Teljes körű IT infrastruktúra menedzsment: Megfigyelhetőség, javítás és ellenőrzés

PRIANTO

Cybersecurity & Digitalisation Software Distributor

Urzica Olivér – Regionális ügyvezető
oliver.urzica@prianto.com

2024.08.06, Budapest

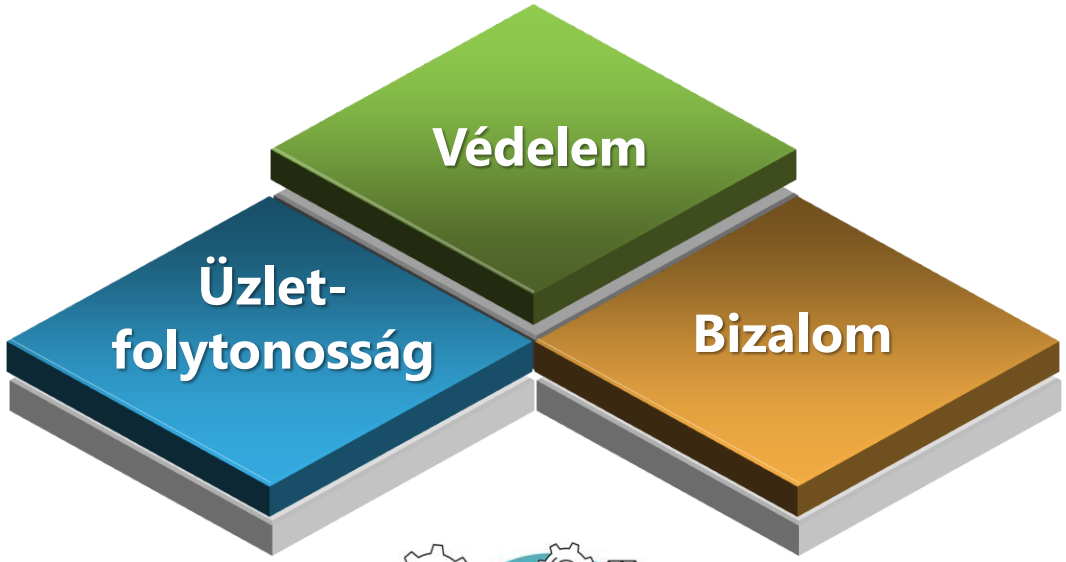
PRIANTO

KIBERBIZTONSÁGI kitekintés 2024

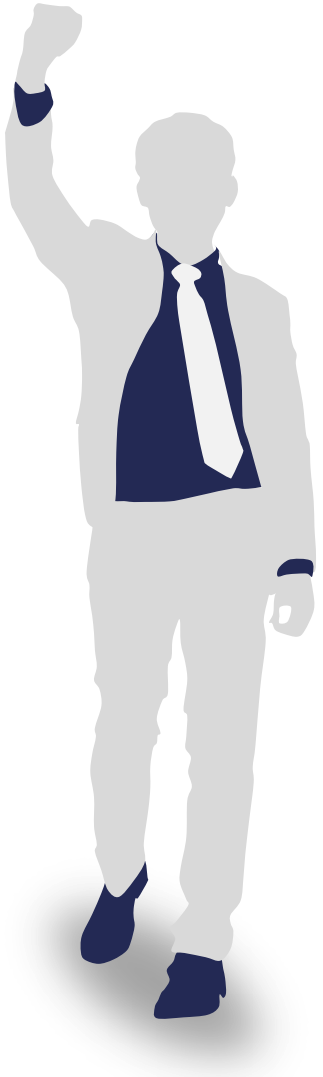
A JÖVŐ VÉDELME!

- Kiberbiztonsági tudatosság, belső fenyegetések növekedése
- Ellátási lánc elleni támadások
- Kiemelt fókusz a kritikus infrastruktúrákra
- IT/OT egységes menedzsment
- Nemzetközi állam által támogatott kiberháborúskodás
- SOC-ok (Security Operations Center) előtérben, nagyobb kereslet
- Külső Kiberfenyegetési Intelligencia
- Kiberbiztonság mint szolgáltatás
- Felhőszolgáltatások és MSP-k (kezelt szolgáltatók) elleni támadások
- Data Governance
- Személyazonosság lopás/ megszemélyesítés
- Költséghatékony biztonsági platformok konszolidációja
- Ransomware és phishing támadások
- Kiberbiztonsági szabályozások végrehajtása
- Automatizálásra és láthatóságra való összpontosítás
- AI/ML/UEBA alkalmazása

Mik a céljaink a technológiáinkkal?



Kiberbiztonsági kockázatok csökkentése
Szolgáltatások folytonosságának garantálása
Értékesítési lánc szereplői közötti bizalomnövelés



INNOVÁCIÓ

VERSENYELŐNY

SZOROS KOOPERÁCIÓ

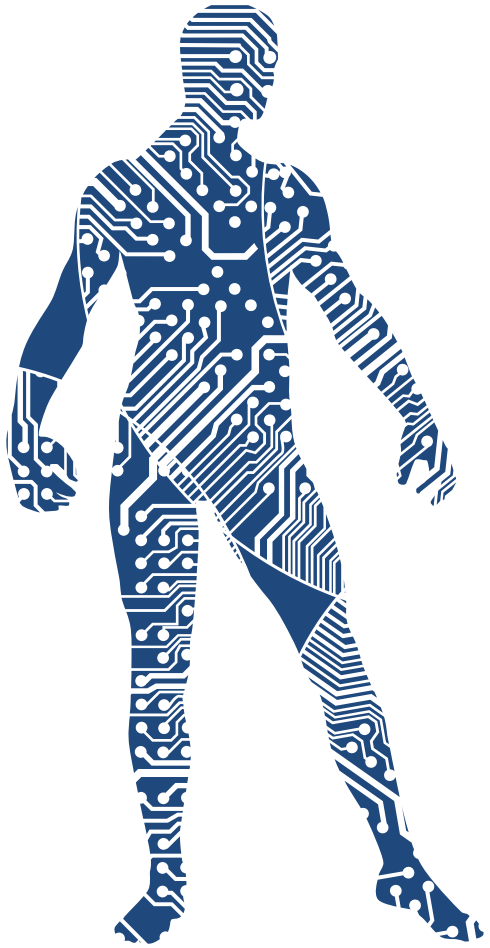
ERŐFORRÁS OPTIMALIZÁLÁS

REZILIENCIA

PRIANTO

Megoldásaink, amelyek segítenek…

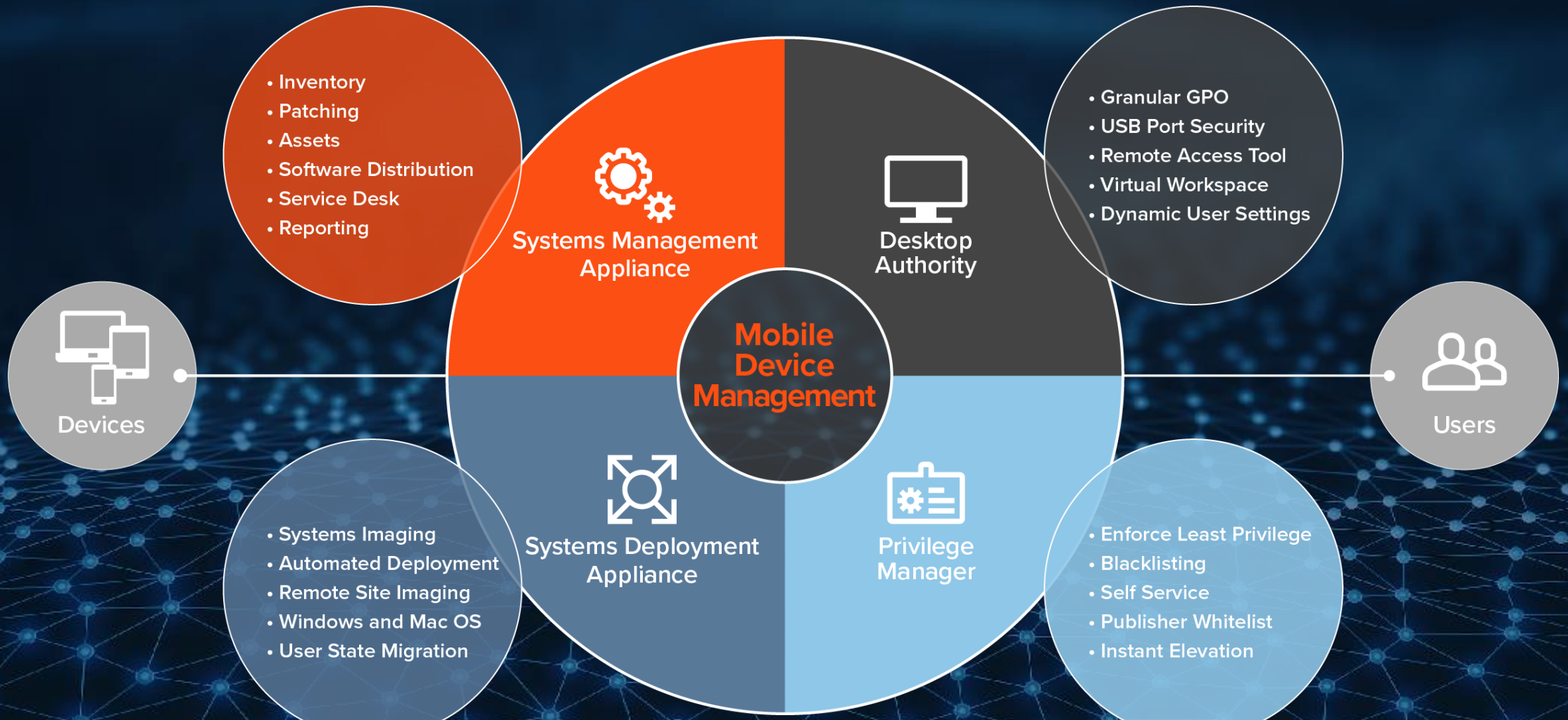
- Biztonságos hálózati infrastruktúra kialakítása, valós idejű monitorozása és védelem
- SIEM+SOAR+BCS+EDR bevezetése, incidenskezelés
- Sérülékenység- vizsgálat és menedzsment, behatolás tesztelés
- Cyber Threat Intelligence és Threat Hunting megoldások és szolgáltatások



- MSP/SOC megoldások és szolgáltatások
- IT & OT biztonsági és menedzsment megoldások
- Jogosultság, felhasználókezelés és hozzáférés menedzsment megoldások
- Adatmentés, Disaster Recovery és üzletfolytonosságot biztosító megoldások

PRIANTO

Quest KACE - Egységes végpontmenedzsment



Quest KACE – Egységes Végpontmenedzsment (UEM)

Inventory & IT asset management	Részletes nyilvántartást vezet az összes IT eszközről, beleértve a hardver- és szoftverleltárt, valamint a licencek kezelését.
Patch management & security	KACE rendszeresen ellenőrzi az eszközöket a hiányzó biztonsági javítások és frissítések szempontjából, és automatikusan telepíti ezeket a védelem érdekében. Védelmi mechanizmusokat tartalmaz.
Szoftverdisztribúció	Automatikusan telepíti és frissíti a szoftvereket az összes hálózati eszközön, biztosítva a kompatibilitást és a frissítések naprakészségét.
Service desk	Teljes körű service desk funkciókat kínál, beleértve a jegykezelést, a probléma nyomon követését és az ügyféltámogatást.

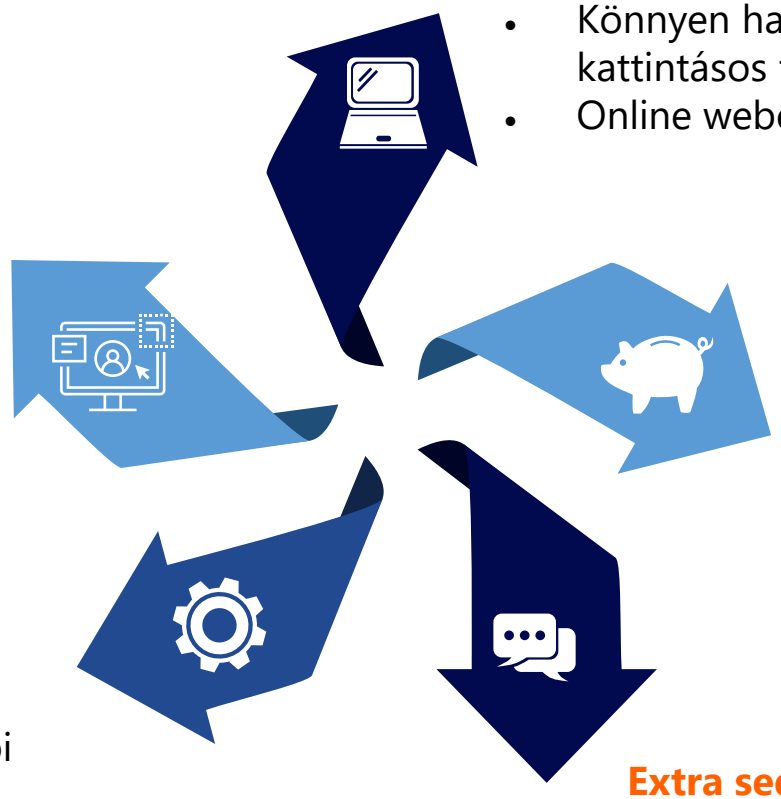
Quest KACE – Egységes Végpontmenedzsment (UEM)

Teljeskörű megoldás

- A telepítéstől kezdve a folyamatos karbantartáson, felügyeleten és támogatáson át a rendszer nyugdíjazásáig.
- Támogatja a Windows, Mac, Chromebook, Linux és UNIX rendszereket.
- Számítógépekhez, szerverekhez, mobileszközökhöz és csatlakoztatott nem számítástechnikai/IoT eszközökhöz.

Egyszerű használat

- Kiterjedt, integrált, all-in-one megoldás.
- Könnyen használható felhasználói felület, egyetlen kattintásos frissítések.
- Online webes képzés.



Gyors megtérülés (ROI)

- Virtuális készülékként vagy felügyelt szolgáltatásként érhető el.
- A legfontosabb funkciók könnyen érthetőek, és szinte azonnal használatba vehetők.
- Hetek alatt teljes mértékben működőképes, nem hónapok vagy évek alatt.

Támogatás

- Az ingyenes webes képzés, a szakértői támogató személyzet és a támogató videósorozatok segítségével a felhasználók soha sem maradnak egyedül.

Extra segítség:

- Az ITNinja, a Quest Közösség, a Backyard BootKamps, a UserKon támogató hálózatokat biztosít a KACE felhasználók számára.

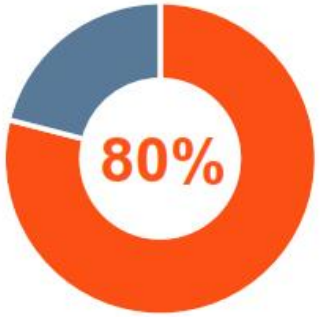
Referenciák

KACE is a Global Leader in UEM

15 For 15 years KACE has been helping businesses manage their IT infrastructure

50k Currently supporting more than 50,000 customers worldwide

8m Supporting more than 8 million endpoints and growing

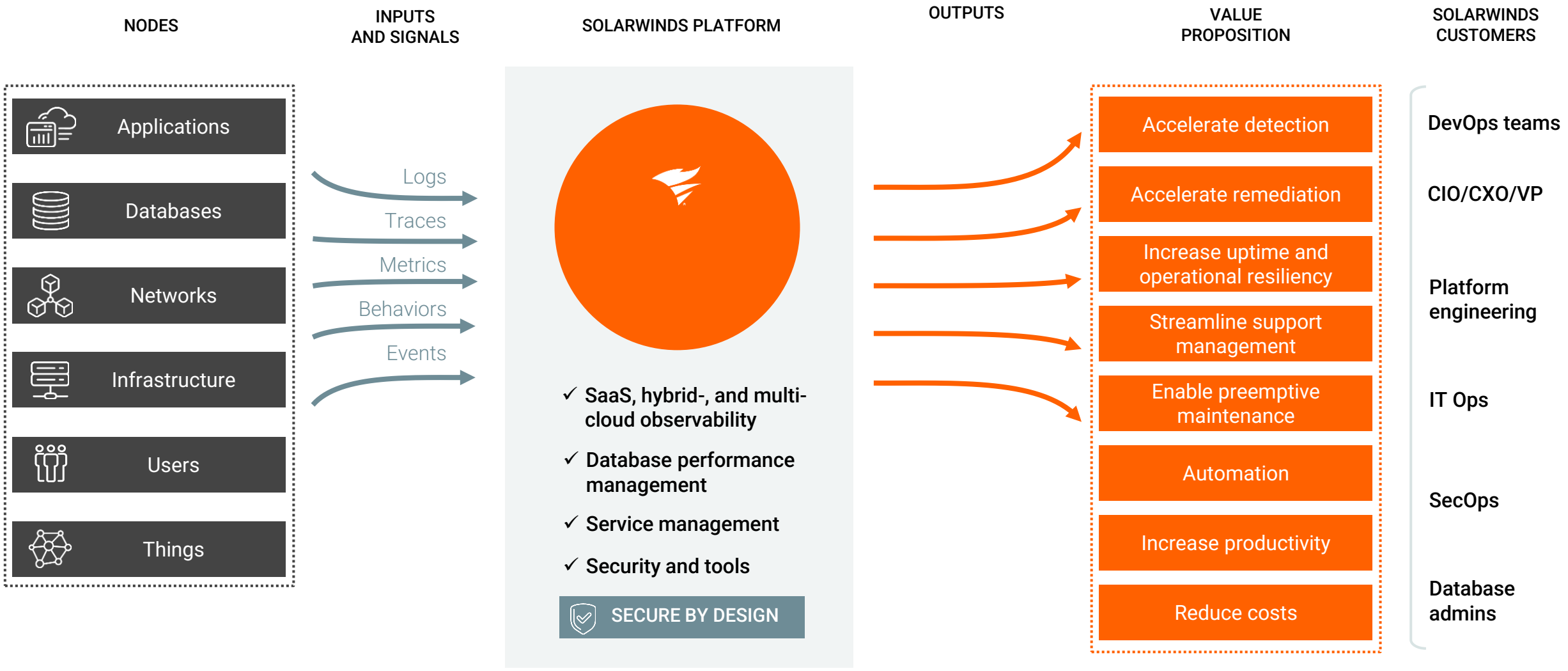


of **Top100** Most Valuable Brands

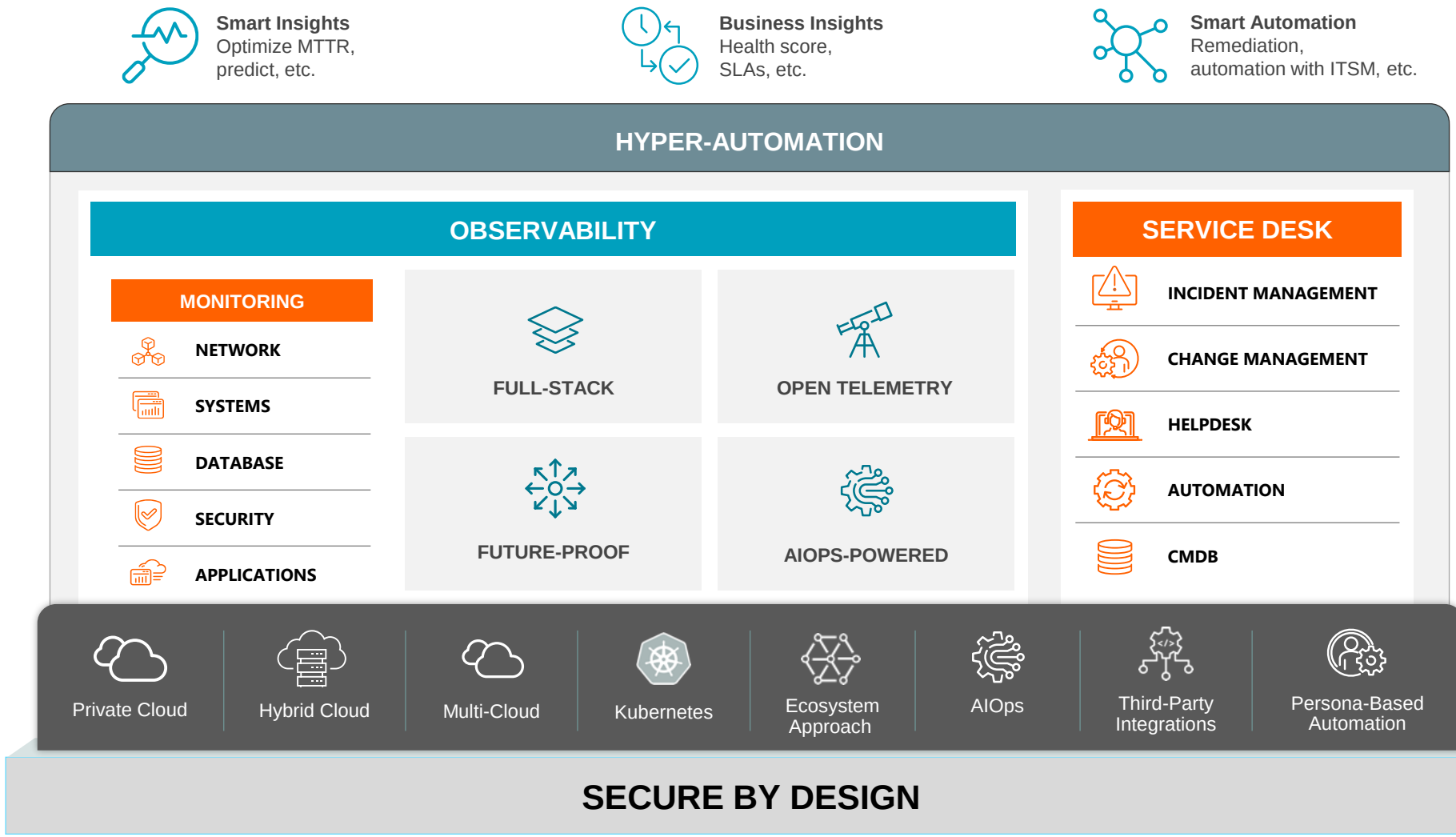
of Tech **Top20**

VISA BARCLAYS citi
PayPal Chevron
MERCK Ford UBER
Bank of America EY TOYOTA
American Airlines bp HYUNDAI
AIRFRANCE SUZUKI
LOUIS VUITTON
MARS Allianz
Microsoft intel
ebay YAHOO!
SIEMENS SONY PICTURES
AT&T

Solarwinds – Több mint rendszerfelügyelet…ez **Observability**



Solarwinds Observability Platform



Teljes infrastruktúra megfigyelhetőség és kezelés

SolarWinds Hybrid Cloud Observability: Átfogó megoldás a hibrid felhő monitorozásához és fejlesztéséhez. Automatizálás, elemzés, megfigyelés, kezelés és problémamegoldás, beleértve a felhőszolgáltatások nyomon követését is.

Eszközszaporulat megszüntetése

Alakítsa át a szétszórt adatokat fókuszált, gyakorlatias betekintéssé összetett hibrid környezetekben, és csökkentse a hibrid IT láthatósághoz szükséges eszközök számát.

Riasztási fáradtság csökkentése

Csökkentse a riasztások zaját, és gyorsabban azonosítsa a problémák forrását a gépi tanulással továbbfejlesztett felhőalapú AIOps-szolgáltatásunk által biztosított anomália alapú riasztásokkal.

Megfigyelhetőség a hibrid IT-n keresztül

Szerezzen láthatóságot a helyszíni és hibrid környezetekben, hogy megelőzően észlelhesse és kezelhesse a problémákat a rugalmas, ügynökalapú, ügynök nélküli és API-ból származó metrikákkal.

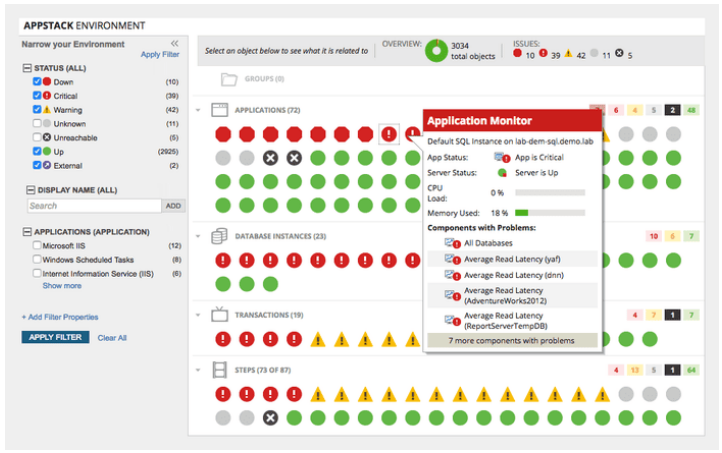
Felkészülés a növekedésre rugalmas licenceléssel

Egyszerűsített licencelés, vállalati szintű beépített lekérdezőmotorokkal, és a csomópontok egyetlen licenccel történő elosztásának rugalmassága.

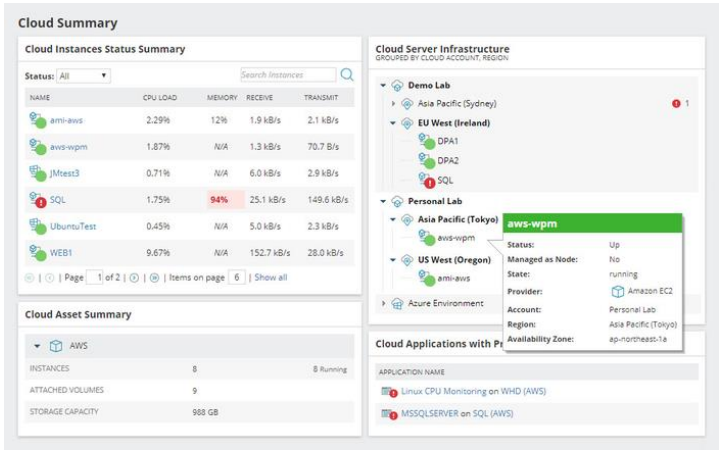
PRIANTO

Sokszínű átfogó nézet, egy kezelői felület

Mélyreható láthatóság a hálózatok, szerverek, alkalmazások és adatbázisok között.

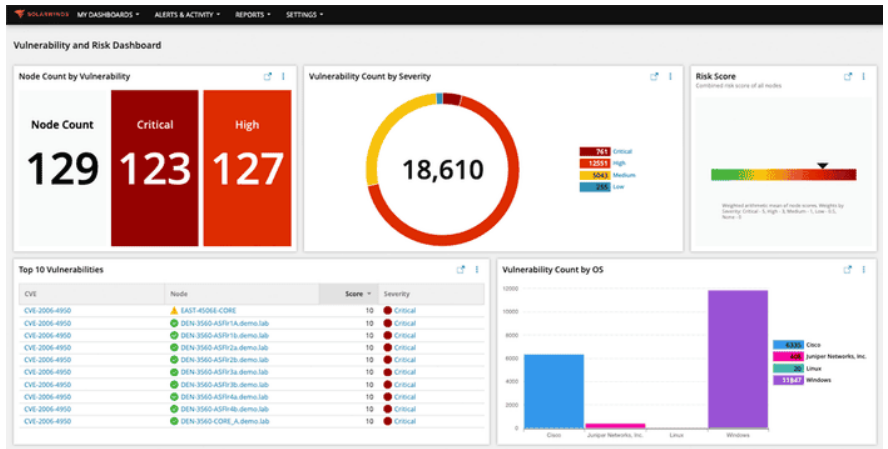


Páratlan hálózati láthatóság és irányítás



Haladjon előre magabiztosan: intelligens, skálázható IT-megoldások

A biztonság mindenki felelőssége



Fejlett szerver- és alkalmazásfigyelés, könnyedén

Pár kiemelt fókuszterület, amit a Solarwinds kiválóan lefed

- **Teljesítmény- és Rendelkezésre állás-figyelés:** A SolarWinds lehetővé teszi a hálózatok, szerverek, és alkalmazások teljesítményének és rendelkezésre állásának folyamatos monitorozását, biztosítva, hogy a kritikus rendszerek optimálisan működjenek és azonnali értesítést küldjenek bármilyen probléma esetén.

- **Hálózati Biztonság és Anomália-észlelés:** A platform segít azonosítani a hálózati biztonsági fenyegetéseket és anomáliákat, mint például a nem szokásos forgalmi mintákat vagy a potenciális behatolási kísérleteket, lehetővé téve a gyors reagálást és a biztonsági incidensek kezelését.

- **Felhőalapú Erőforrások Kezelése:** A SolarWinds Hybrid Cloud Observability biztosítja a felhőalapú infrastruktúra és szolgáltatások, beleértve az alkalmazások felhőben való migrációját és kezelését, átfogó láthatóságot nyújtva a felhők közötti és on-premise erőforrások felett.

- **Konfigurációkezelés és Compliance:** Automatizált konfigurációs naplózás és auditálás funkciókat kínál, segítve a szervezeteket a szabályozási megfelelésben és a konfigurációs változások nyomon követésében, amelyek kritikusak compliance előírások és sztenderdek betartásához.

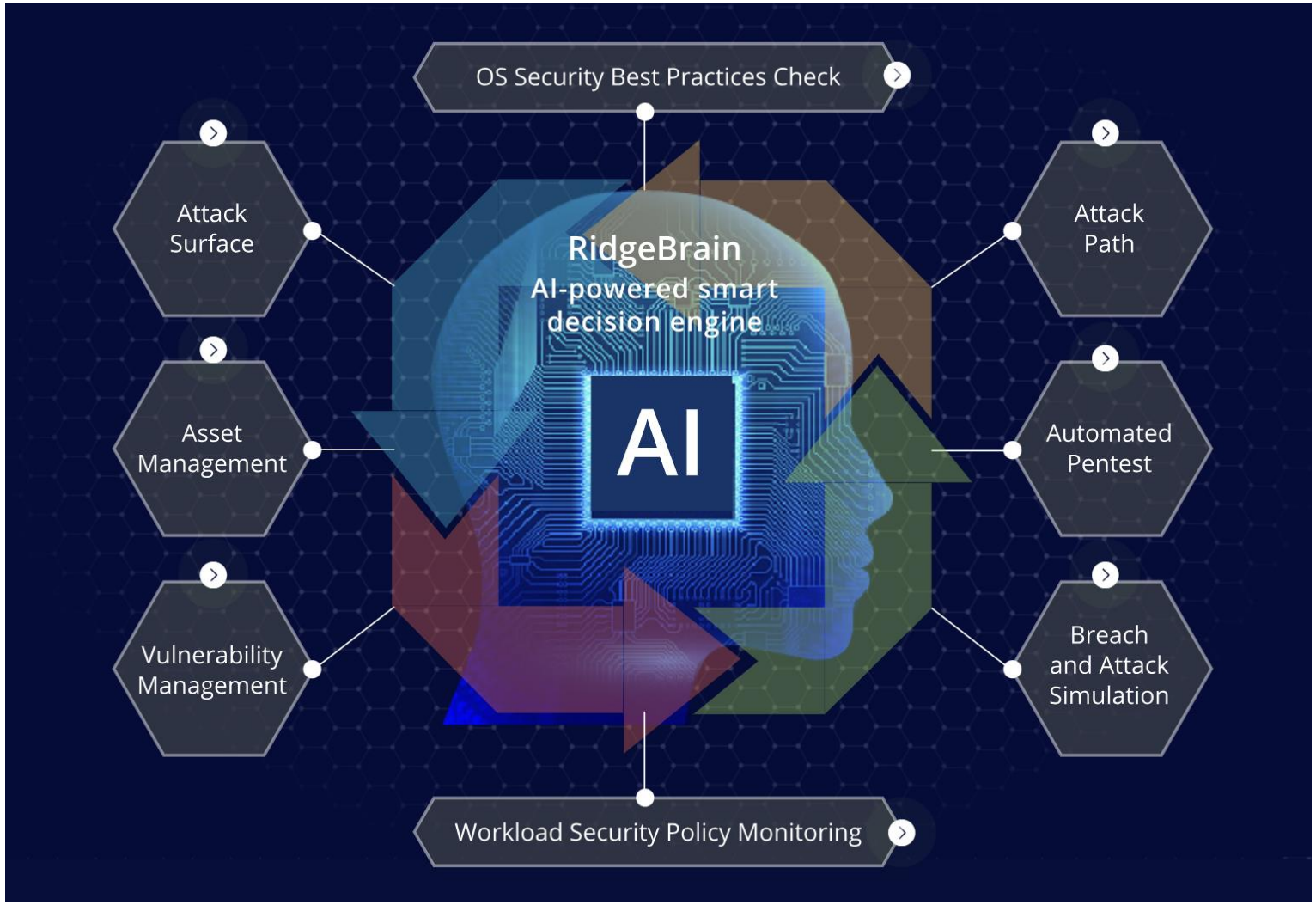
- **Katasztrófa-elhárítás és Üzletfolytonosság:** A platform segítségével a szervezetek fejleszthetik és tesztelhetik a katasztrófa-elhárítási és üzletfolytonossági terveiket, biztosítva, hogy a kritikus rendszerek gyorsan helyreállíthatók legyenek bármilyen incidens után.

- **Hálózati Topológia és Traffik Elemzés:** A SolarWinds átfogó eszközöket nyújt a hálózati topológia vizualizálására és a hálózati traffik elemzésére, segítve a döntéshozókat a hálózati tervezés és optimalizálás terén, valamint a kiberbiztonsági fenyegetések kezelésében.

- **Integráció és Automatizálás:** A SolarWinds platform integrálható más biztonsági és hálózati eszközökkel, automatizálva a rutin feladatokat és reagálást, így növelve a műveletek hatékonyságát és csökkentve az emberi hiba lehetőségét.

Referenciák minden iparágból

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.

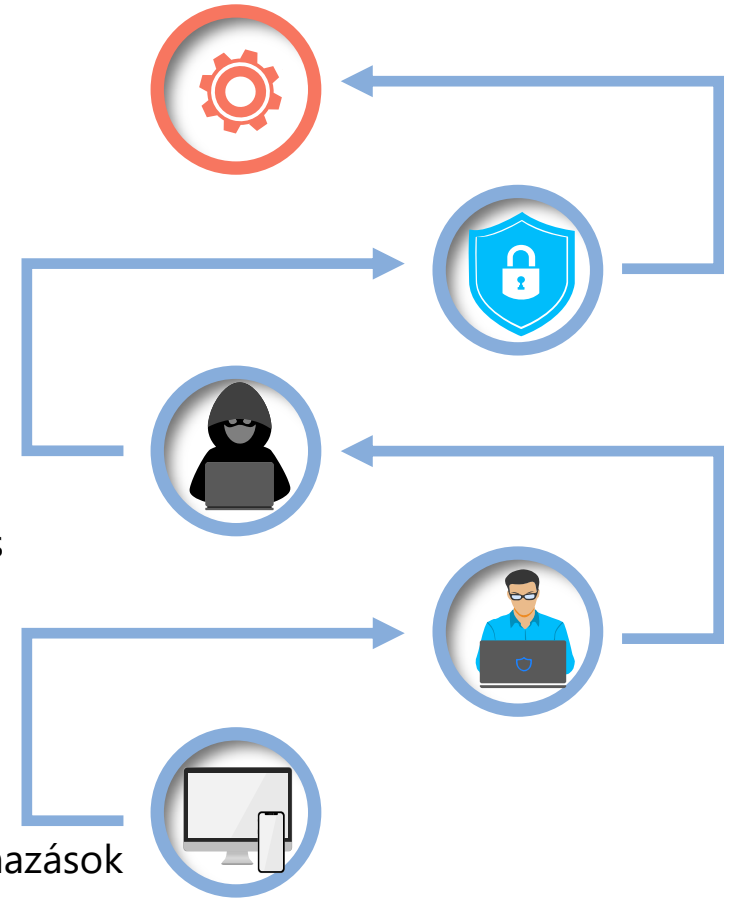
🧠 **AI szabadalom**
A megbízható AI szabadalommal támogatva a Ridgebot biztosítja a precíz és intelligens fenyegetés-felismerést és -elhárítást.

⚙️ **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

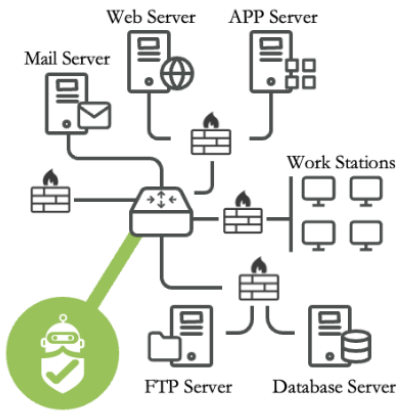
- Támadási Lánc Vizualizáció és Kihasználási Bizonyítékok
- Egészségügyi Pontszám, Kockázatok és Sebezhetőségek Priorizálása
- Kockázati és Sebezhetőségi Részletek és Kezelési Javaslatok
- Harmadik Fél VA Szkenner Integráció
- OWASP Top-10 Jelentéskészítés
- VM Historikus/Trend Elemzés

Eszközkezelés

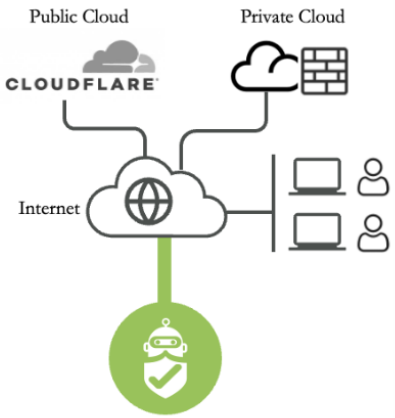
- Hosztok és szolgáltatások/alkalmazások
- Weboldalak és domainek
- Botlet telepítés és állapot
- Támadási felületek azonosítása

PRIANTO

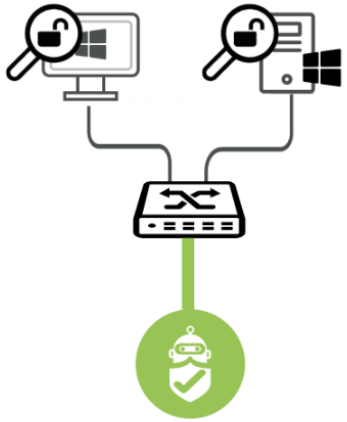
Internal Attack



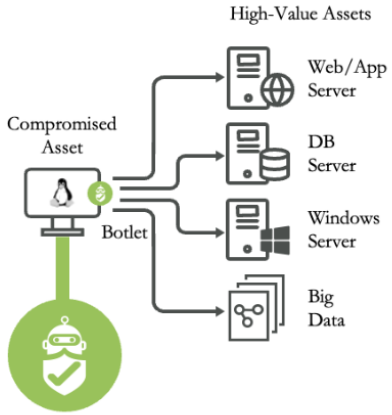
External Attack



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.

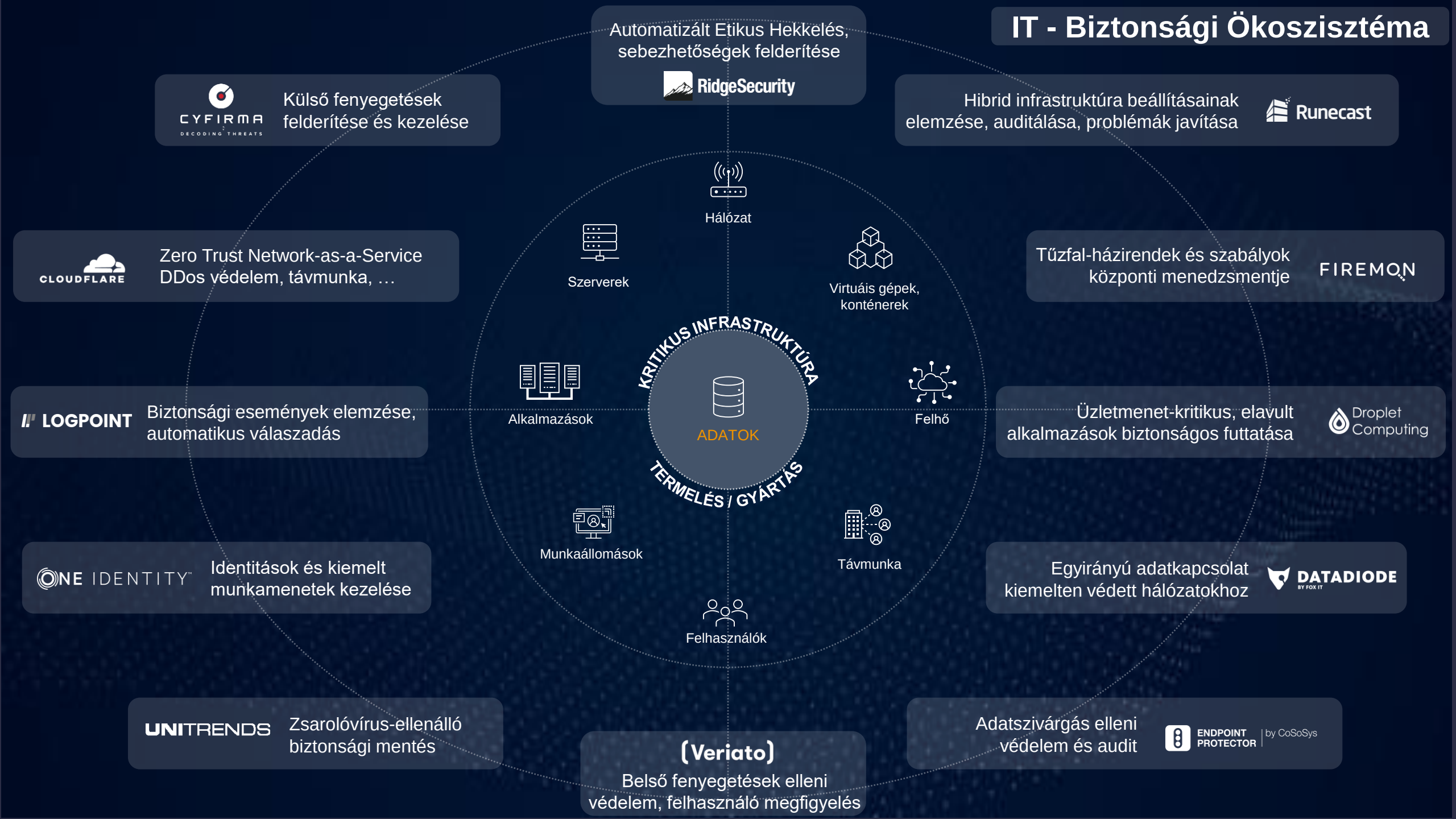
Enhancing Supply Chain Operational Resilience in the Logistics Sector with CTEM

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

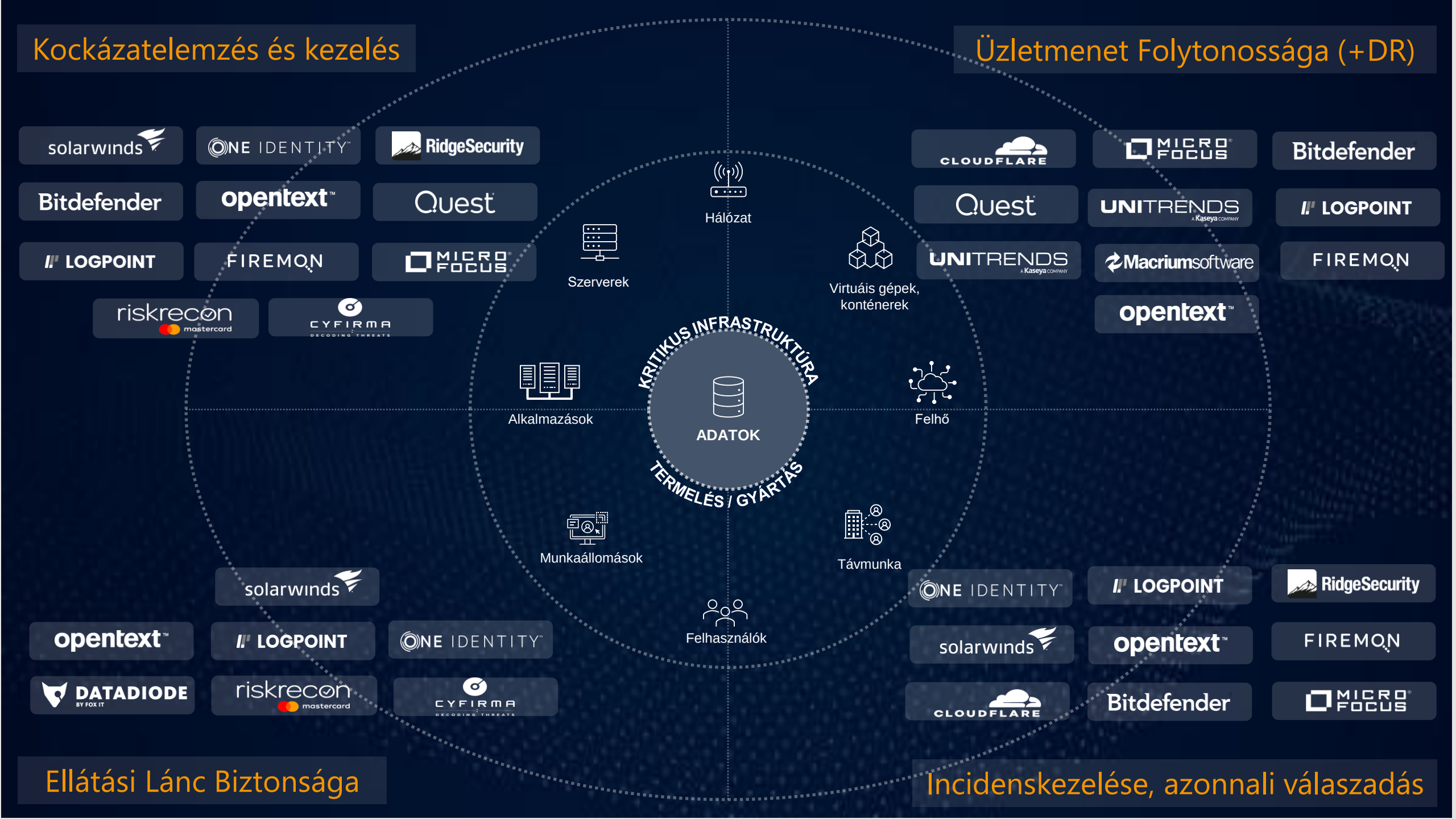
ONE IDENTITY
Identitások és kiemelt munkamenetek kezelése

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

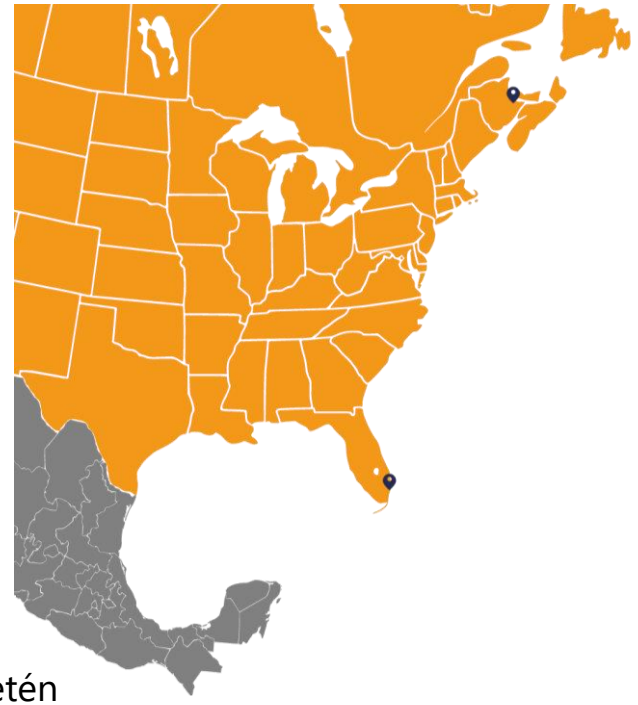
Köszönöm a figyelmet!

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

Tanácsadás

Szoftver disztribúció

Szoftver-beszerzés

Értékesítés

MSP szolgáltatás

Üzletfejlesztés

Ipar 4.0

Kibervédelem

Pre-Sales

Műszaki támogatás

Digitalizáció

Implementáció

Marketing támogatás

Kompetencia központ

Képzések

Teszt-rendszerek, POC

PRIANTO

PRIANTO „**NEURON-HÁLÓZATA**"

Végfelhasználók

MSP/SOC szolgáltatók

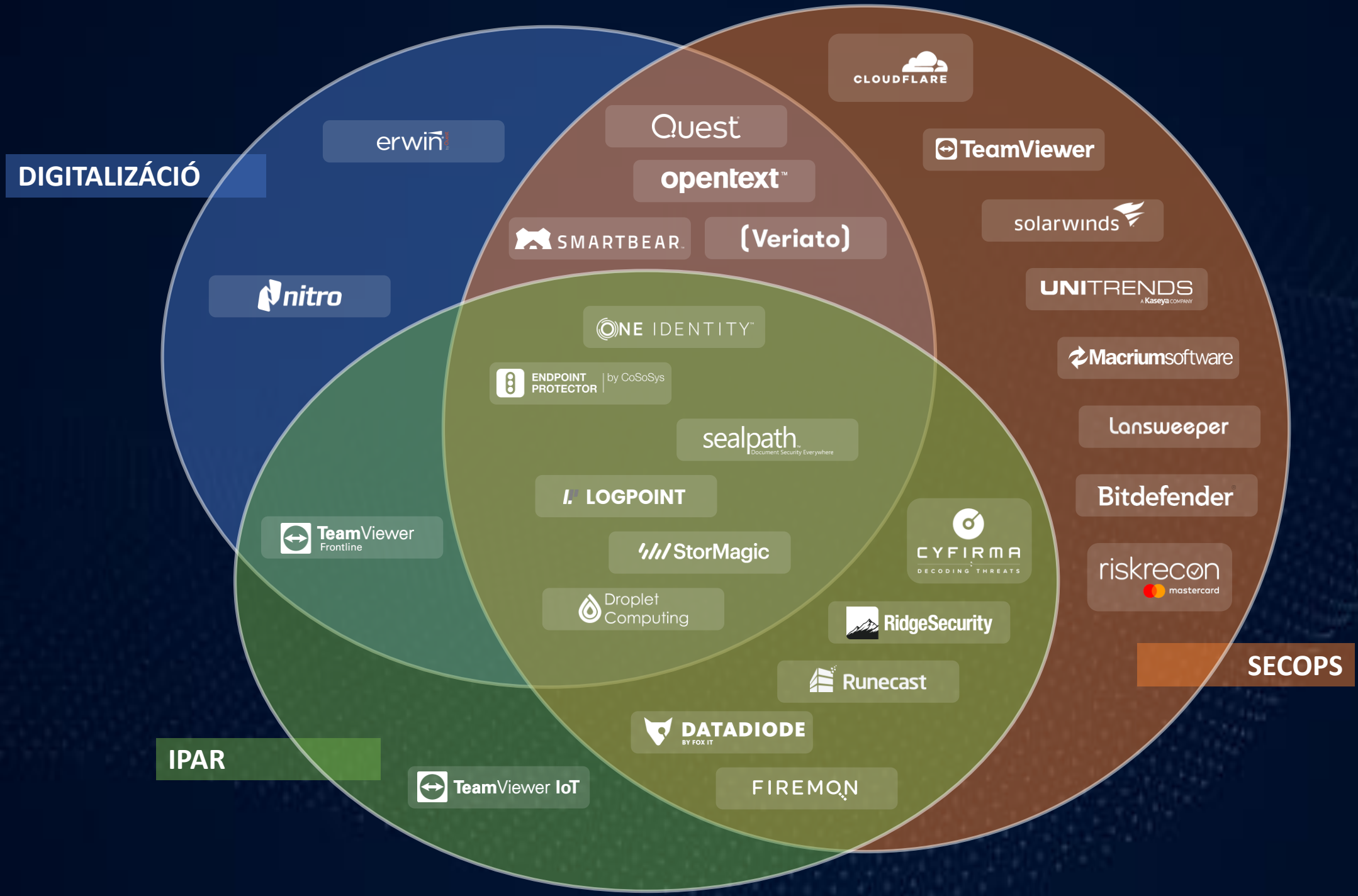
IT szállítók

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