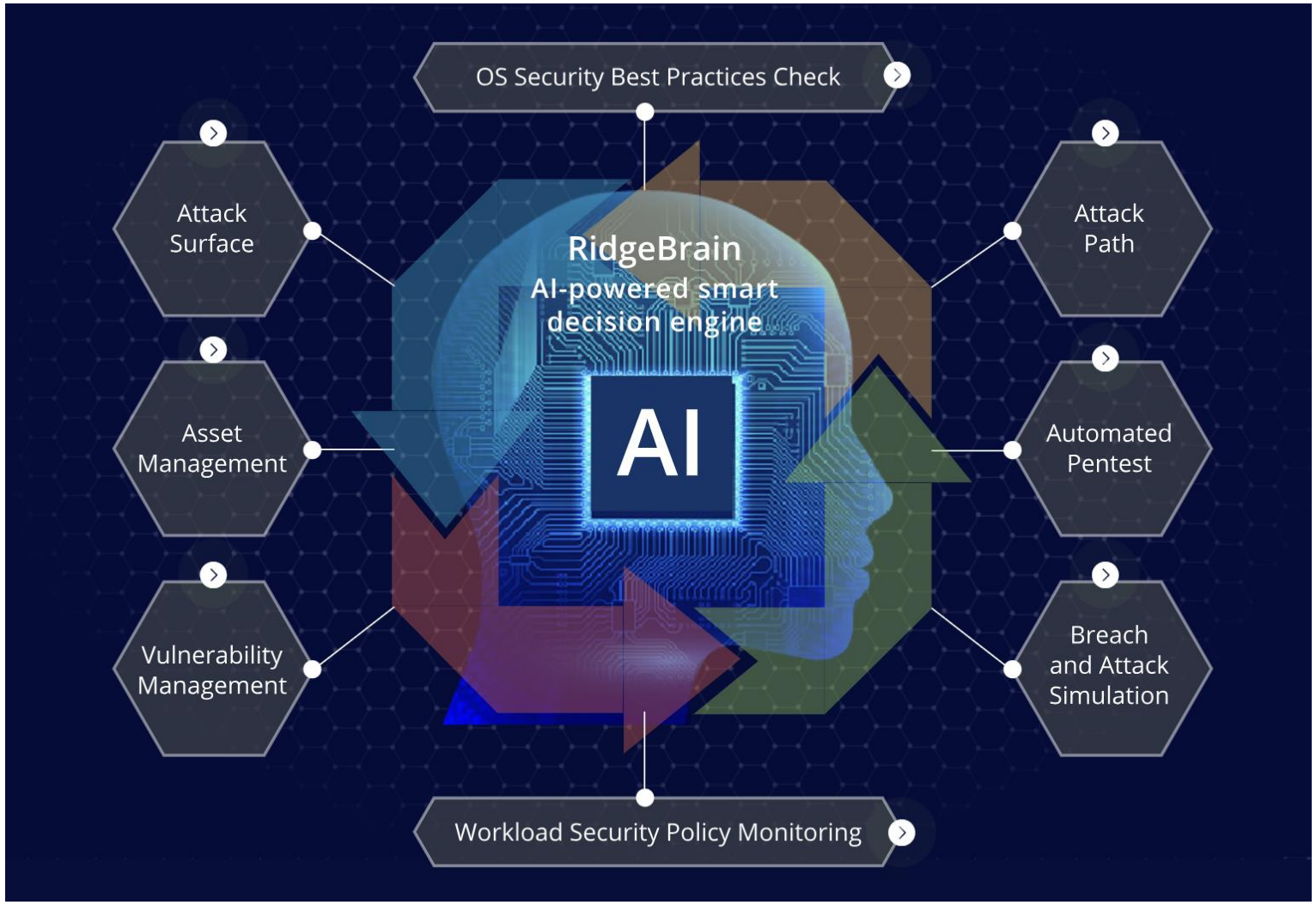
Ridgebot - a fejlett automatizált penetrációs tesztelő eszköz



🔒 **Automatizált penetrációs tesztelés**
A Ridgebot csúcstechnológiás AI-t használ, hogy automatikusan végezzen átfogó penetrációs teszteket, azonosítsa a sebezhetőségeket és biztosítson cselekvési javaslatokat.

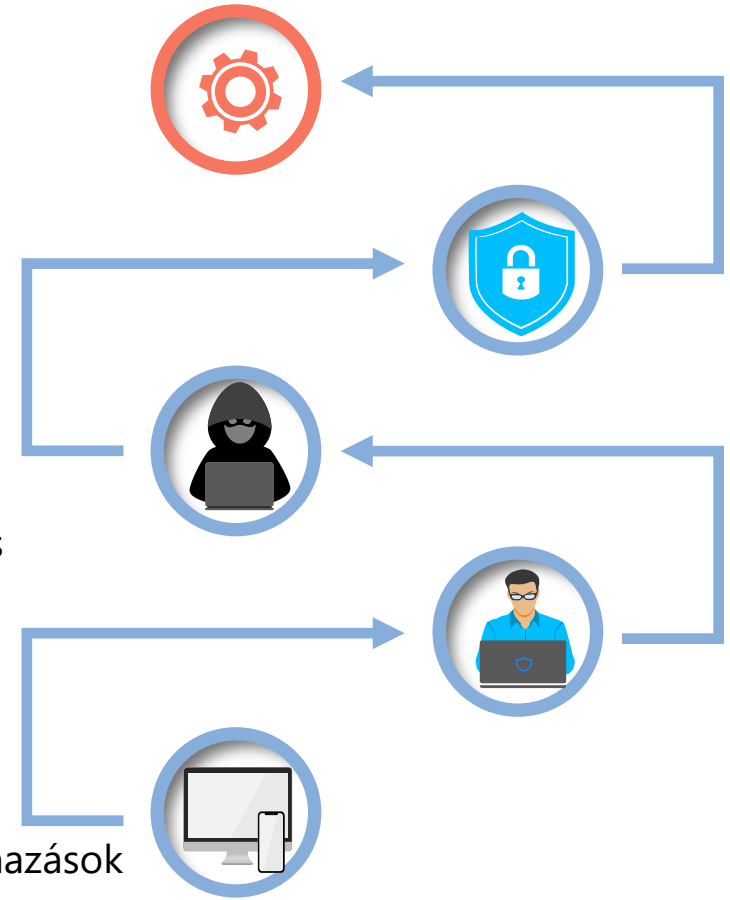
🧠 **AI szabadalom**
A megbízható AI szabadalommal támogatva a Ridgebot biztosítja a precíz és intelligens fenyegetés-felismerést és -elhárítást.

⚙️ **Fenyegetettség kitettségének kezelése**
Hatékonyan kezeld és mérsékeld a fenyegetettségeket a Ridgebot átfogó kezelőrendszerével, hogy vállalkozásod biztonságban maradjon.

Ridgebot által lefedett feladatok

Automatizált Behatolás Tesztelés

- Eszközprofilozás
- Sebezhetőségfeltárás
- Automatikus Kihasználás
- Kihasználás utáni tevékenységek
- Hitelesített Behatolás
- Oldalirányú Mozgás
- Behatolás Tesztelési Kockázatkezelés



Biztonsági Ellenőrzések Validálása

- Érzékeny Adatok Kiszivárogtatása
- Végpont Biztonság
- Windows AD Szabályzat Ellenőrzés
- Folyamatos Mérés
- Mitre Att&ck Keretrendszer Összehangolás

Kockázatalapú Sebezhetőségkezelés

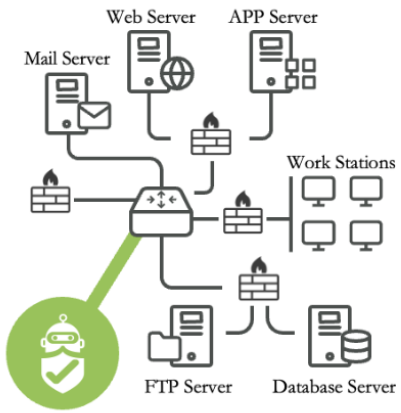
- Támadási Lánc Vizualizáció és Kihasználási Bizonyítékok
- Egészségügyi Pontszám, Kockázatok és Sebezhetőségek Priorizálása
- Kockázati és Sebezhetőségi Részletek és Kezelési Javaslatok
- Harmadik Fél VA Szkenner Integráció
- OWASP Top-10 Jelentéskészítés
- VM Historikus/Trend Elemzés

Eszközkezelés

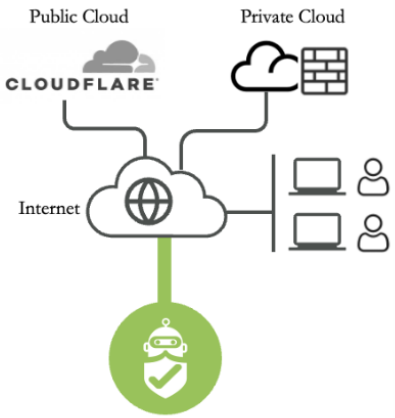
- Hosztok és szolgáltatások/alkalmazások
- Weboldalak és domainek
- Botlet telepítés és állapot
- Támadási felületek azonosítása

PRIANTO

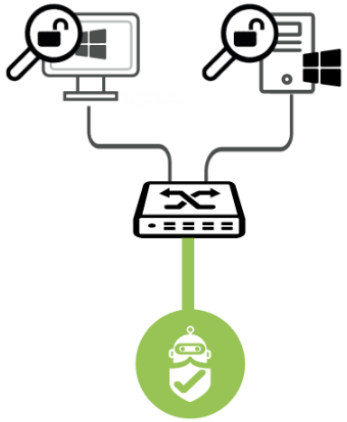
Internal Attack



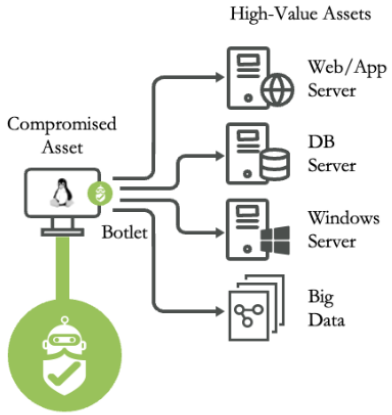
External Attack



Authenticated Penetration



Lateral Movement



	RidgeBot®	**Számos versenytárs (hagyományos folyamatok)**
Validált kockázatok *	Teljesen automatizált behatolásvizsgálat, amely felderíti és megjelöli a validált kockázatokat a SOC csapatok általi javítás érdekében. A teszt NEM igényel magasan képzett személyzetet.	Különböző eszközök által támogatott manuális folyamat a tesztelendő lehetséges célok azonosítására. Magasan képzett tesztelőket igényel, és sokkal hosszabb időt vesz igénybe.
Folyamatos tesztelés	A RidgeBot® egy fáradhatatlan szoftverrobot, amely havonta, hetente vagy akár naponta is képes biztonsági validációs feladatokat futtatni, és historikus trendjelentést készíteni. Folyamatos nyugalmat biztosít ügyfeleink számára.	Túl lassú és drága ahhoz, hogy negyedévente vagy évente többször megismételjük.
Biztonsági helyzetértékelés	Értékelje biztonsági házirendjei hatékonyságát a Mitre Att&ck keretrendszer szerinti emulációs tesztek futtatásával.	A kék csapat mindent megtesz annak érdekében, hogy a biztonsági eszközök megfelelően legyenek konfigurálva, de validációs tesztek nélkül.
Sebezhetőségek kezelése	Elsőbbséget élveznek azok a biztonsági rések, amelyeket a szervezetében egyértelmű bizonyítékokkal alátámasztva kihasználnak. Ez nulla téves riasztást jelent.	Minden lehetséges biztonsági rést bemutat validálás nélkül, ami magas téves riasztási arányhoz vezet.

* Minden RidgeBot® által validált kockázat azt jelenti, hogy a biztonsági rést egy hacker ki tudja használni az adott hálózati és szerverkonfigurációban. A RidgeBot valós POC kódok használatával validálja a biztonsági réseket a sebezhetőség kihasználása érdekében. Az ügyfél SOC mérnökeinek azonnal meg kell szüntetniük a kockázatot.

Esettanulmányok

IDŐ vs. KÖLTSÉG vs. ELÉRHETŐSÉG vs. KOMPLEXITÁS vs. FOLYTONOSSÁG

Tocumen International Airport Chooses RidgeBot Automated Pentesting for More Secure, Agile, and Resilient Security Operations

The airport encountered significant security challenges deploying new systems into production and changing existing systems. With dozens of critical applications, Tocumen absorbed cyberattacks daily.

Capital Assets Exceeding $1B (USD) With More Than 1M Customers

A commercial bank serving the ASEAN countries, had an IT infrastructure consisting of mainly Windows® Servers in a virtualized environment, hosting several external websites that they secured with an PS and firewalls in High Availability mode.

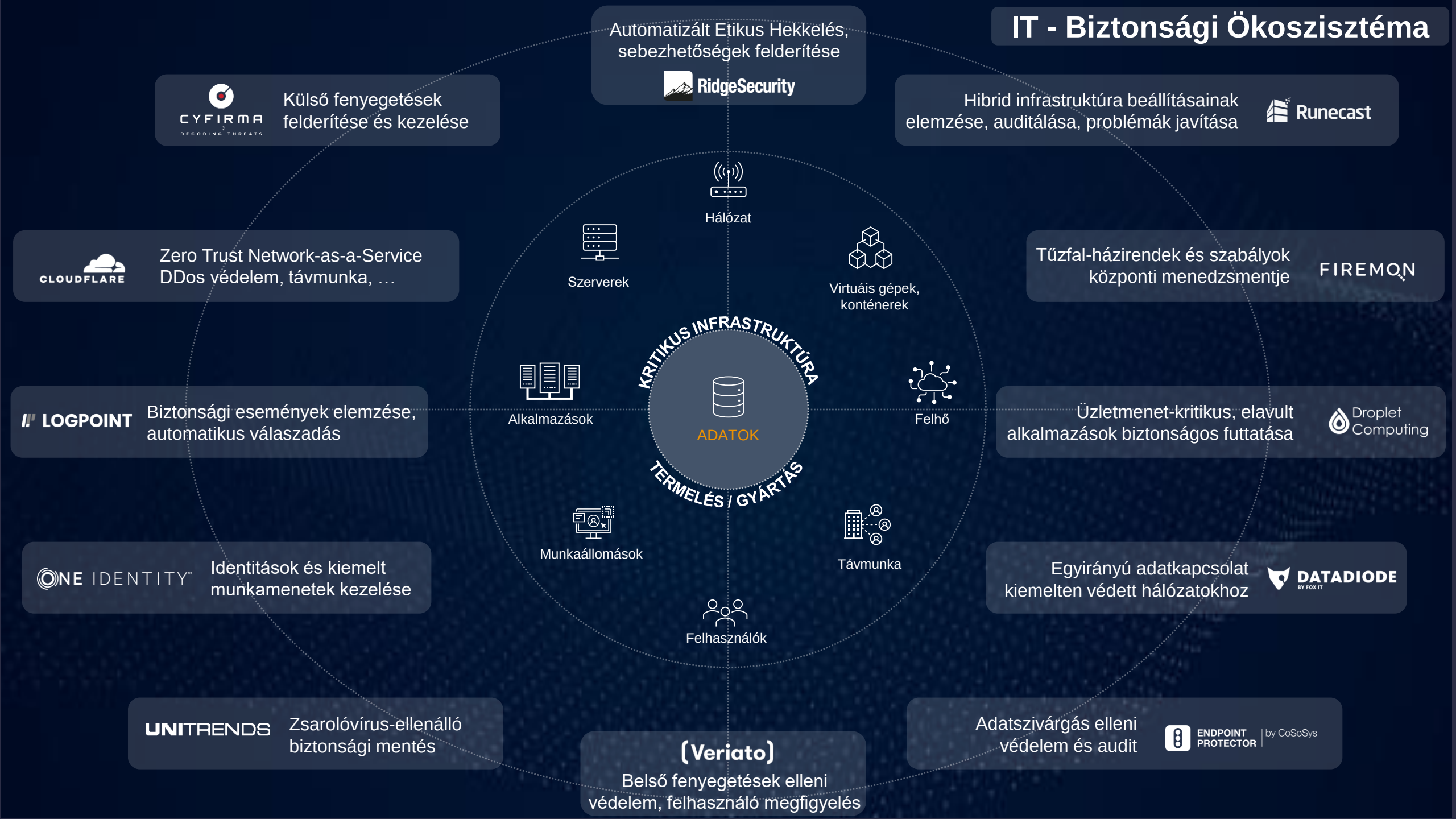
Enhancing Supply Chain Operational Resilience in the Logistics Sector with CTEM

As a large conglomerate, the customer confronts formidable challenges when safeguarding operations and minimizing risks across its vast logistical services. Maintaining uninterrupted solutions is crucial for seamless logistics.

Enabling PCI DSS through Automated Penetration Testing

A leading payment gateway provider complies with PCI DSS Level 1, using RidgeBot® for automated penetration testing. With 100 IP licenses and 10 web licenses, it ensures secure transactions and meets PCI DSS requirements.

IT - Biztonsági Ökoszisztéma



Automatizált Etikus Hekkelés, sebezhetőségek felderítése
RidgeSecurity

CYFIRMA DECODING THREATS
Külső fenyegetések felderítése és kezelése

Hibrid infrastruktúra beállításainak elemzése, auditálása, problémák javítása
Runecast

CLOUDFLARE
Zero Trust Network-as-a-Service
DDos védelem, távmunka, …

Tűzfal-házirendek és szabályok központi menedzsmentje
FIREMON

LOGPOINT
Biztonsági események elemzése, automatikus válaszadás

Üzletmenet-kritikus, elavult alkalmazások biztonságos futtatása
Droplet Computing

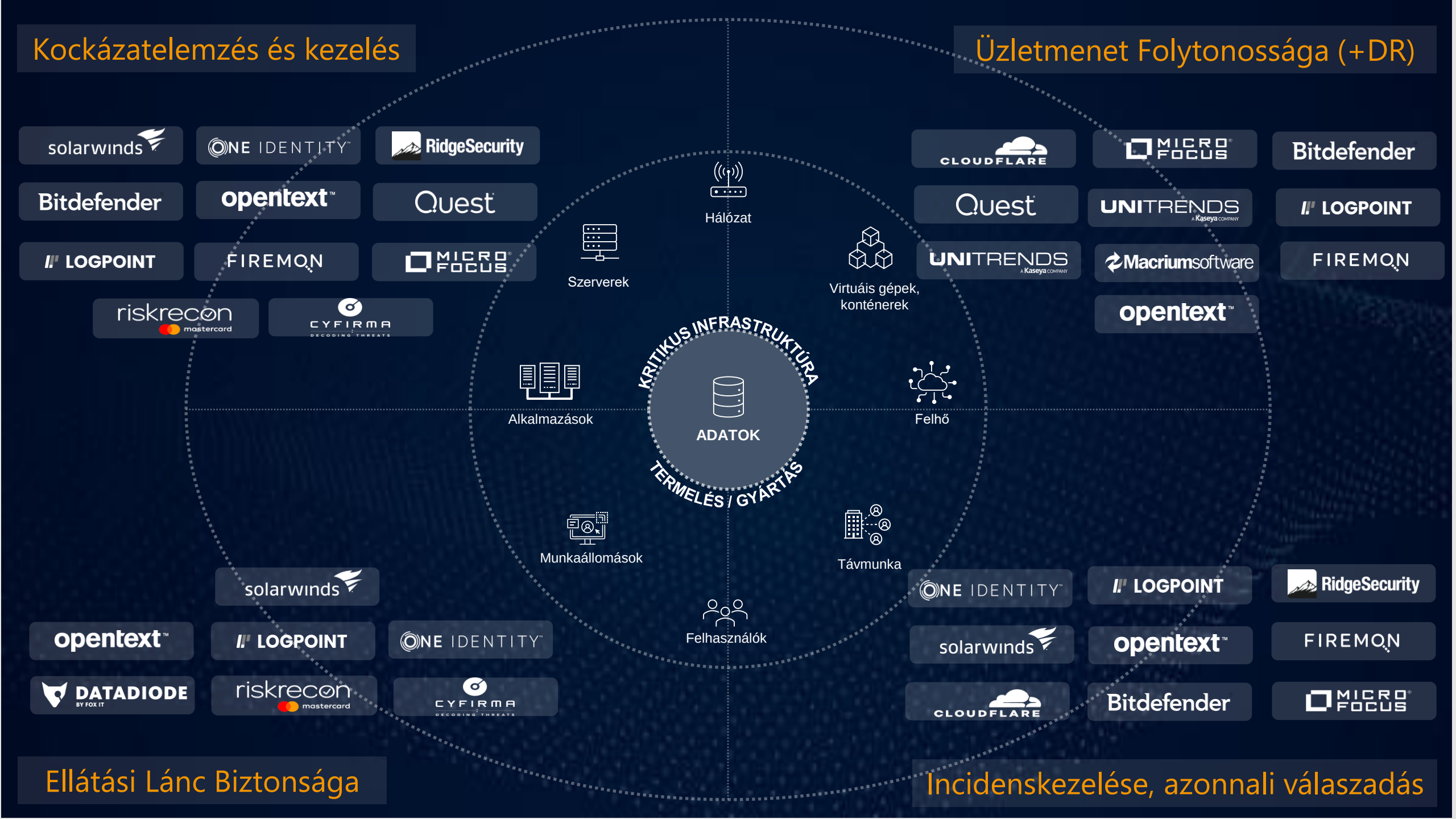
ONE IDENTITY
Identitások és kiemelt munkamenetek kezelése

Egyirányú adatkapcsolat kiemelten védett hálózatokhoz
DATADIODE BY FOX IT

UNITRENDS
Zsarolóvírus-ellenálló biztonsági mentés

Adatszivárgás elleni védelem és audit
ENDPOINT PROTECTOR | by CoSoSys

(Veriato)
Belső fenyegetések elleni védelem, felhasználó megfigyelés


Kockázatelemzés és kezelés
Üzletmenet Folytonossága (+DR)
solarwinds
ONE IDENTITY
RidgeSecurity
Bitdefender
opentext
Quest
LOGPOINT
FIREMON
MICRO FOCUS
riskrecon
mastercard
CYFIRMA
DECODING THREATS
CLOUDFLARE
MICRO FOCUS
Bitdefender
Quest
UNITRENDS
A Kaseya COMPANY
LOGPOINT
Macriumsoftware
FIREMON
opentext
Hálózat
Szerverek
Virtuális gépek, konténerek
Alkalmazások
KRITIKUS INFRASTRUKTÚRA
ADATOK
TERMELÉS / GYÁRTÁS
Felhő
Munkaállomások
Távmunka
Felhasználók
solarwinds
opentext
LOGPOINT
ONE IDENTITY
DATADIODE
BY FOX IT
riskrecon
mastercard
CYFIRMA
DECODING THREATS
ONE IDENTITY
LOGPOINT
RidgeSecurity
solarwinds
opentext
FIREMON
CLOUDFLARE
Bitdefender
MICRO FOCUS
Ellátási Lánc Biztonsága
Incidenskezelése, azonnali válaszadás

PRIANTO

Miért a Prianto?

Gyors, rugalmas, megbízható

Az ügyfélközpontúság és a gyorsaság alapelveink, melyek mentén a vállalat minden szintjén hatékony, bürokráciamentes és eredményorientált munkát végzünk.

Nemzetközi szakértői hálózat

17 nemzetközi irodánk garantálja a Prianto egyszerű és szakképzett szoftverdisztribúciós szolgáltatásait, amelyek korszerű vállalati szoftvermegoldásokkal párosulnak.

Tapasztalt szakmai csapat

Magasan kvalifikált és segíteni akaró csapatunk alapos ismerettel rendelkezik a szakmában. Ügyfeleinkért mindig megtesszük az extra mérföldet!

Innovatív újgenerációs piacvezető technológiák

Előrelátóan követjük a következő generációs trendeket, legyen szó IT biztonságról, digitalizációról, adatvagyongazdálkodásról vagy felhő/MSP megoldásokról.

Üzleti és technológiai szemlélet kombinációja

Partnereink számára olyan profitábilis üzleti lehetőségeket azonosítunk, melyek tökéletesen egybevágnak vállalkozási céljaikkal és üzleti stratégiájukkal.

Vonzó kereskedelmi kondíciók és költséghatékony megoldások

Piacvezető megoldásaink magas fedezet és attraktív kondíciók mellett érhetőek el, minden szükséges támogatást biztosítva a sikeres projekt érdekében

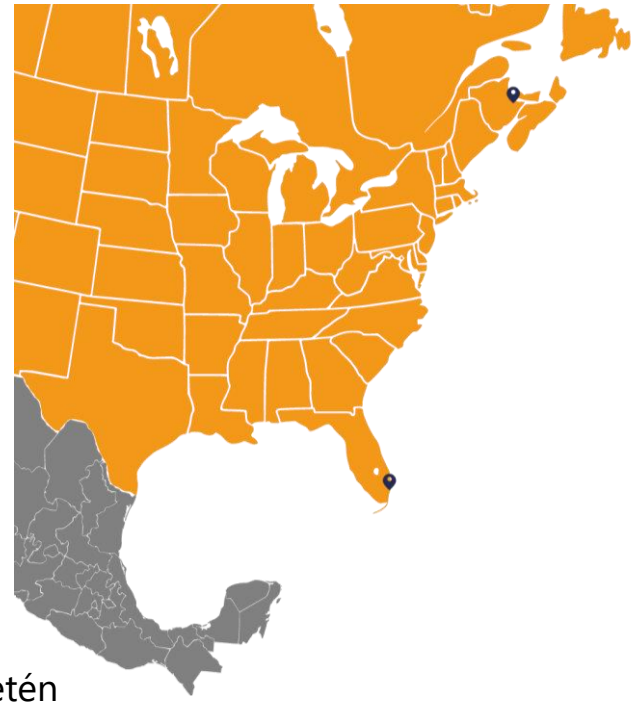
Köszönöm a figyelmet!

PRIANTO
Értéknövelt szoftverdisztribútor

Urzica Olivér / CEO
Mob: +36 70 418 7177
Email: oliver.urzica@prianto.com

Prianto Csoport

Értéknövelt szoftverdisztribútor, nagyvállalati IT megoldások és gyártók képviselője
Kiemelt területek: IT biztonság, virtuálizáció, digitális transzformáció, cloud-SaaS, infrastruktúra kezelés, adatvagyongazdálkodás
2009-ben alapította William Geens és Oliver Roth
Forgalom 2023: 180M EUR
Magántulajdon, tőke: 4M EUR
Alkalmazottak száma: 175
17 iroda-képviselet Európa és Észak Amerika területén



Prianto Csoport:

- 2011 – Prianto UK, Prianto Switzerland
- 2012 – Prianto Austria, Prianto BeNeLux
- 2014 – Prianto Poland
- 2016 – Prianto France
- 2017 – Prianto Czechia, Hungary, Adriatics
- 2019 – Prianto Canada
- 2021 – Prianto USA, Prianto Türkiye
- 2022 – Prianto Romania and Slowakia
- 2023 – Prianto Nordics
- **2023 – Prianto Hungary Kft.** megalapítása

Szolgáltatásaink

Szoftver disztribúció

MSP szolgáltatás

Szoftver-beszerzés

Üzletfejlesztés

Értékesítés

Tanácsadás

Pre-Sales

Marketing támogatás

Kompetencia központ

Műszaki támogatás

Ipar 4.0

Kibervédelem

Implementáció

Képzések

Teszt-rendszerek, POC

Digitalizáció

PRIANTO

PRIANTO „**NEURON-HÁLÓZATA**"

Végfelhasználók

MSP/SOC szolgáltatók

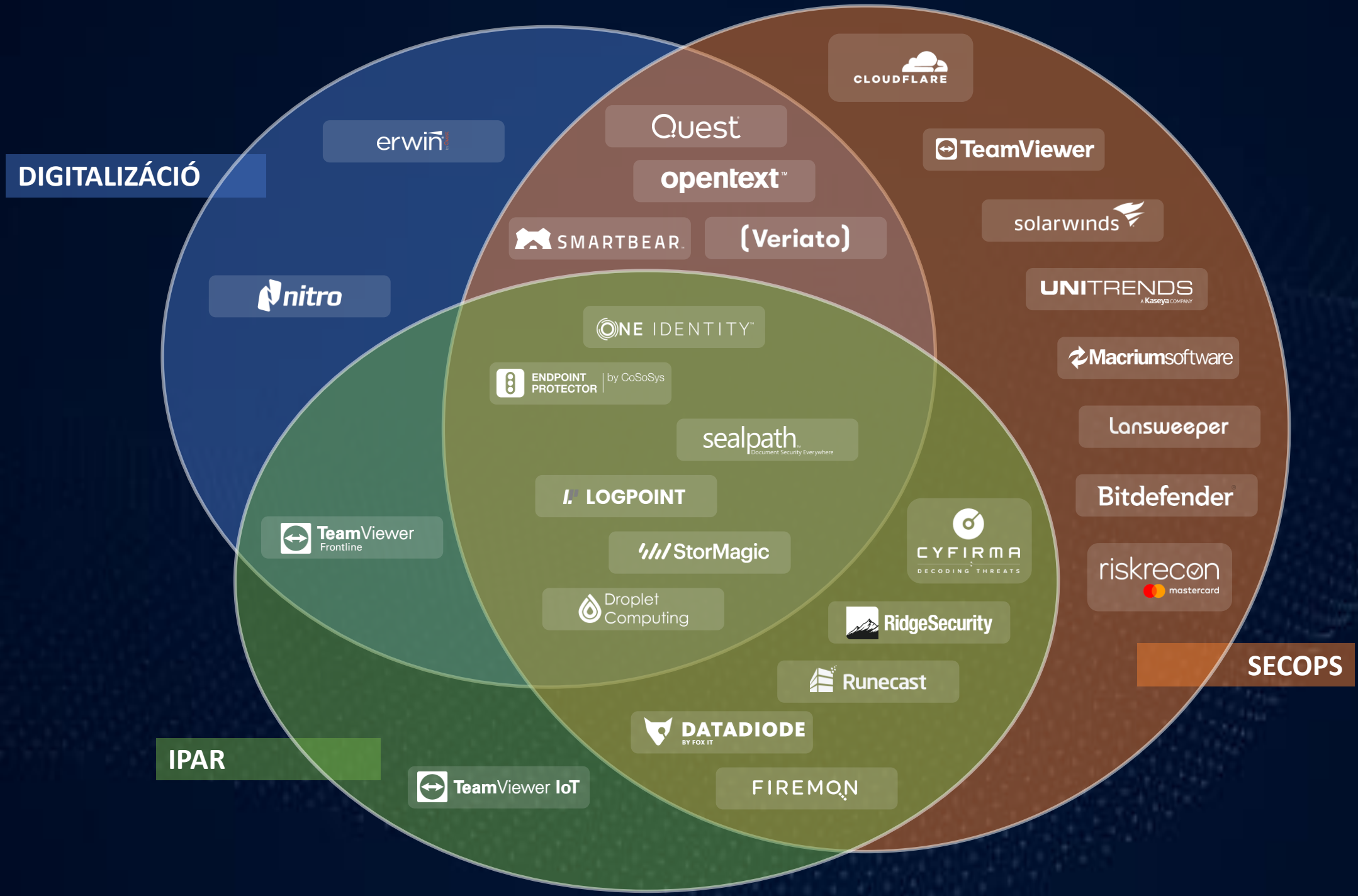
IT szállítók

Hatóságok

Szakértők, auditorok

Vendorok

Felmérés → Tanácsadás → Tervezés → Tesztelés → Implementálás → Támogatás


DIGITALIZÁCIÓ
erwin
nitro
Quest
opentext™
SMARTBEAR
(Veriato)
CLOUDFLARE
TeamViewer
solarwinds
UNITRENDS
A Kaseya COMPANY
Macriumsoftware
Lansweeper
Bitdefender
riskrecon
mastercard
SECOPS
ONE IDENTITY
ENDPOINT PROTECTOR | by CoSoSys
sealpath
Document Security Everywhere
LOGPOINT
StorMagic
Droplet Computing
CYFIRMA
DECODING THREATS
RidgeSecurity
Runecast
DATADIODE
BY FOX IT
FIREMON
TeamViewer Frontline
TeamViewer IoT
IPAR

SZOLGÁLTATÁS & TERMÉK PORTFÓLIÓ