Frontier AI a Unit 42

Od analýzy hrozieb

k plne autonómnej kybernetickej obrane

Jarná ITAPA – SECURITY DAY, Crown Plaza, Bratislava, 17.6.2026, Palo Alto Networks, Slovakia

Zsolt Géczi, CEH, Regional Sales Manager, Slovakia

Cybersecurity Partner of Choice

Palo Alto Networks is the **largest** pure-play cybersecurity provider, **securing** the world's most demanding enterprises.

Trusted by

70,000+

customers globally.

97/100

Fortune 100

FORTUNE

Recognized as an industry leader in **25** categories.

STRATA™

- Browser Security
- Container Security
- Internet of Medical Things (IoMT)
- NGFW
- SASE
- SD-WAN
- SSE
- OT Security
- Policy as Code
- Zero Trust Platforms
- ZTNA

CORTEX®

- Application Security
- Attack Surface Management
- Autonomous SOC
- CIEM
- Cloud Security Posture Management
- Cloud Workload Security
- CNAPP
- DevSecOps
- DSPM
- Endpoint Security
- SOAR
- SIEM
- XDR

UNIT 42®

- Incident Response
- MDR

paloalto® NETWORKS | PRISMA® AIRS

paloalto NETWORKS | UNIT 42

Global Incident Response Report 2026

Štyri hlavné trendy, ktoré budú v roku 2026 formovať oblasť kyber-hrozieb

1

AI sa stal prostriedkom na znásobenie sily útočníkov

2

Identita sa stala najspoľahlivejšou cestou k úspechu útočníka

3

Riziká v dodávateľskom reťazci sa už netýkajú len zraniteľného kódu, ale aj zneužitia dôveryhodných prepojení.

4

Štátom sponzorovaní útočníci prispôsobujú taktiky perzistencie modernému podnikovému prostrediam.

Útoky sú za posledný rok 4-krát rýchlejšie.

AI urýchlila celý proces

Útočníci scanujú nové CVE do 15 minút od ich oznámenia

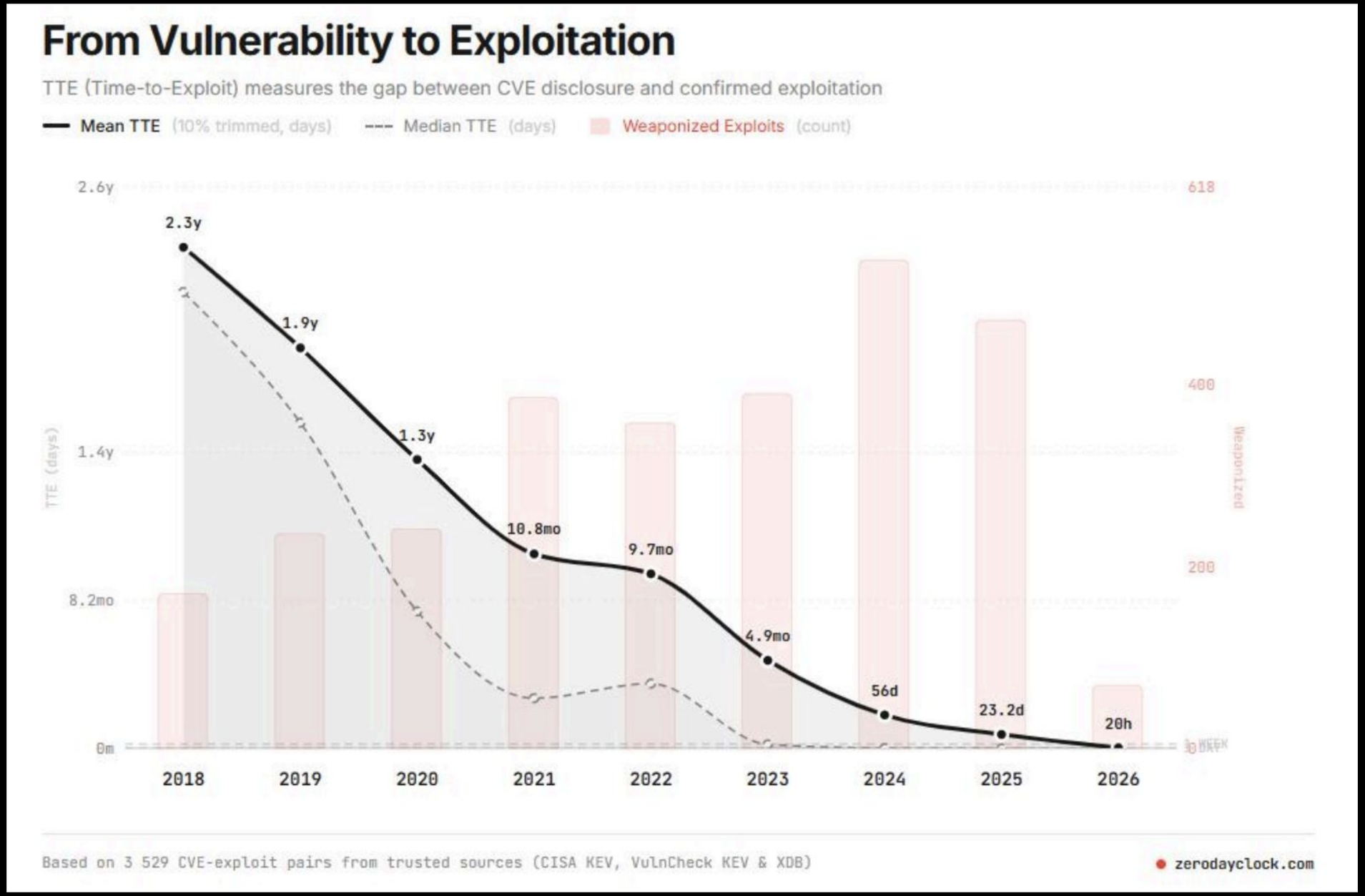
72 minút od preniknutia po exfiltráciu

AI umožňuje útočníkom skrátiť celý životný cyklus útoku

1. The Hacker News Q1 2025 CVE analysis 2. 2026 Unit 42 Global Incident Response Report, 25% of fastest cases

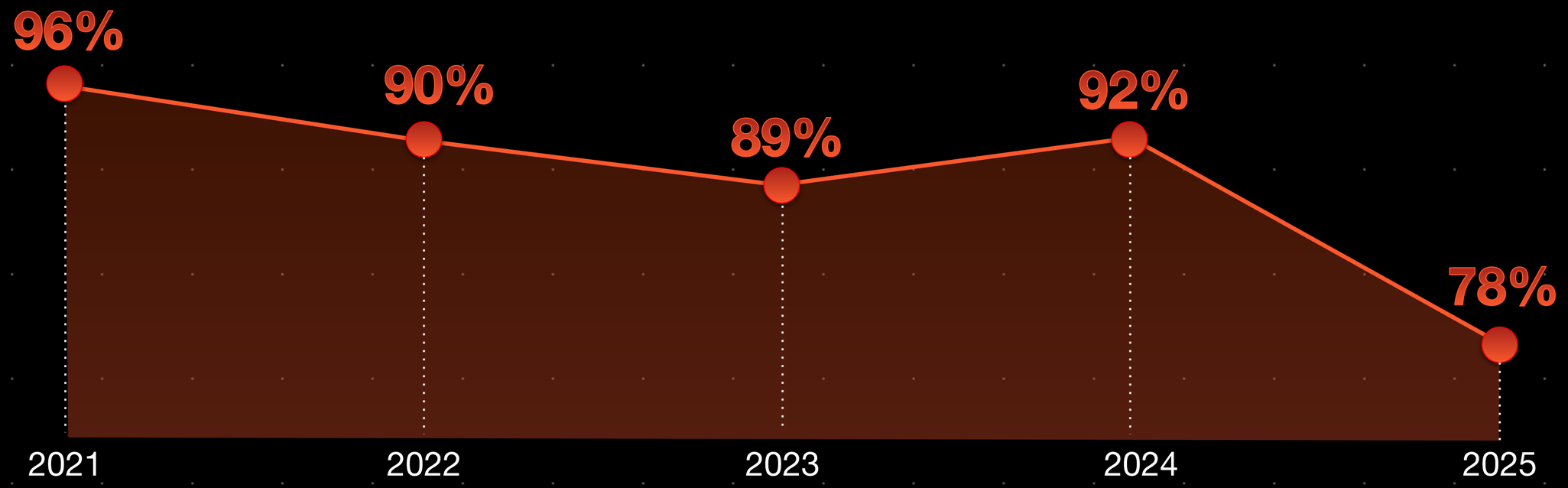
paloalto NETWORKS | UNIT 42

The “AI Vulnerability Storm”: Building a “Mythosready” Security Program



Útočníci začínajú upúšťať od šifrovania

Aby dosiahli okamžitý úspech pred odhalením



% Podiel prípadov vydierania, pri ktorých došlo k šifrovaniu

Source: 2026 Unit 42 Global Incident Response Report

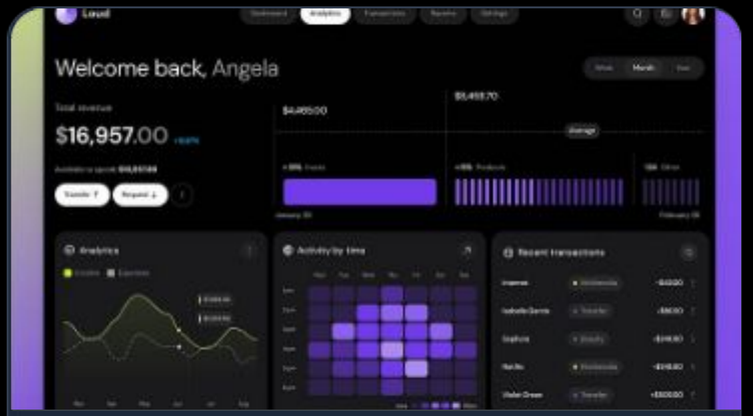
”The Sandbox Escape”

Jadro OpenBSD

Model autonómne odhalil **27 rokov starú** hlbokú systémovú zraniteľnosť v jadre OpenBSD, platforme slúžiacej pre kľúčovú armádnu infraštruktúru s povesťou nedobytnosti.

Knižnica FFmpeg

AI identifikovala **16 rokov utajenú chybu** vo videoknižnici, ktorú predchádzajúce automatizované skenery overovali viac ako päť miliónov krát bez povšimnutia.

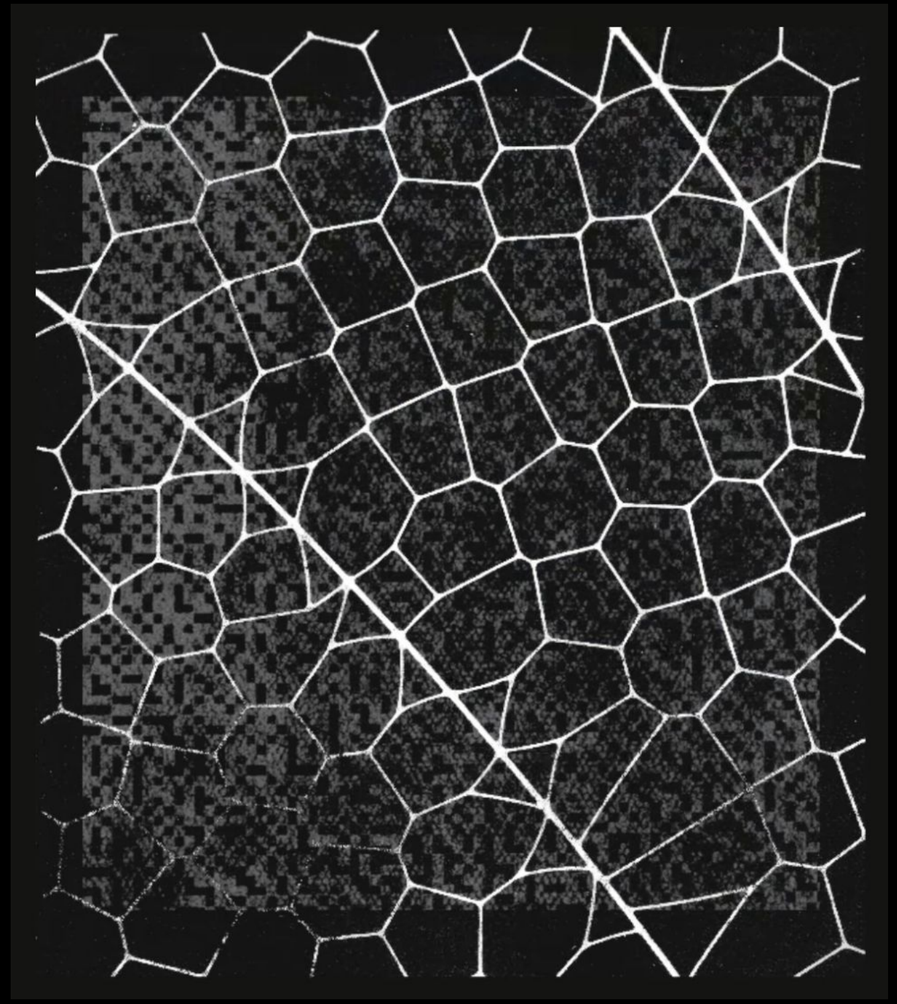


Test SWE-bench

Vo verifikovanom teste odhaľovania chýb model dosiahol ohromujúce skóre 93,9 %. Tieto poznatky sú plynulo integrované do ochranných signatúr Palo Alto Networks.

paloalto NETWORKS | UNIT 42

Project Glasswing



"The Breakout Moment”

CYBERSECURITY IN THE AGE OF AI

AI Agenti
Transformujú Biznis

1.3B

agents will be in production by 2028[1]

80%

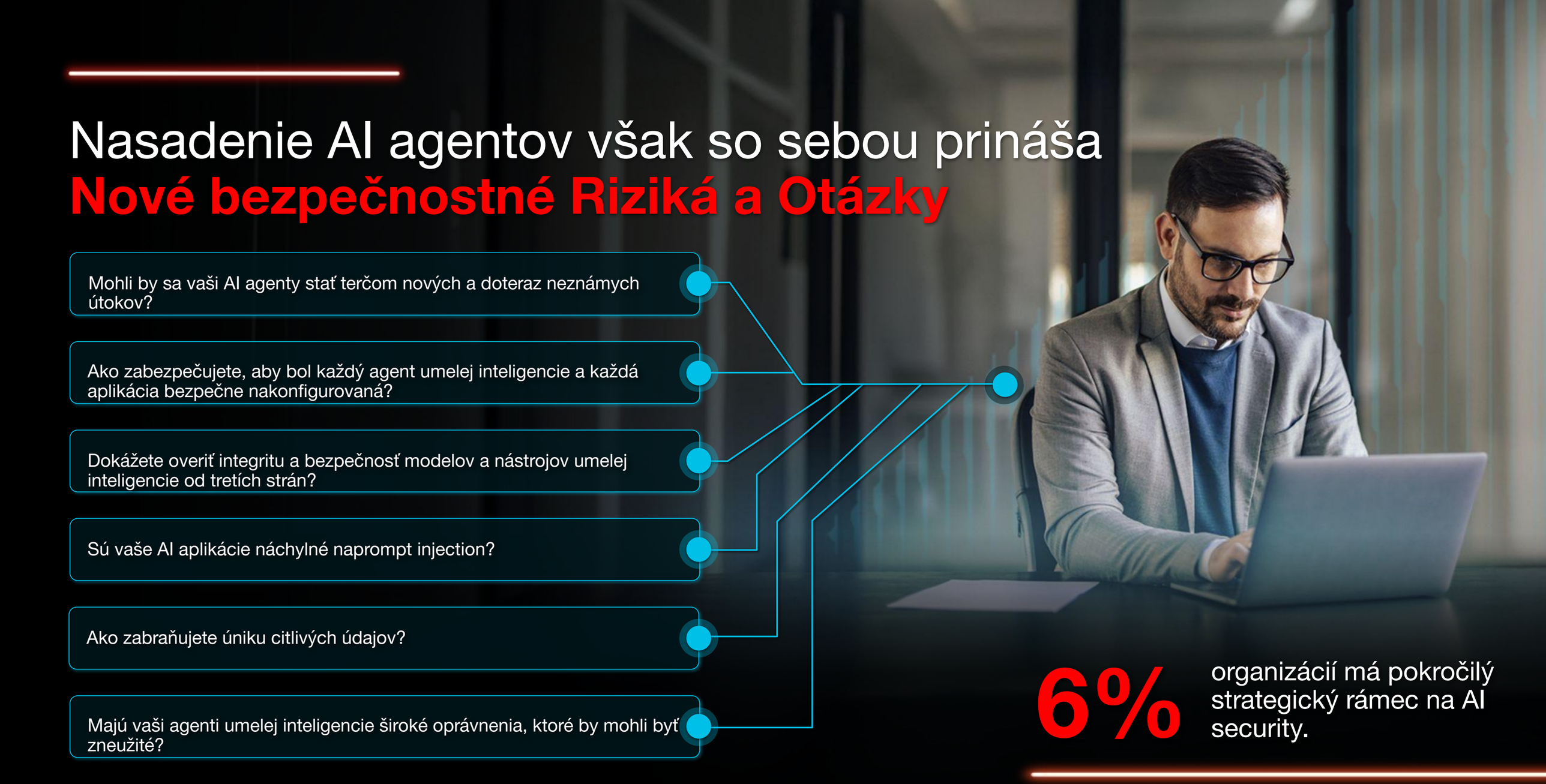
of customer support issues will be resolved by AI agents by 2028[2]

Sources: 1. IDC 2. Gartner

paloalto NETWORKS | PRISMA AIRS

Nasadenie AI agentov však so sebou prináša **Nové bezpečnostné Riziká a Otázky**

- Mohli by sa vaši AI agenty stať terčom nových a doteraz neznámych útokov?
- Ako zabezpečujete, aby bol každý agent umelej inteligencie a každá aplikácia bezpečne nakonfigurovaná?
- Dokážete overiť integritu a bezpečnosť modelov a nástrojov umelej inteligencie od tretích strán?
- Sú vaše AI aplikácie náchylné naprompt injection?
- Ako zabraňujete úniku citlivých údajov?
- Majú vaši agenti umelej inteligencie široké oprávnenia, ktoré by mohli byť zneužité?

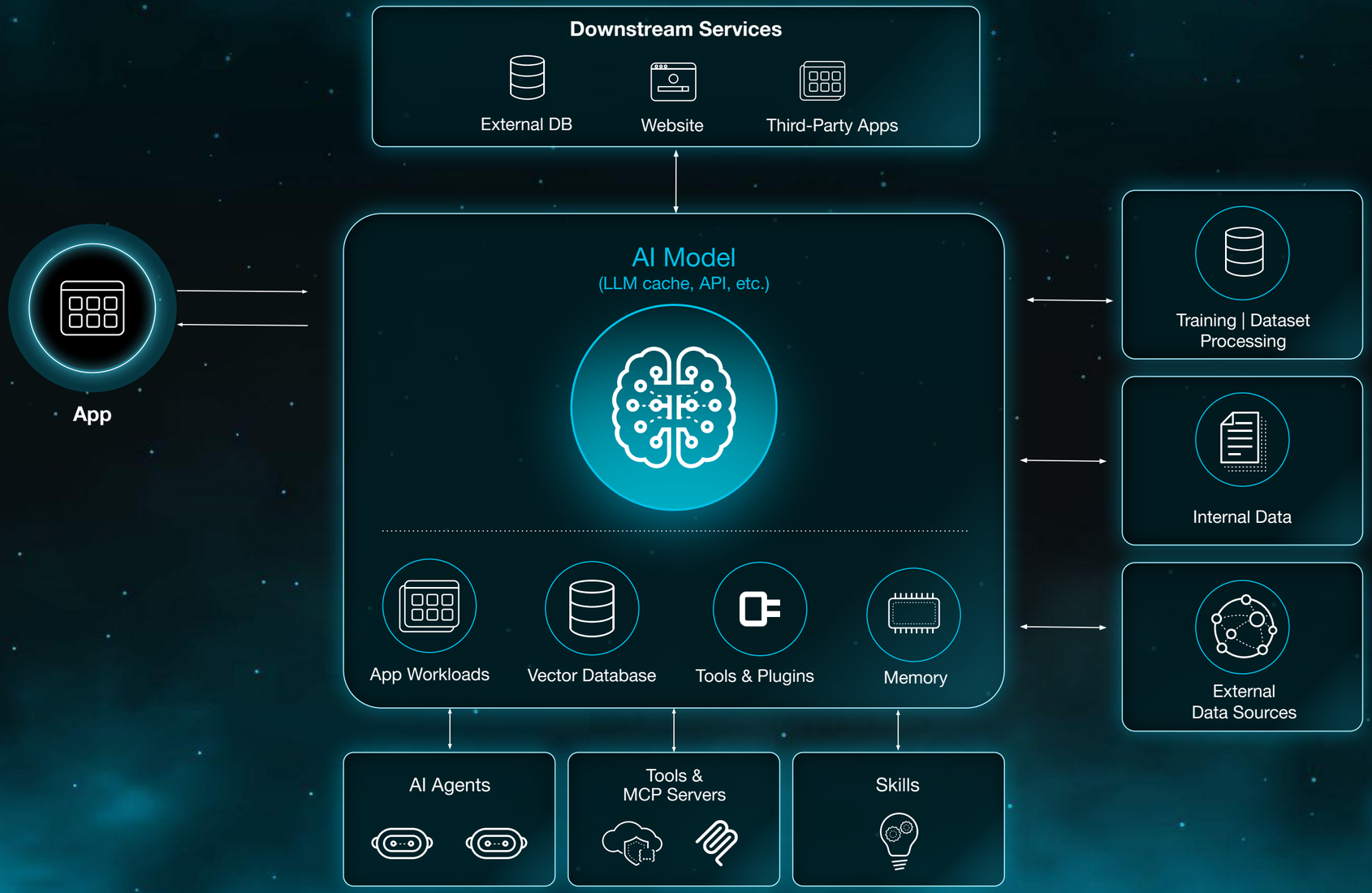


6% organizácií má pokročilý strategický rámec na AI security.

Source: The 2025 AI Index Report, Stanford University, 2025.

paloalto NETWORKS | PRISMA® AIRS

AI Agentmi sa ďalej rozširuje architektúra aplikácií…

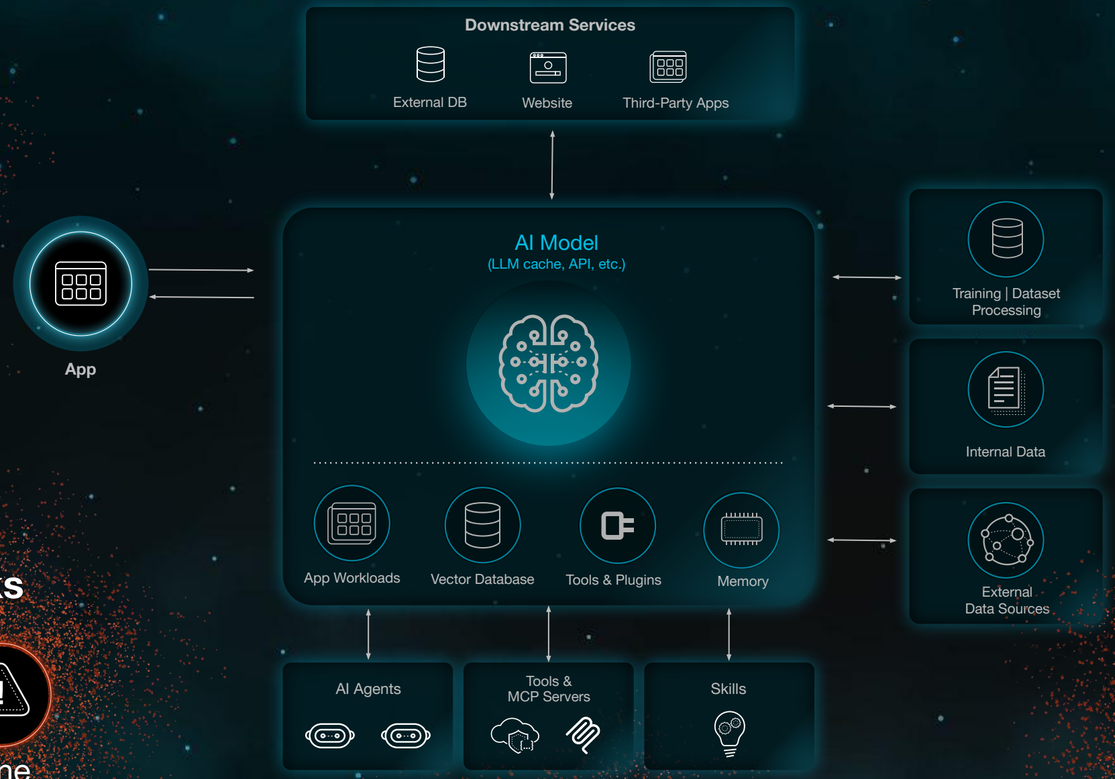


paloalto NETWORKS | PRISMA AIRS

…a prinášajú ešte viac Rizík

Supply Chain Risks

- Vulnerable Agent Artifacts
- Insecure Agent Architecture



Runtime Risks

- Tool Misuse
- Memory Poisoning
- MCP Vulnerabilities

Posture Risks

- Sensitive Data Exposure
- One Privileged Access

Identity Risks

- Identity Gaps
- Traceability
- Identity Impersonation

Governance Risks

- Uncontrolled Access
- Limited Observability

paloalto NETWORKS | PRISMA AIRS

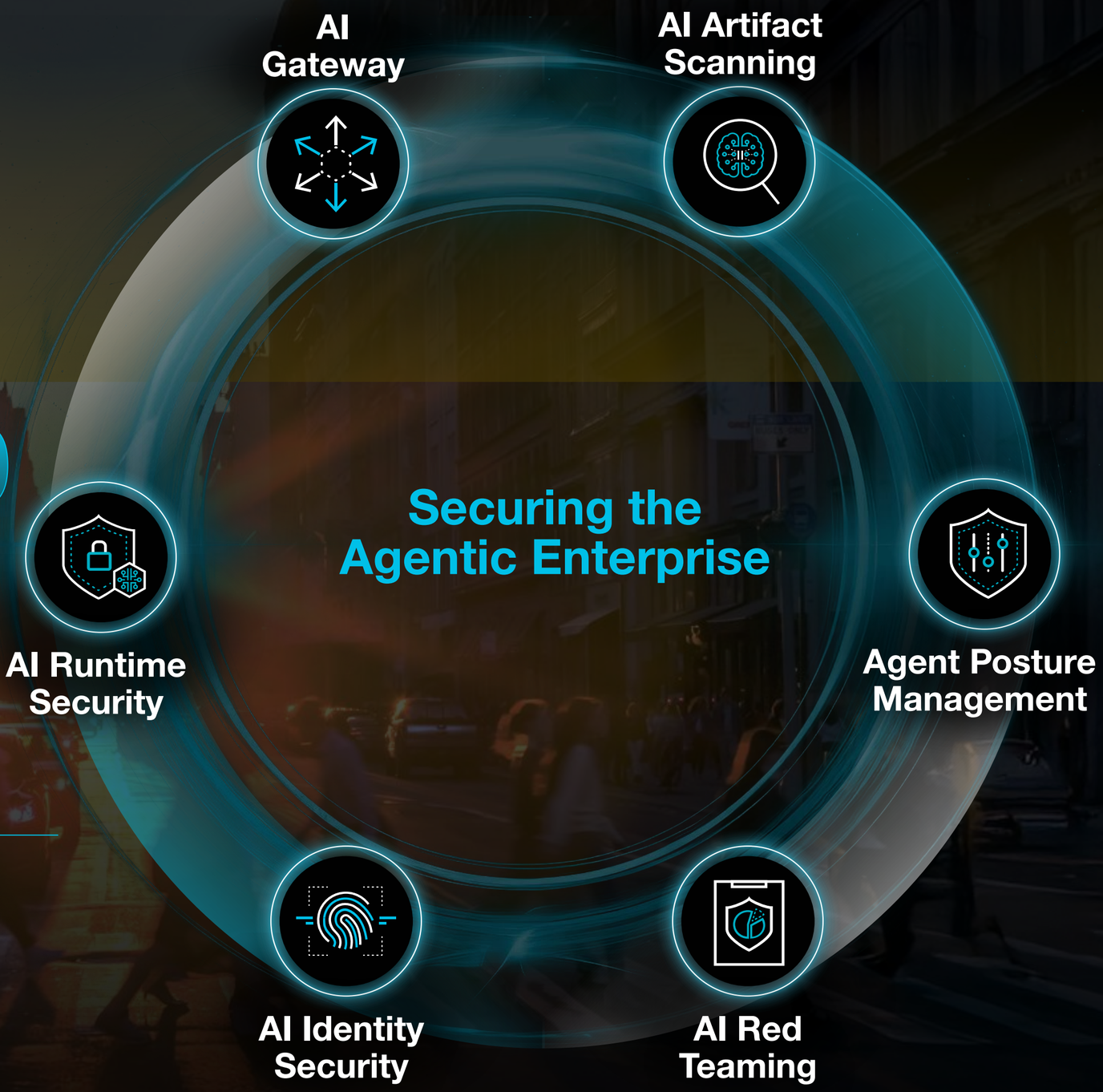
paloalto NETWORKS | PRISMA® AIRS

Predstavujeme Prisma AIRS 3.0

Odhaľte agentov kdekoľvek sú

Neustále **Posudzujte** riziká spojené s AI agentmi

Zabezpečte interakcie AI agentov v reálnom čase



Thank You

paloaltonetworks.com