Digitális kockázatok 2026-ban: mire kell felkészülnie egy KKV vezetőjének?

A KKV-kat érintő legfontosabb digitális fenyegetések, a gyártó és szolgáltató vállalkozások kiberbiztonsági kihívásai, valamint a védekezés gyakorlati lehetőségei és a Palo Alto Networks megoldásai.

Rácz László - Palo Alto Networks BDM, ALEF
Horváth Krisztián - Palo Alto Networks Senior Systems Engineer, ALEF

ALEF

Mi történne, ha holnap reggel nem működne az ERP rendszer?

Nem lehet számlázni

Az üzletmenet azonnal sérül.

Nem láthatók a megrendelések

Az üzletmenet azonnal sérül.

Nem érhetők el a vállalati adatok

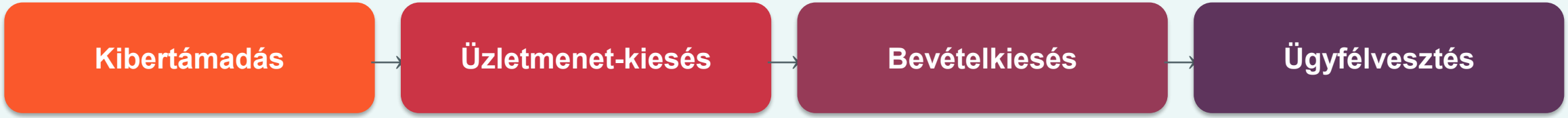
Az üzletmenet azonnal sérül.

Nem tudjuk, mikor áll helyre

Az üzletmenet azonnal sérül.

Mennyi ideig tudna így működni a vállalkozás?

A kiberbiztonság már üzleti kérdés



Nem IT probléma. Üzleti kockázat.

Milyen fenyegetések érik ma a KKV-kat?

AI és adatvesztés

Érzékeny adatok kerülhetnek külső AI-szolgáltatásokba.

Adathalászat és csalások

AI-generált, személyre szabott és hitelesnek tűnő üzenetek.

Zsarolóvírus

Leállás, titkosítás, helyreállítási költség és reputációs kár.

Az AI új lehetőség és új kockázat is

Mit adunk az AI-nak?

Szerződések
Árajánlatok
Műszaki dokumentáció
Ügyféladatok

Hol használják?

ChatGPT
Microsoft Copilot
Gemini
Claude és több száz más alkalmazás

Tudjuk, milyen AI-eszközöket használnak a munkatársaink?

Adathalászat 2026-ban

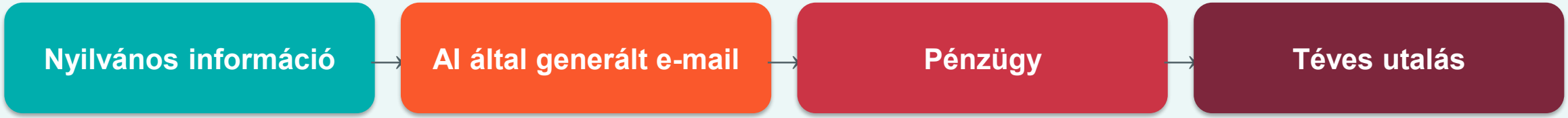
Régen

Hibás magyar nyelv
Általános megszólítás
Furcsa formázás
Könnyebben felismerhető

Ma

AI-generált, hibátlan szöveg
Személyre szabott tartalom
Valós üzleti kontextus
Hiteles hang és vizuális elemek

CEO fraud és hamis számlák



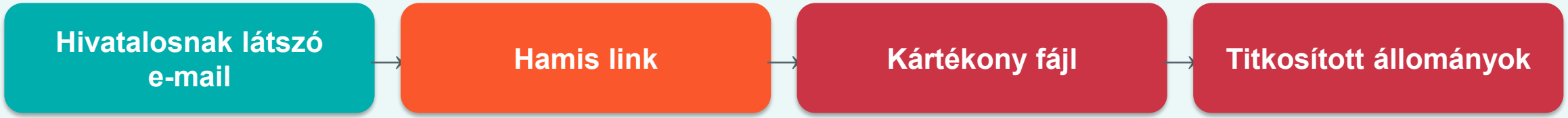
Nem a rendszert támadják. Az embert.

Mit jelent egy ransomware incidens?

- Termelésleállás
- Adatvesztés
- Bevételkiesés
- Reputációs kár

A helyreállítás nem csak technikai feladat: üzleti prioritásokról, kommunikációról és döntési jogkörökről is szól.

Magyar példa: az Ügyészség nevével visszaélő kampány (2026)



A hitelesség látszata és a sürgetés együtt veszi rá az áldozatot a kattintásra.

Miért veszélyeztetettek a KKV-k?

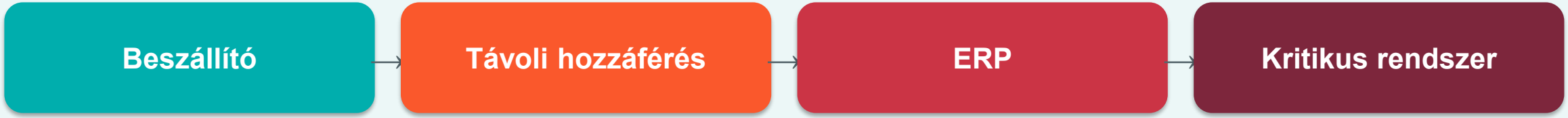
Gyártó vállalatok

PLC-k és gyártósorok
OT és régi protokollok
Külső karbantartók
Leállás = közvetlen termelési veszteség

Szolgáltató vállalatok

Ügyféladatok és CRM
Microsoft 365
Távoli munkavégzés
Sok SaaS és személyes eszköz

A legtöbb támadás nem ott indul, ahol a kár keletkezik



A kapcsolatok és jogosultságok lánca határozza meg a tényleges kockázatot.

Valós OT példa Magyarországról

SECTOR 16 incidens (2025)

Mi történt?

- Több magyar ipari és épületautomatizálási rendszerhez szereztek hozzáférést a kampányban.
- Egy magyar geotermikus termelőrendszer vezérlőfelületébe be is jutottak és az üzem működésére vonatkozó adatokat és beállításokat is elérték.
- Bizonyítékként képernyőképeket és üzeneteket publikáltak nyilvános csatornáikon.
- Nem hajtottak végre szabotázst vagy rendszer-módosítást, de igazolták a jogosulatlan hozzáférést.

Mi tette lehetővé a támadást?

- Internet felől elérhető OT/ICS rendszerek.
- Gyenge vagy könnyen kitalálható jelszavak.
- Elégtelen hálózati szegmentáció és hozzáférés-kezelés.

Mit jelent a védekezés a gyakorlatban?

Láthatóság

Hozzáférés-kezelés

AI kontroll

Incidenskezelés

Szegmentáció

Az öt pillér együtt csökkenti a meglepetések számát és gyorsítja a reagálást.

Tudjuk-e, mi történik a környezetünkben?

Eszközök

Milyen rendszereink és eszközeink vannak?

Adatok

Milyen adatokat tárolunk és hol?

Hozzáférések

Ki, honnan és mihez fér hozzá?

Ki venné észre először, ha ma kibertámadás történne?

IT

Pénzügy

Ügyfél

Támadó

Az első óra döntései meghatározzák a kár mértékét.

Ezekre a problémákra keresünk választ

Problémák

Láthatatlanság
Túl széles hozzáférés
AI-adatszivárgás
Lassú észlelés
Összekapcsolt IT és OT

Megoldási irányok

Egységes láthatóság
Zero Trust hozzáférés
AI- és adatkontroll
Automatizált reagálás
Szegmentáció

Hogyan segíthet a Palo Alto Networks?

Why Palo Alto Networks? Innovation Built for Your Security Journey

Data

Each day we analyze

1.4B+

new and unique objects across network, endpoint and cloud

R&D Investments

Invested nearly

$1.7B+

In research per year

Growth

Acquired

19

Companies in 10 years to protect customers

Efficacy

Leader in

22

Magic Quadrants and Waves

https://investors.paloaltonetworks.com/static-files/1c75f5af-1aaa-4957-911c-4541e5614700

 © 2024 Palo Alto Networks, Inc. All rights reserved.

Our Mission

The cybersecurity partner of choice, protecting our digital way of life.

15K Employees | 90K+ Customers Globally | ~$100B Market Cap

9 of 10
of the Fortune 10

8 of 10
Largest U.S. Banks

10 of 10
Largest Utilities in the World

6 of 10
Largest Oil & Gas in the World

8 of 10
Largest Manufacturing Companies in the World

7 of 10
Top U.S. Hospitals

© 2024 Palo Alto Networks, Inc. All rights reserved.

paloalto NETWORKS

What We Provide

Our next-gen platforms enable cyber transformation

Network Security
STRATA

Best-in-class security delivered across hardware, software and SASE

Cloud Security
PRISMA CLOUD

Comprehensive platform to secure everything that runs in the cloud

Security Operations
CORTEX

A new approach to SOC with fully integrated data, analytics and automation

Threat Intelligence and Advisory Services

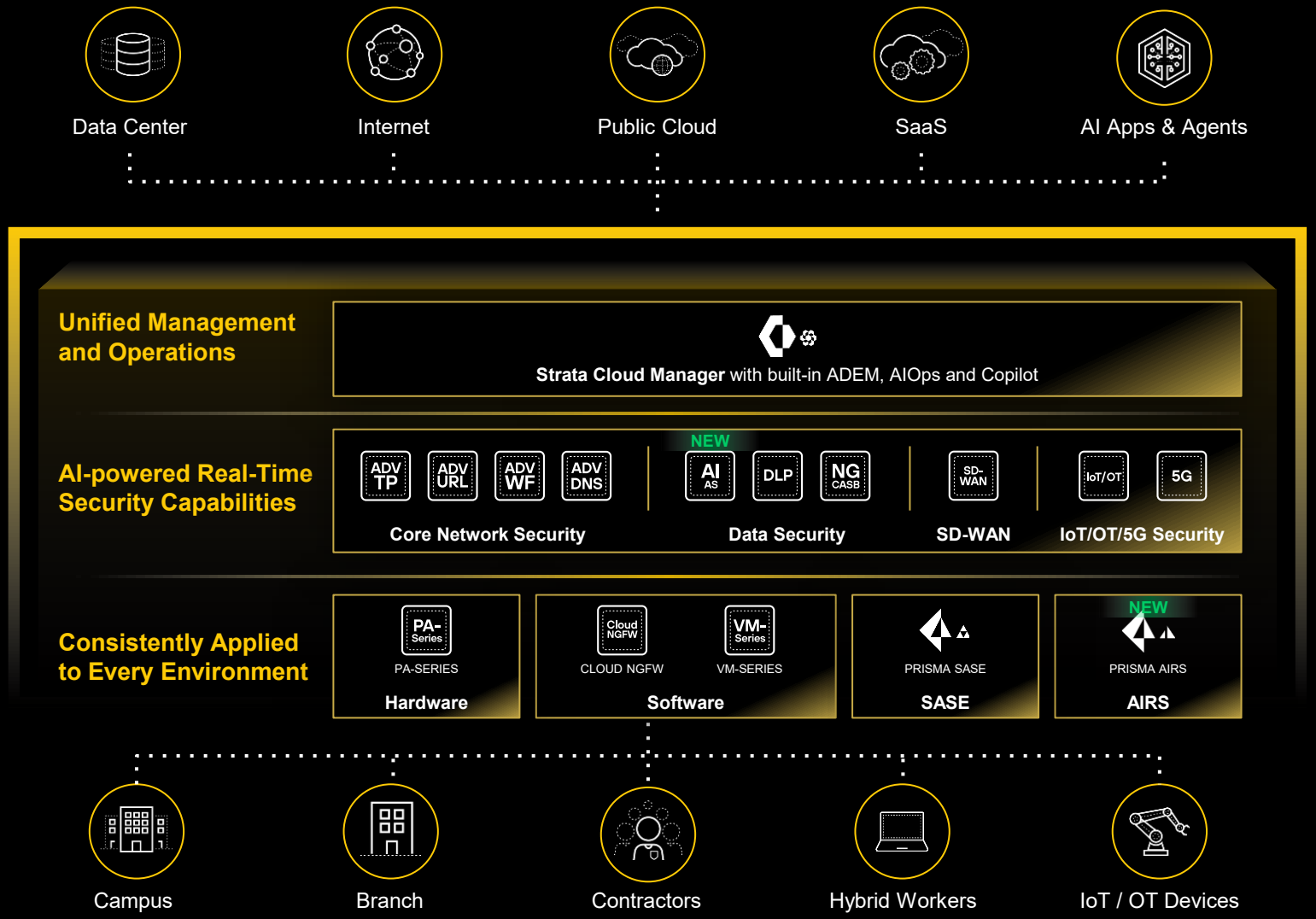
World-renowned threat intelligence, cyber risk management and advisory services

© 2024 Palo Alto Networks, Inc. All rights reserved.

paloalto NETWORKS

Strata Network Security Platform powered by Precision AI®

Simple & unified. Prevents threats in real time, everywhere.



Unified Management and Operations

Write policy once and enforce everywhere. Proactively strengthen security and prevent outages using Generative AI.

AI-powered Real-Time Security

Prevent threats in real time using ML and Deep Learning applied to rich data from **70,000+ customers**.

Consistently Applied to Every Environment

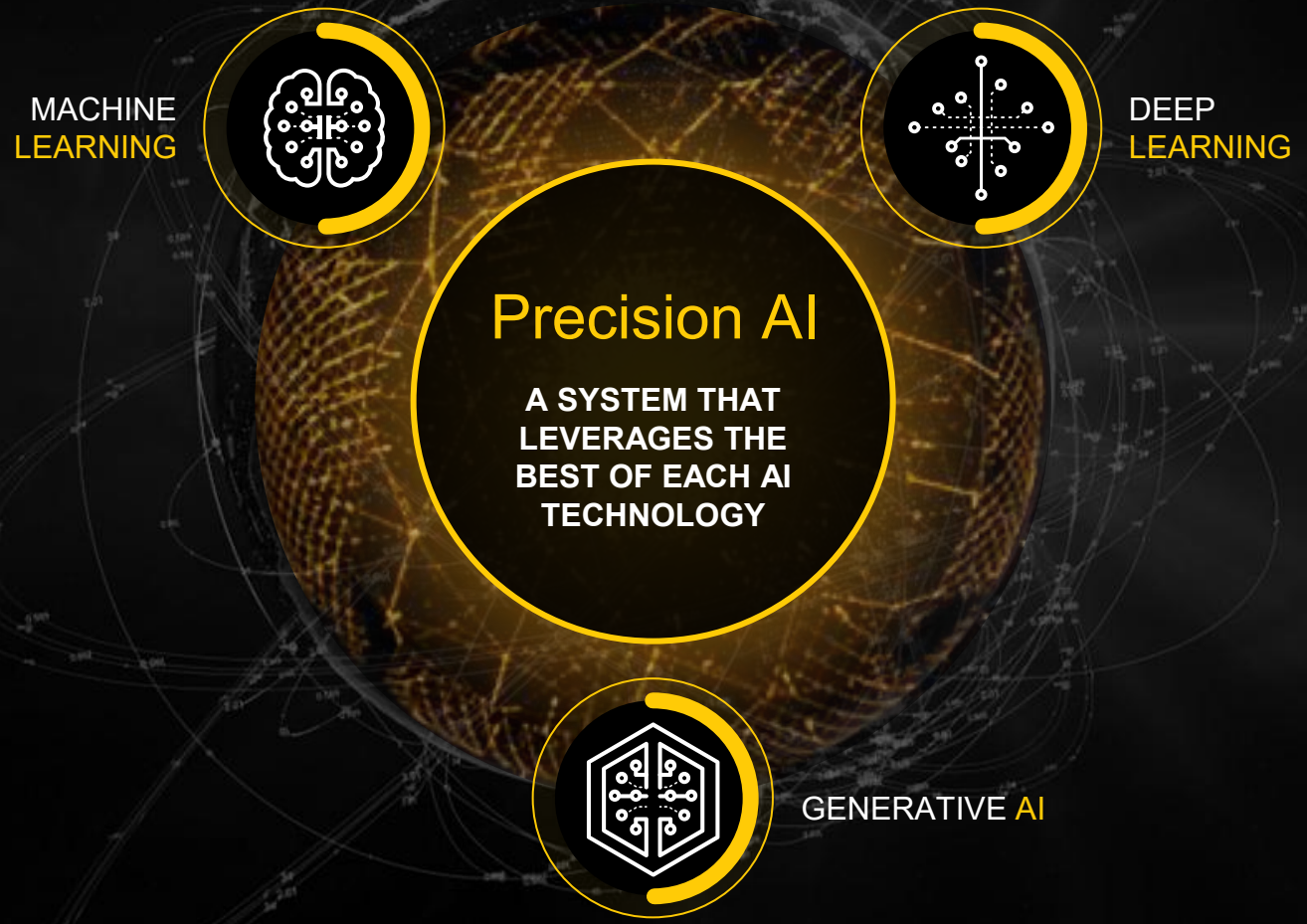
Secure AI and non-AI workloads against network and AI-specific threats. Deploy in clouds, containers and data centers.

© 2024 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto NETWORKS | STRATA

Strata Network Security Platform

Addresses the intensifying threat landscape with Precision AI®



© 2024 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

AI Access Security Safely Enables Employee Use of AI

Employees



Understand GenAI Usage & Risk

Prevent Sensitive Data Loss

Defend Against Malicious Responses

CONVERSATIONAL CHATS

CODE ASSISTANTS & GENERATORS

VIDEO & IMAGE GENERATORS

… +100s MORE

© 2024 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Device Security by Palo Alto Networks

Discover, identify, assess and proactively secure every device in your enterprise



Comprehensive Discovery

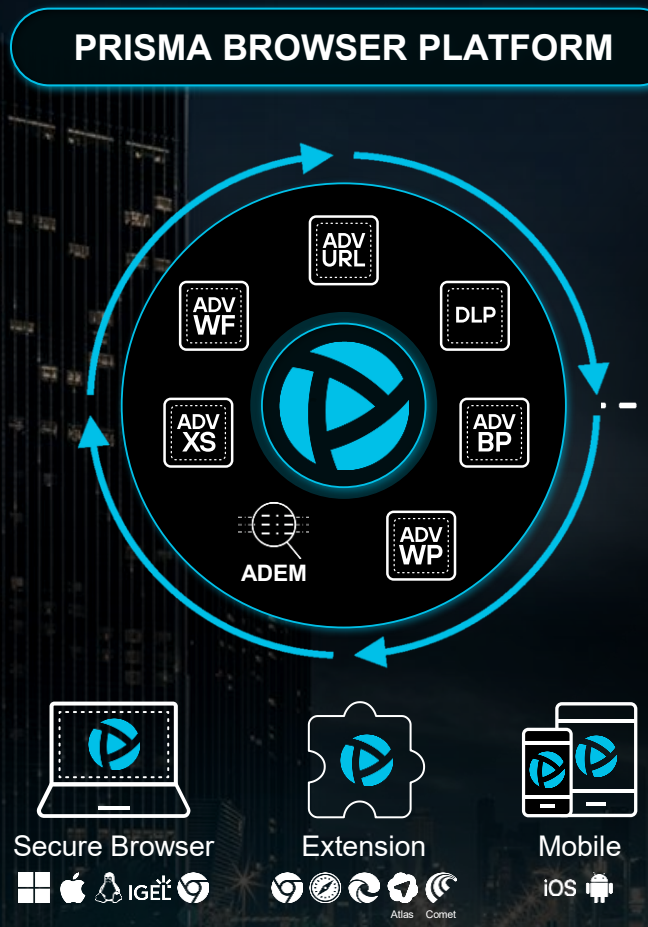
Insight Driven Proactive Security

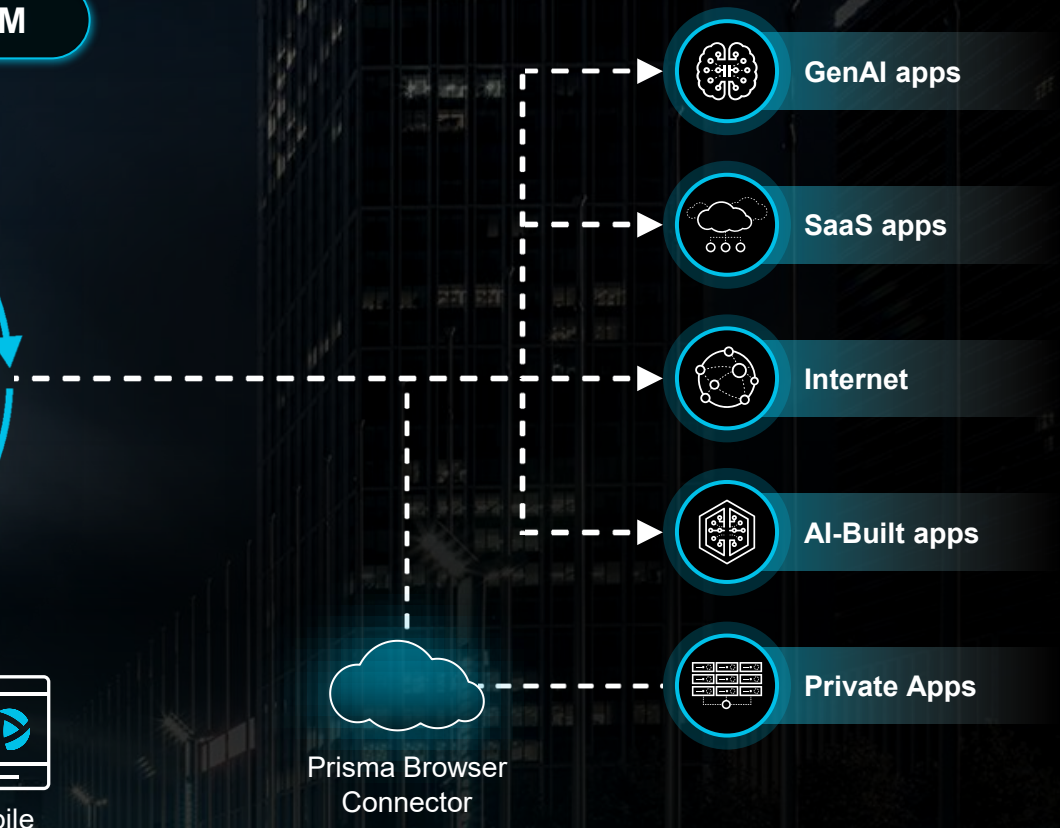
Fully integrated in one platform

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

The Most Secure Browser for the Modern Workspace

- Chromium-based, native UX
- Zero infrastructure changes
- No admin privileges required





© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto NETWORKS | PRISMA BROWSER

Három dolog, amit holnap meg lehet tenni

1

Készítsenek incidens-forgatókönyvet.

2

Mérjék fel az AI használatot.

3

Ellenőrizzék a kritikus rendszerek elkülönítését.

Nem az a kérdés, hogy ér-e kibertámadás egy vállalkozást.

Hanem az, hogy mennyire felkészülten éri.

Köszönöm a figyelmet.