

Bezpečná IT pevnosť na technológiách Palo Alto

Panelová diskusia

Technológie a procesy

Kybernetické útoky sa neustále vyvíjajú a sú čoraz sofistikovanejšie. Aby sme boli schopní čeliť týmto útokom, musíme mať vo svojom arzenáli dve dôležité zbrane: **procesy** a **technológie**.

Procesy sú neoddeliteľnou súčasťou bezpečnosti a ich obsah sa v priebehu času radikálne nemení. Čo sa však radikálne mení, je **technológia**, ktorá chráni naše údaje a systémy.

Je v podstate nemožné brániť sa proti útoku šitému na mieru pomocou umelej inteligencie bez použitia technológie, ktorá je prinajmenšom rovnako pokročilá.

Antivírus

EDR a XDR

XSIAM

SIEM a Log Management

SOAR



Palo Alto Unit42

WHAT IS THE RANSOMWARE RESILIENCE?

The Ransomware Resilience, powered by Palo Alto Networks, is a community of cybersecurity professionals standing shoulder to shoulder to form a united front against the ever-growing threat of AI-powered cyberthreats. By joining, you'll stay informed about upcoming virtual and in-person events happening in your area. Stay connected with the latest news, insights, and developments in the world of ransomware.

Take a stand today. Join the Ransomware Resilience and be a force for change.

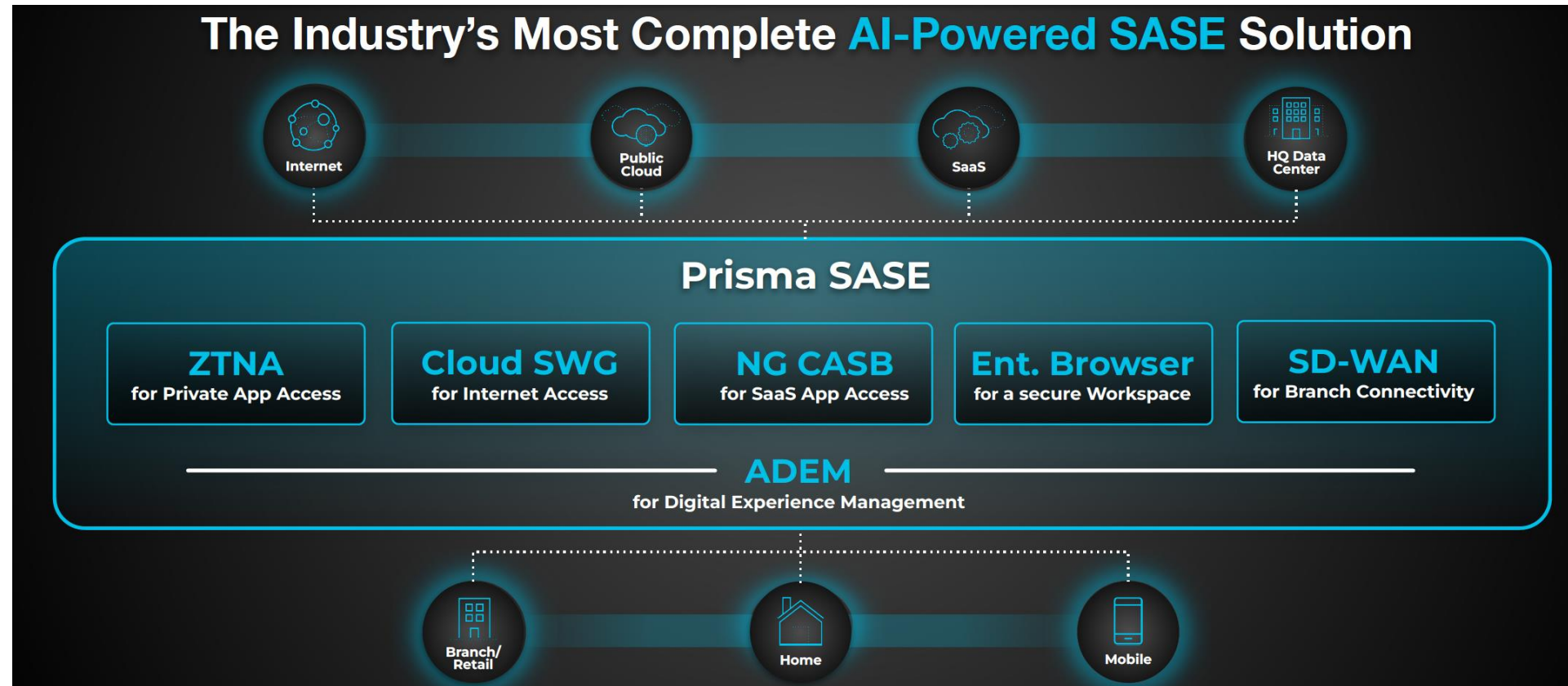


<https://www.paloaltonetworks.com/ransomware-resilience>



Palo Alto a SASE

Securing Any User, Device or App, Anywhere



Palo Alto a OT/IoT

Device Discovery & Visibility

1 Use multiple device discovery techniques to tune setup and quickly establish device inventory within Panorama

Device Behavior Understanding

2 Gain understanding of device communications and device behavior baseline within Panorama

Policy Creation & Enforcement

3 Create & enforce Device-ID policy based on behavior insight for least privilege access within the same dashboard

Zero Trust Security for IoT/OT

Find all devices, assess all risks, monitor behavior anomalies, prevent known and unknown threats, and secure every digital interaction.

Automated Policy Recommendations

Makes Zero Trust adoption easy with prescriptive least-privileged access policy recommendations & one-click enforcement

Network Segmentation

Segment connected IoT/OT devices & apply Zero Trust policies to prevent attacks & lateral movement of threats

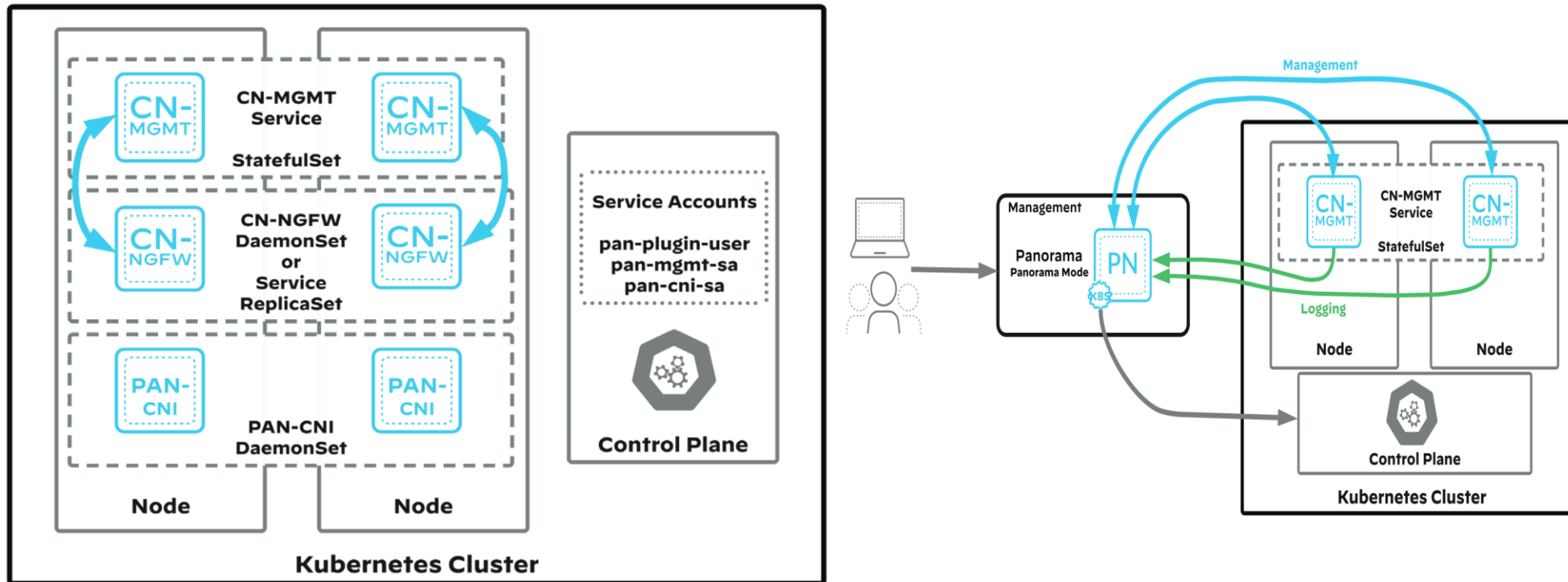
Asset Management

Transform a static asset inventory into a dynamic asset inventory with complete visibility, and context-based risk analysis



Palo Alto a ochrana K8s prostředí

The CN-Series firewall is natively integrated into Kubernetes (K8s) to provide complete application (Layer 7) visibility, application-level segmentation, DNS Security, and protection from advanced threats for traffic entering, exiting, and moving within a trusted zone.



ĎAKUJEME ZA POZORNOST

Alanata

Technology Meets Business

Alanata a.s.

Einsteinova Business Center
Krasovského 14
851 01 Bratislava 5
Slovenská republika

www.alanata.sk