paloalto NETWORKS

Alanata
Technology Meets People

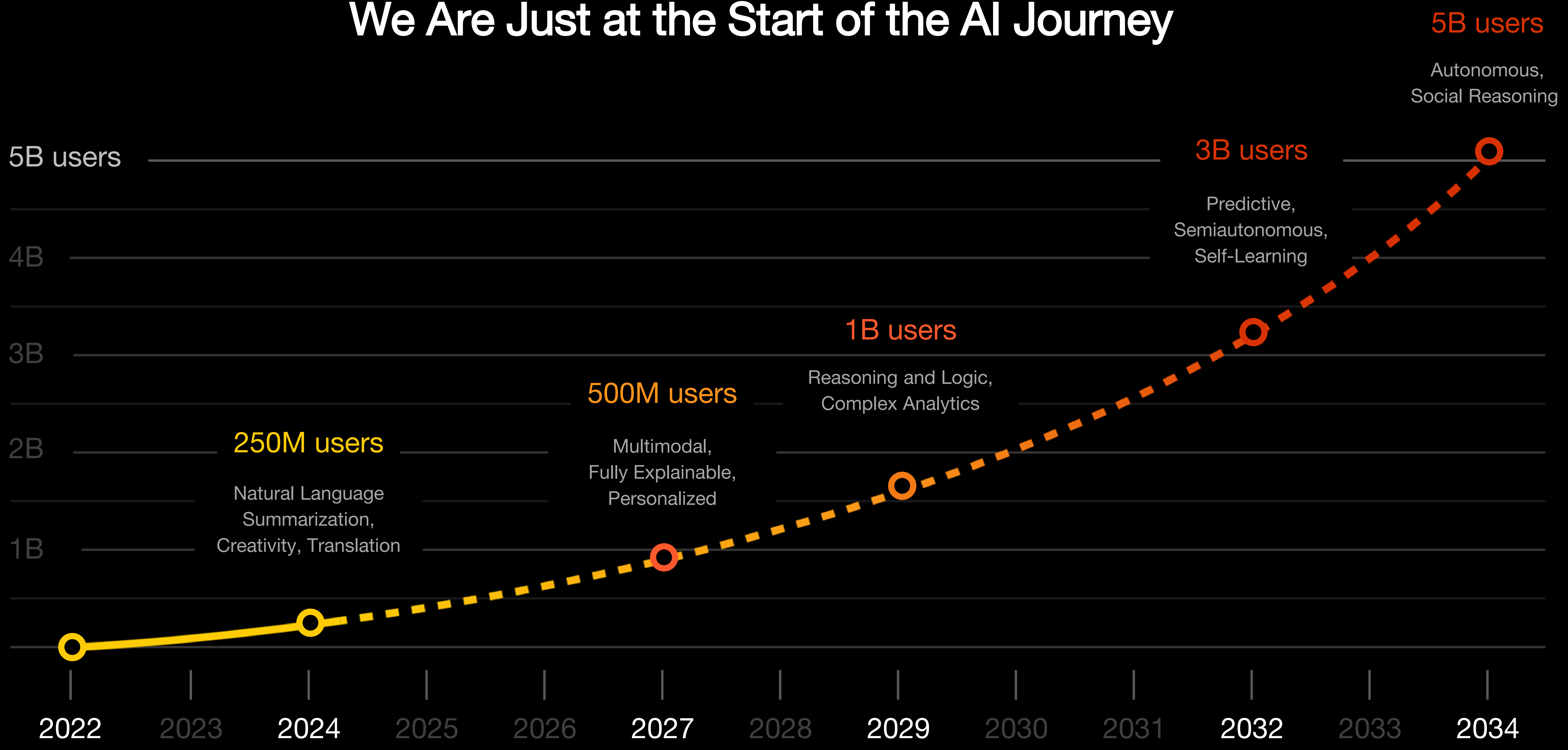
Future of AI and Cyber Security

Luboš Klokner

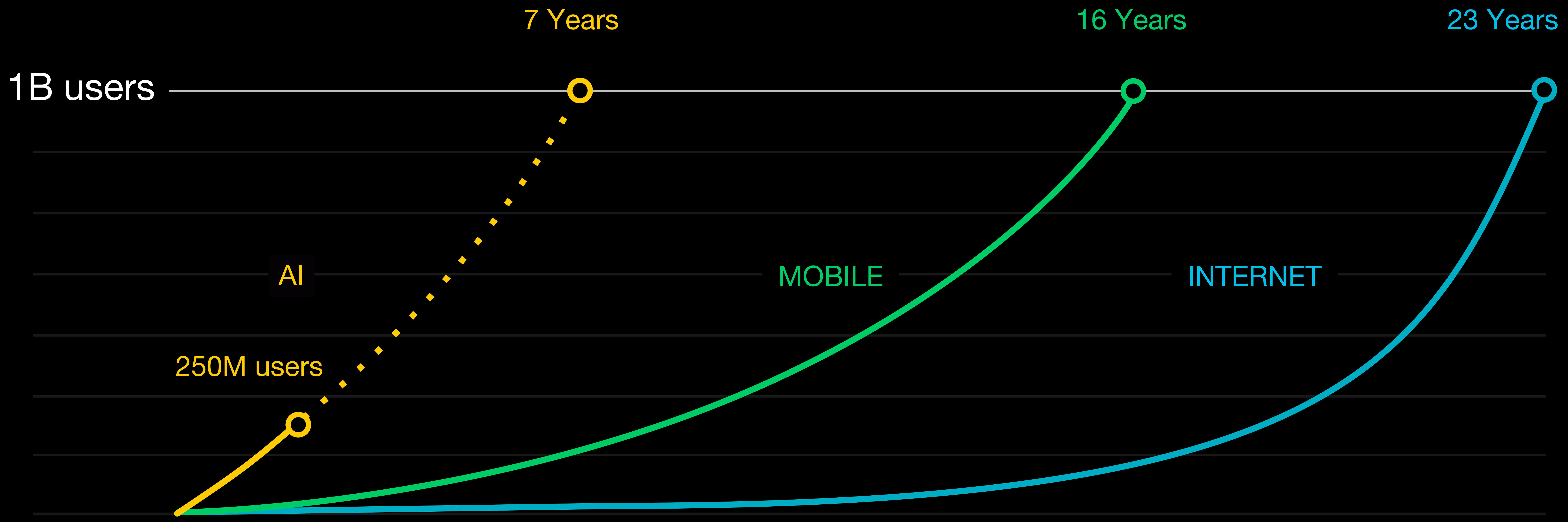
Solutions Consultant | Palo Alto Networks

SOMEWHERE ACROSS THE BUSINESS

We Are Just at the Start of the AI Journey



AI Is Already the Fastest-Growing Technology in Our History



Source: Internet World Stats; assumed internet inception in 1982 after US DoD standardized TCP/IP protocol

Cybersecurity Has Seen Progress Toward Autonomous Security

Signature-Based Attack Prevention

IDS → IPS

ML-Based Prevention

AV → EDR

Preprogrammed Workflow Automation

RPA → SOAR

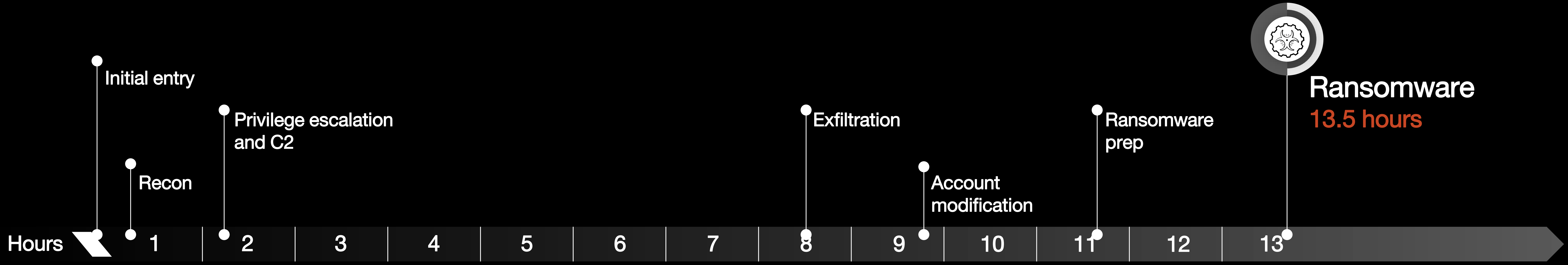
Automated Analytics

Dashboards → AIOps

Yet Being a Security Practitioner Is Still Too Complicated

AI Will Significantly Accelerate and Scale Ransomware Attacks

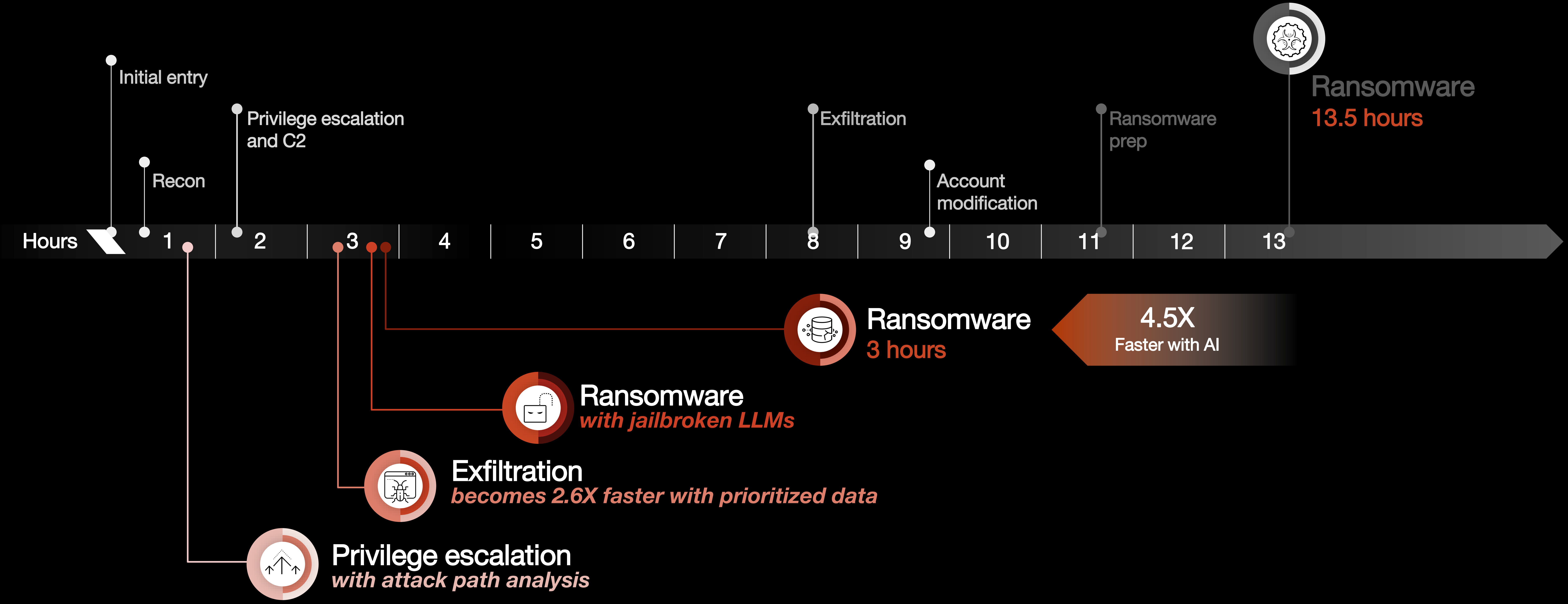
Unit 42 Casefile: What if Black Basta Attack Leveraged AI?



https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2024-unit42-incident-response-report.pdf

AI Will Significantly Accelerate and Scale Ransomware Attacks

Unit 42 Casefile: What if Black Basta Attack Leveraged AI?



Initial entry

Recon

Privilege escalation and C2

Exfiltration

Account modification

Ransomware prep

Ransomware 13.5 hours

Ransomware 3 hours

4.5X Faster with AI

Ransomware *with jailbroken LLMs*

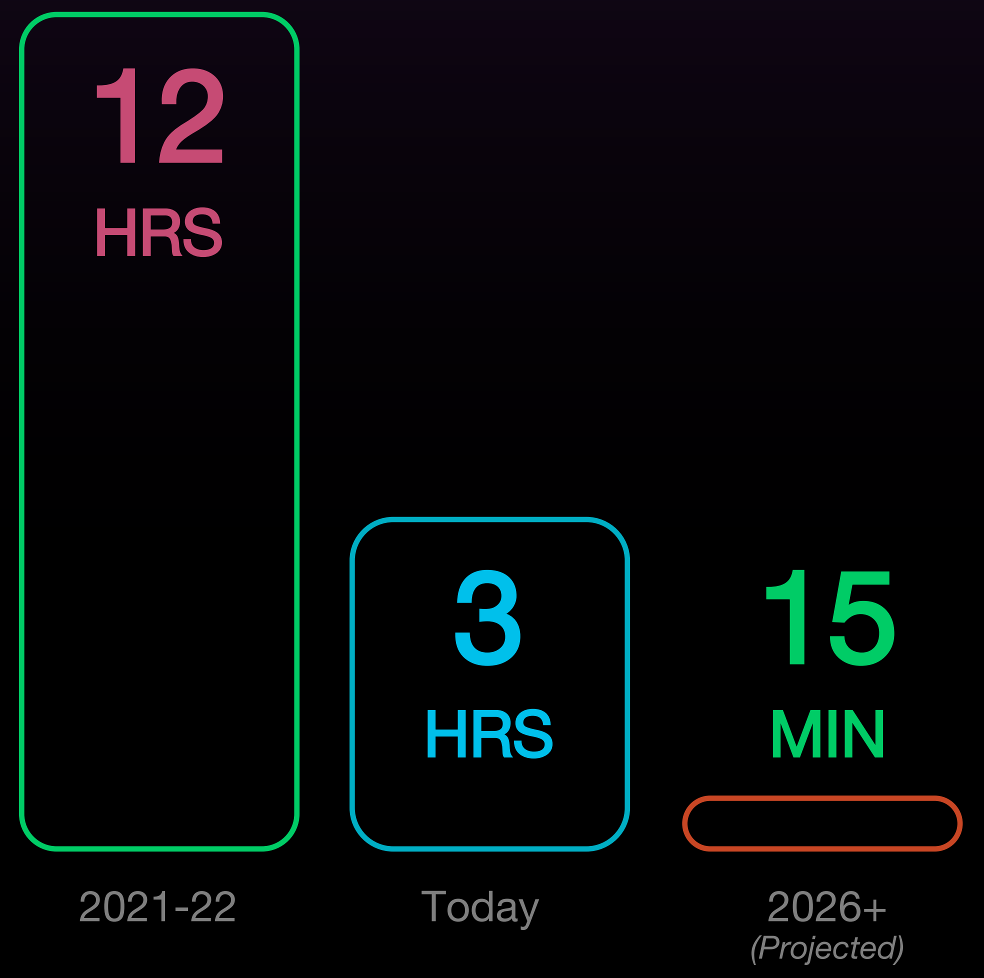
Exfiltration *becomes 2.6X faster with prioritized data*

Privilege escalation *with attack path analysis*

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2024-unit42-incident-response-report.pdf

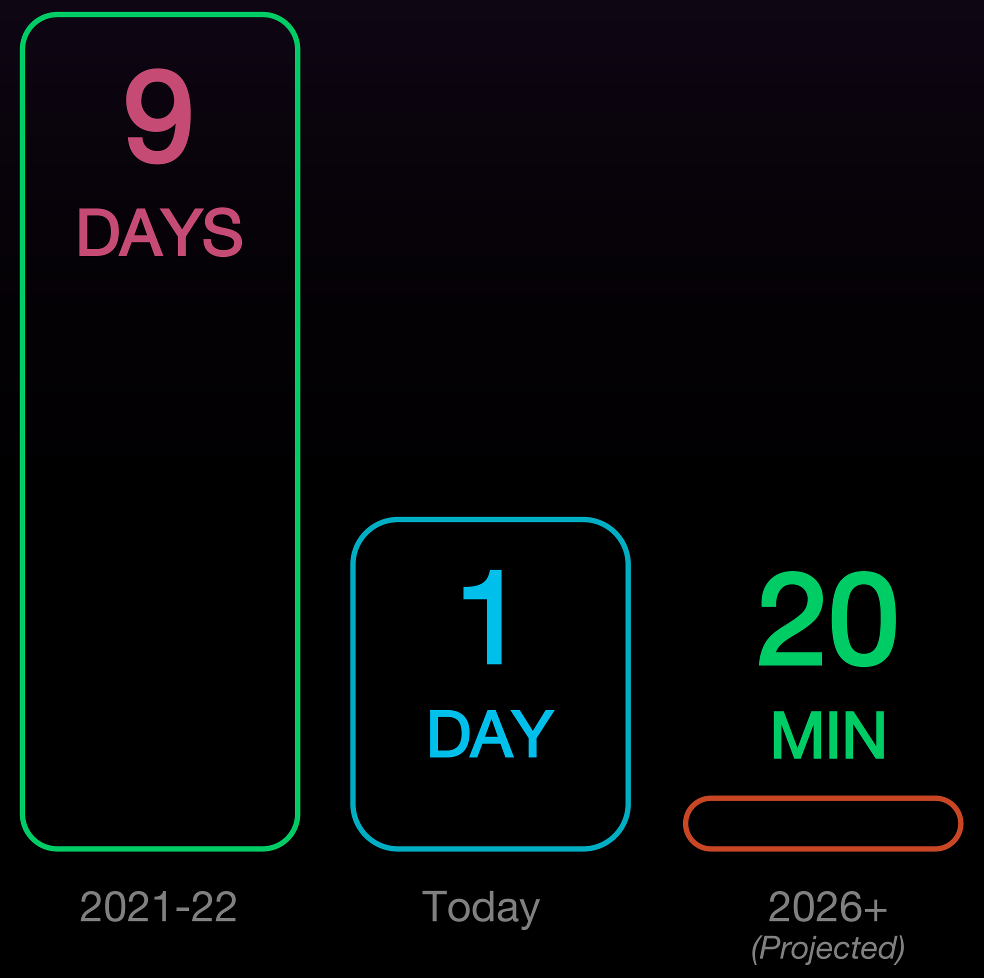
AI Is Turbocharging the Speed and Scale of Attacks

Build Ransomware



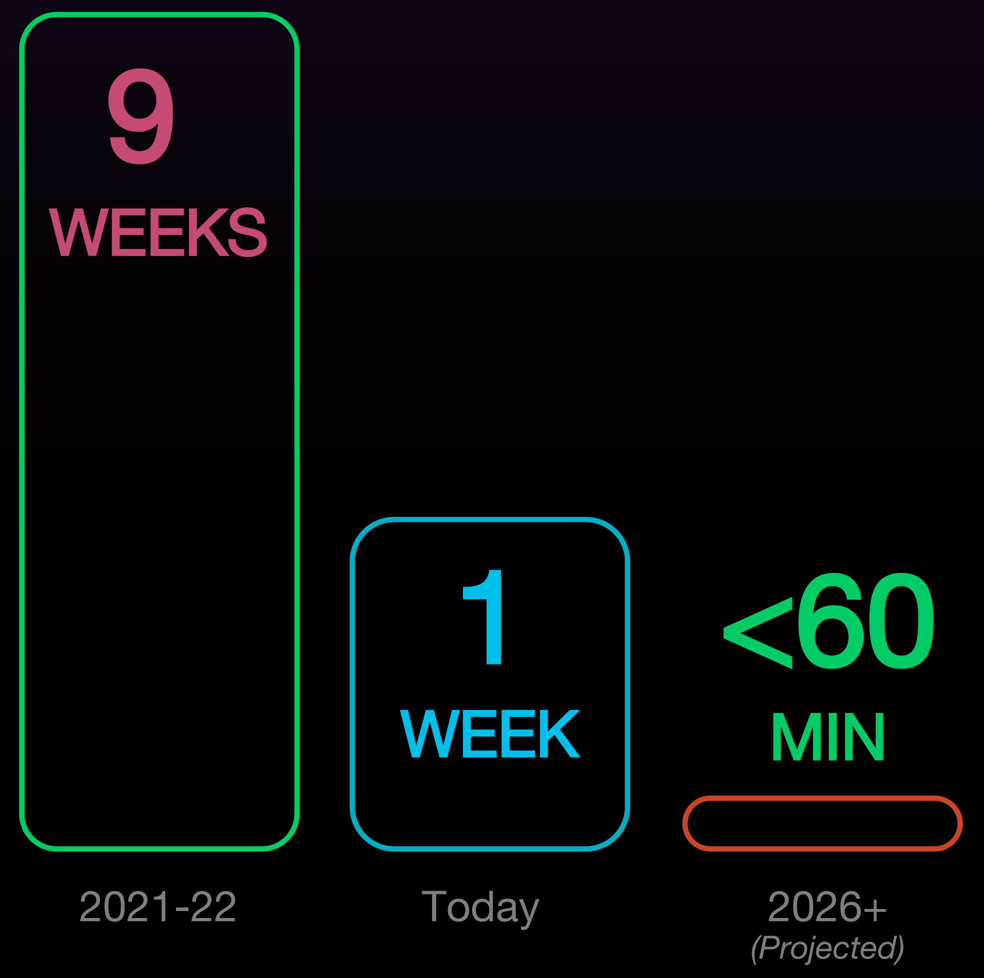
$2B impact from attack on a US health insurer in 2024

Compromise & Exfiltrate



15 million users' PII and confidential data exfiltrated in Jan 2024

Exploit Vulnerability



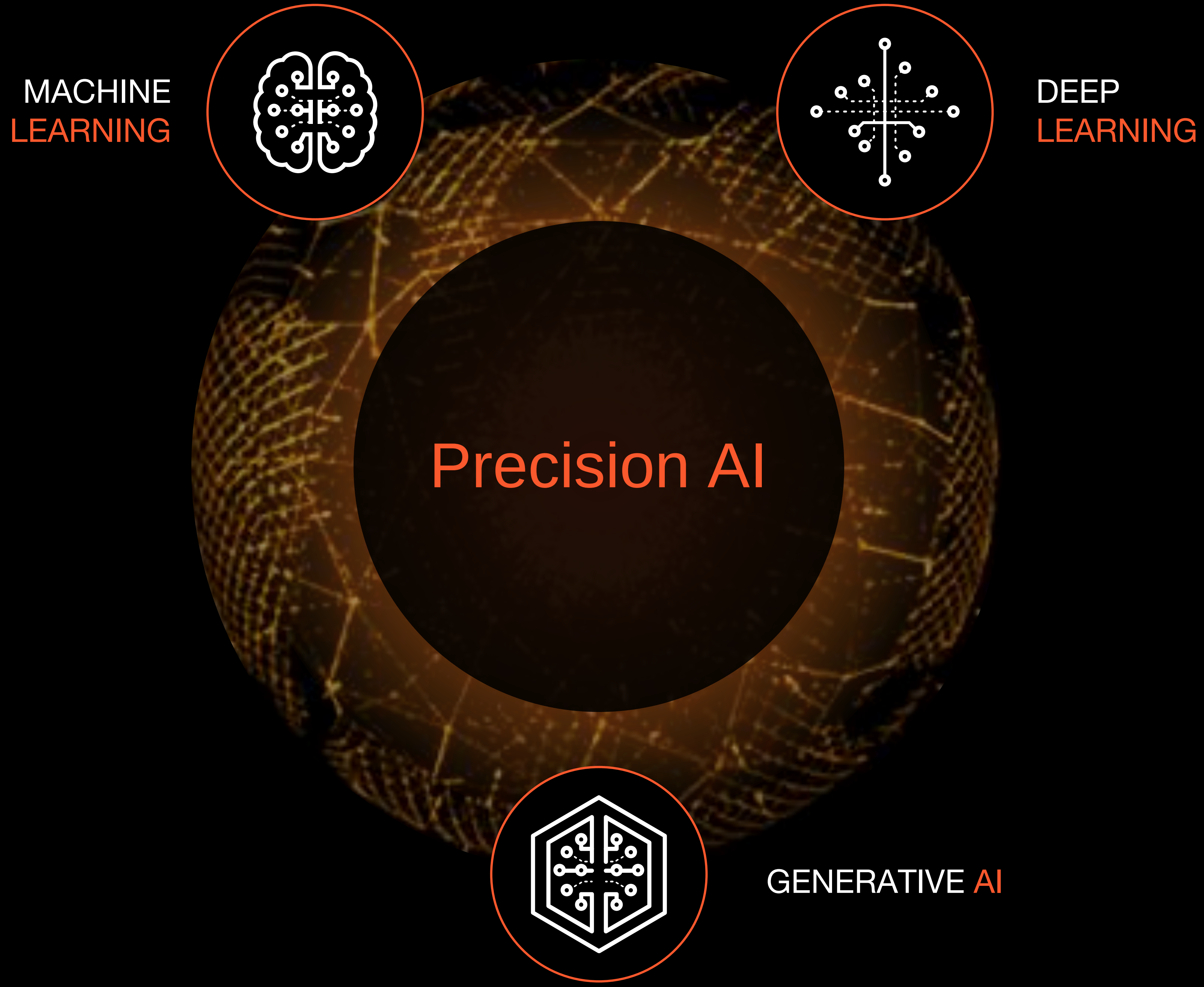
500+ organizations and 35+ million people affected by MoveIT vulnerability

Sources: 56% increase in exploited Zero Days in 2023 (Year-on-Year increase based on Google Cloud Blog March 26 2024), 73% increase in Ransomware attacks in 2023 (SANS Blog Jan 15 2024),78% increase in data breaches and leaks in 2023 (WSJ Article March 15 2024), Most companies need >2-3 days to resolve an incident (XSIAM customer interviews and XSIAM product telemetry for customers)

Precision AI™

Is How We Counter Adversarial AI

Leveraging the best of AI; avoiding the limitations



Precision AI

We're Ready for the AI Fight

STRATA™

ZERO TRUST PLATFORM

Inspect connections and block attacks with Precision AI

ADV TP	ADV URL	ADV WF	ADV DNS
DLP	GP	NG CASB	IoT

PRISMA® CLOUD

CODE TO CLOUD PLATFORM

Identify and remediate cloud security issues at scale with Precision AI

CSPM	CIEM	VM-Series
DPSM	CWP	WAAS

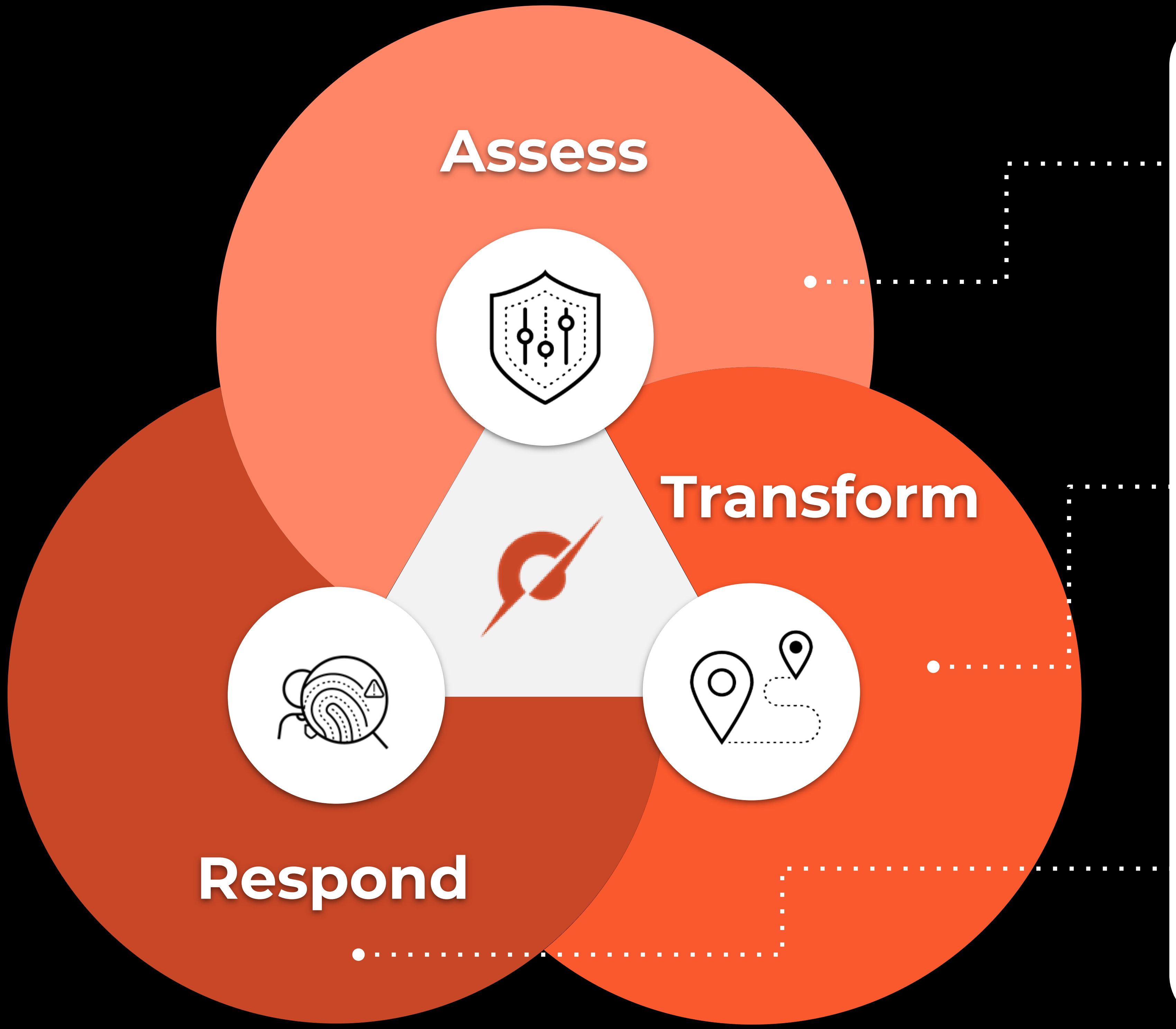
CORTEX®

AI-DRIVEN SOC PLATFORM

Real-time detection, investigation, and remediation with Precision AI

SIEM	EDR	SOAR	NTA
ASM	ITDR	TIM	CDR

UNIT 42 Intelligence Driven. Response Ready.



Cyber Risk Management

Assess and test your security controls against the right threats with Proactive Assessments and Incident Simulation Services

Transform your security strategy with a threat-informed approach with Strategic Advisory Services

Incident Response

Respond in record time with Incident Response and Digital Forensics Services

Unit 42 Retainer
Get Unit 42 on speed dial as your proactive partner. All hours can be used for Incident Response or for any of our Cyber Risk Management Services.

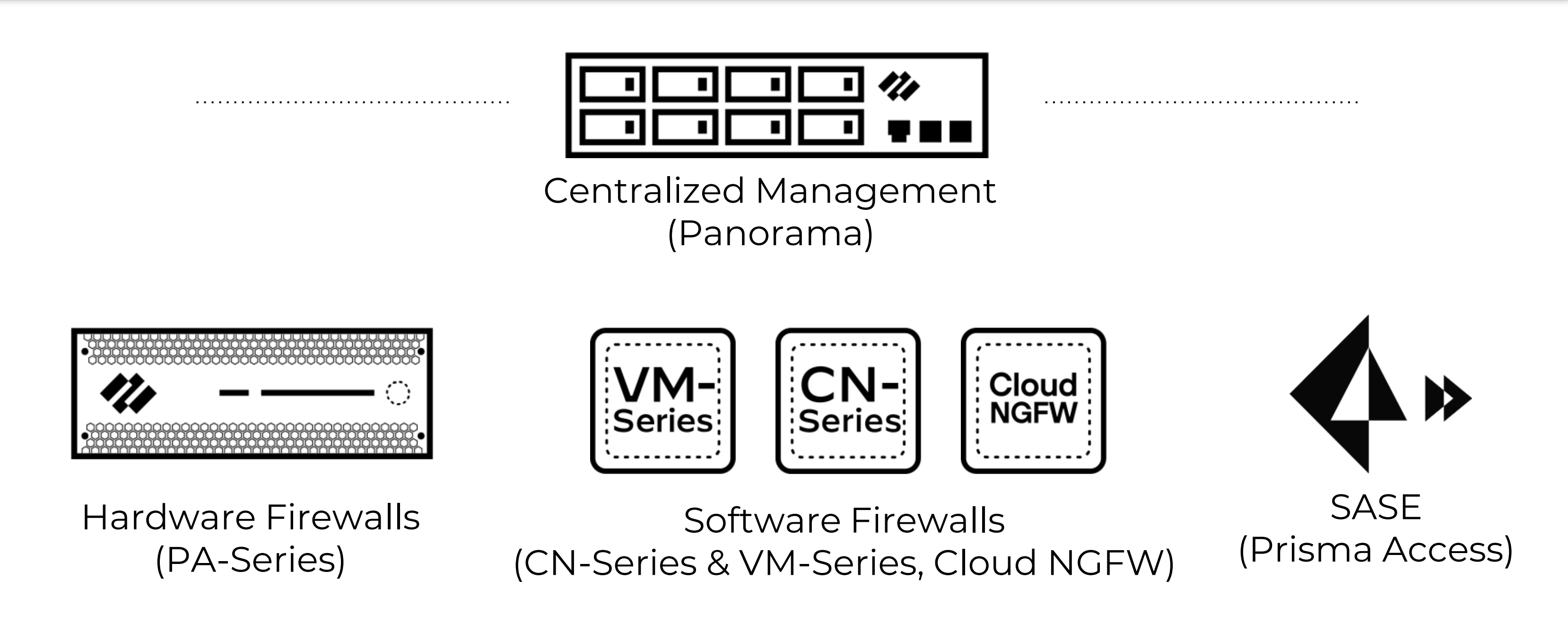
STRATA™

BY PALO ALTO NETWORKS

Future Proof Your Network Security

- APP-ID
- Identity
- Content-ID
- Device-ID
- TLS & SSL Decryption
- Single-Pass Architecture

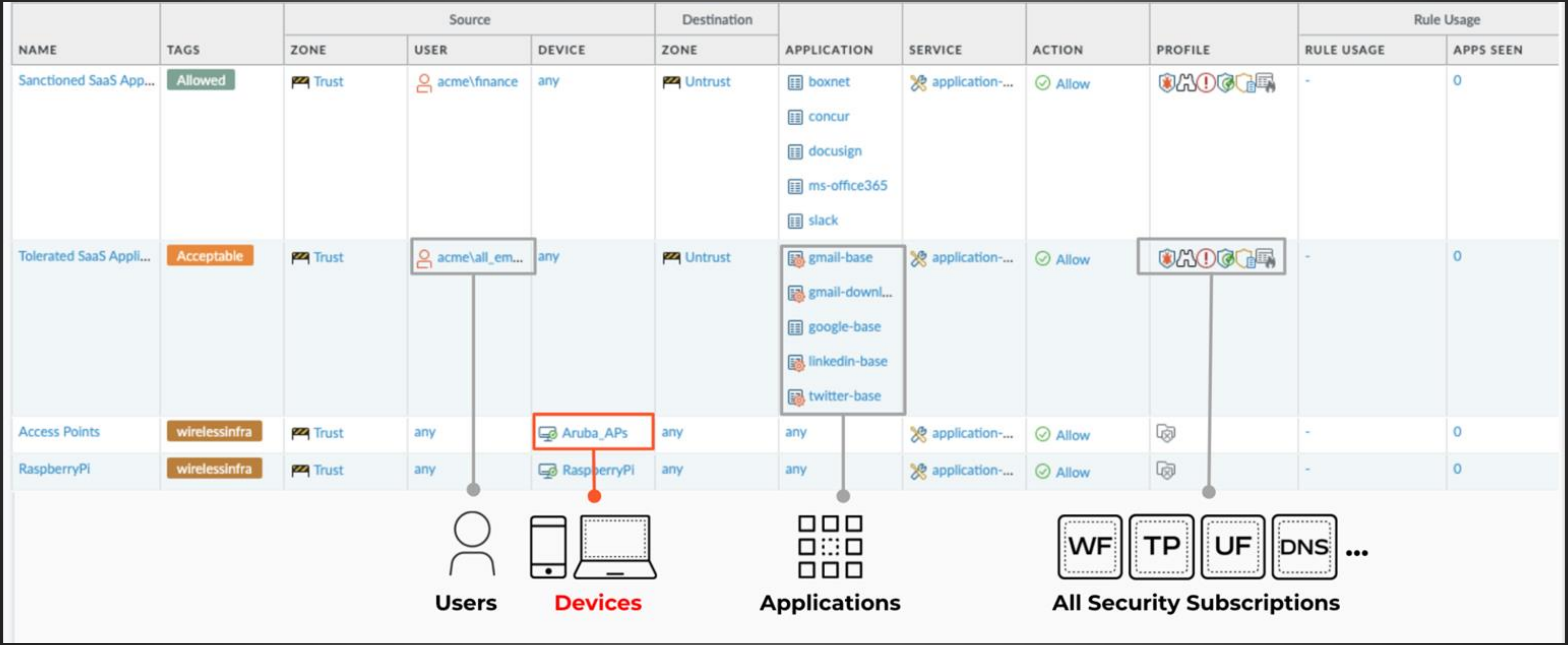
Powered by the same PAN-OS



STRATA

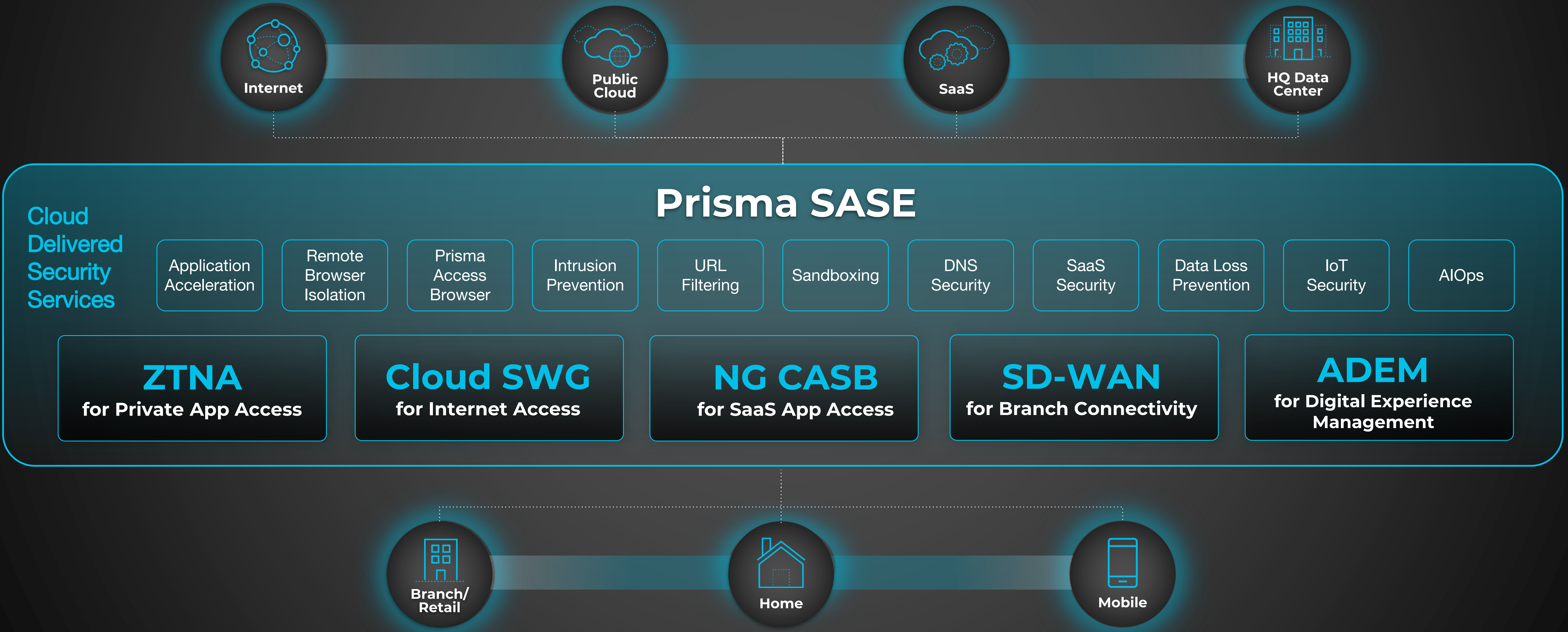
Next Generation Firewalls | **PAN-OS** | Cloud Delivered Security Services | Secure Access Service Edge (SASE)

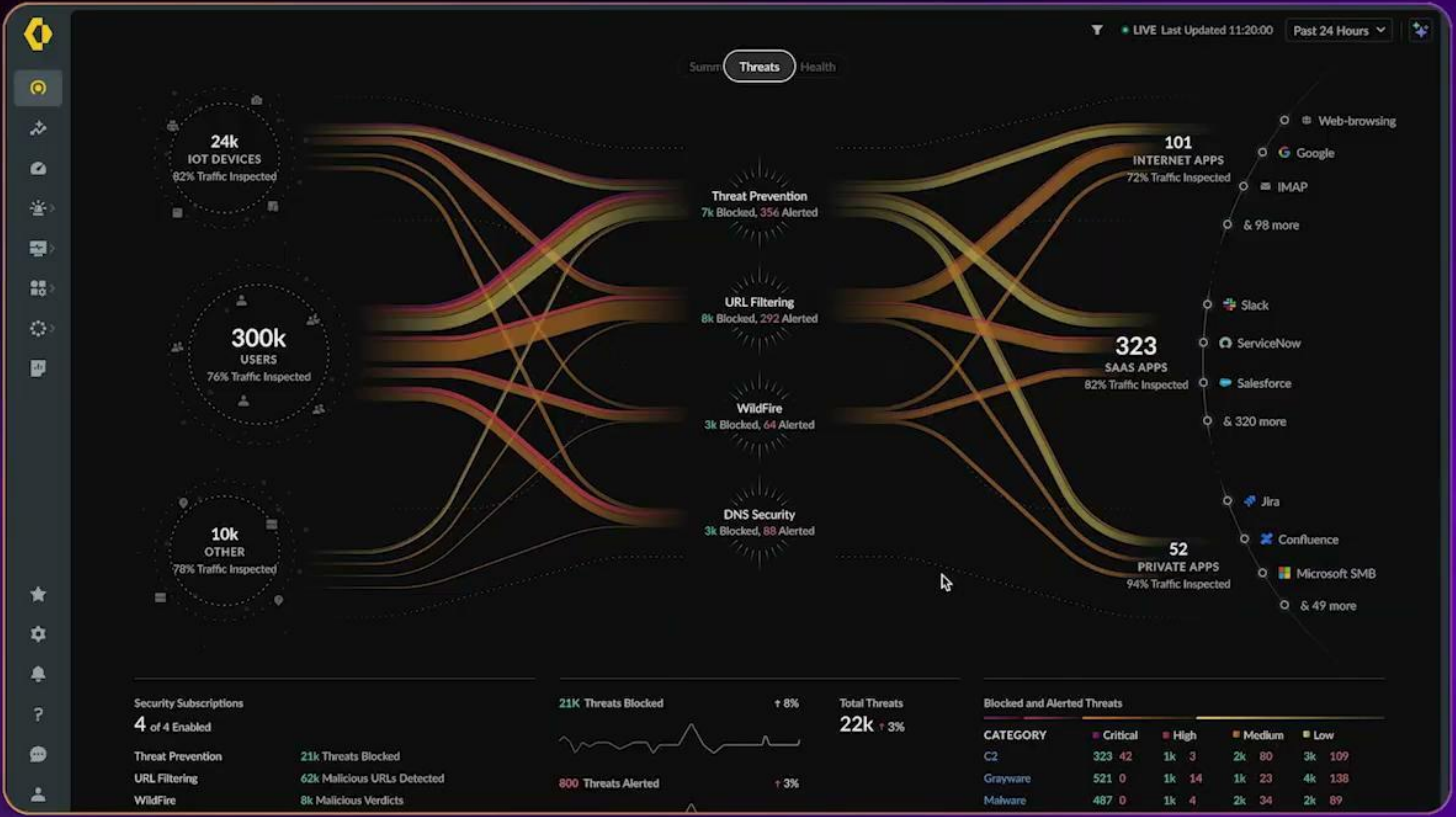
APP-ID | Identity | Cloud Identity Engine | Content-ID | Device-ID | TLS & SSL Decryption | Single Pass Architecture | Web Proxy for NGFW



		Source			Destination					Rule Usage	
NAME	TAGS	ZONE	USER	DEVICE	ZONE	APPLICATION	SERVICE	ACTION	PROFILE	RULE USAGE	APPS SEEN
Sanctioned SaaS App...	Allowed	Trust	acme\finance	any	Untrust	boxnet concur docusign ms-office365 slack	application-...	Allow		-	0
Tolerated SaaS Appli...	Acceptable	Trust	acme\all_em...	any	Untrust	gmail-base gmail-downl... google-base linkedin-base twitter-base	application-...	Allow		-	0
Access Points	wirelessinfra	Trust	any	Aruba_APs	any	any	application-...	Allow		-	0
RaspberryPi	wirelessinfra	Trust	any	RaspberryPi	any	any	application-...	Allow		-	0

The Industry’s Most Complete AI-Powered SASE Solution





Security Subscriptions
4 of 4 Enabled

Threat Prevention	21k Threats Blocked
URL Filtering	62k Malicious URLs Detected
WildFire	8k Malicious Verdicts

21K Threats Blocked ↑ 8%

800 Threats Alerted ↑ 3%

Total Threats
22k ↑ 3%

Blocked and Alerted Threats

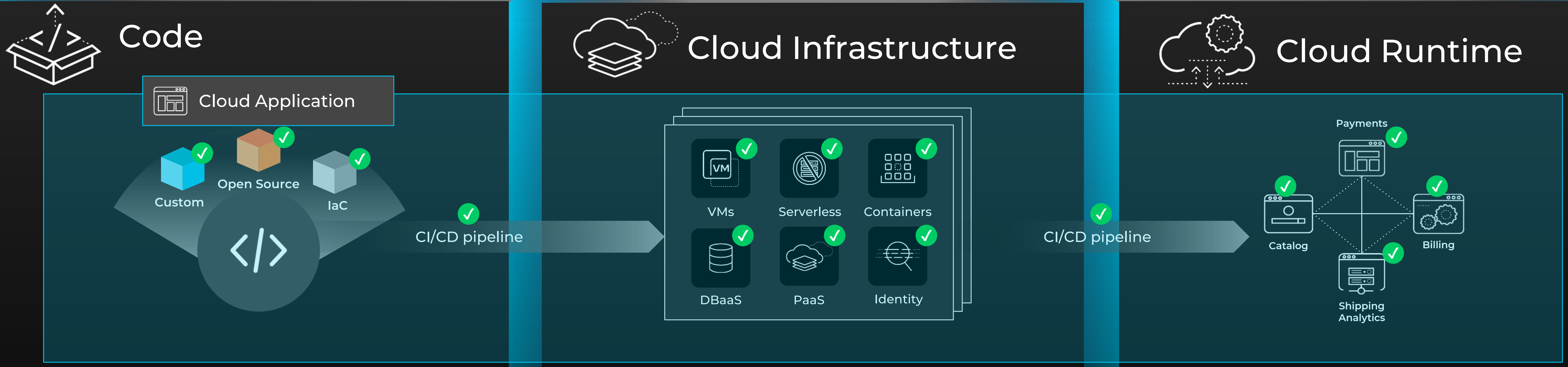
CATEGORY	Critical		High		Medium		Low	
C2	323	42	1k	3	2k	80	3k	109
Grayware	521	0	1k	14	1k	23	4k	138
Malware	487	0	1k	4	2k	34	2k	89

PRISMA®
BY PALO ALTO NETWORKS

PRISMA CLOUD

Secure The Source | Secure The Infrastructure | Secure The Runtime | Licensing

IaC | SCA | CI/CD | Secrets | CSPM | CIEM | DSPM | CDEM | Host Security | Container Security | Serverless Security | WAAS | CNS



Risk Prevention

Complete and contextualized security in Code Phase:
IaC, SCA, CI/CD, Secrets

Secure The Source

Visibility & Control

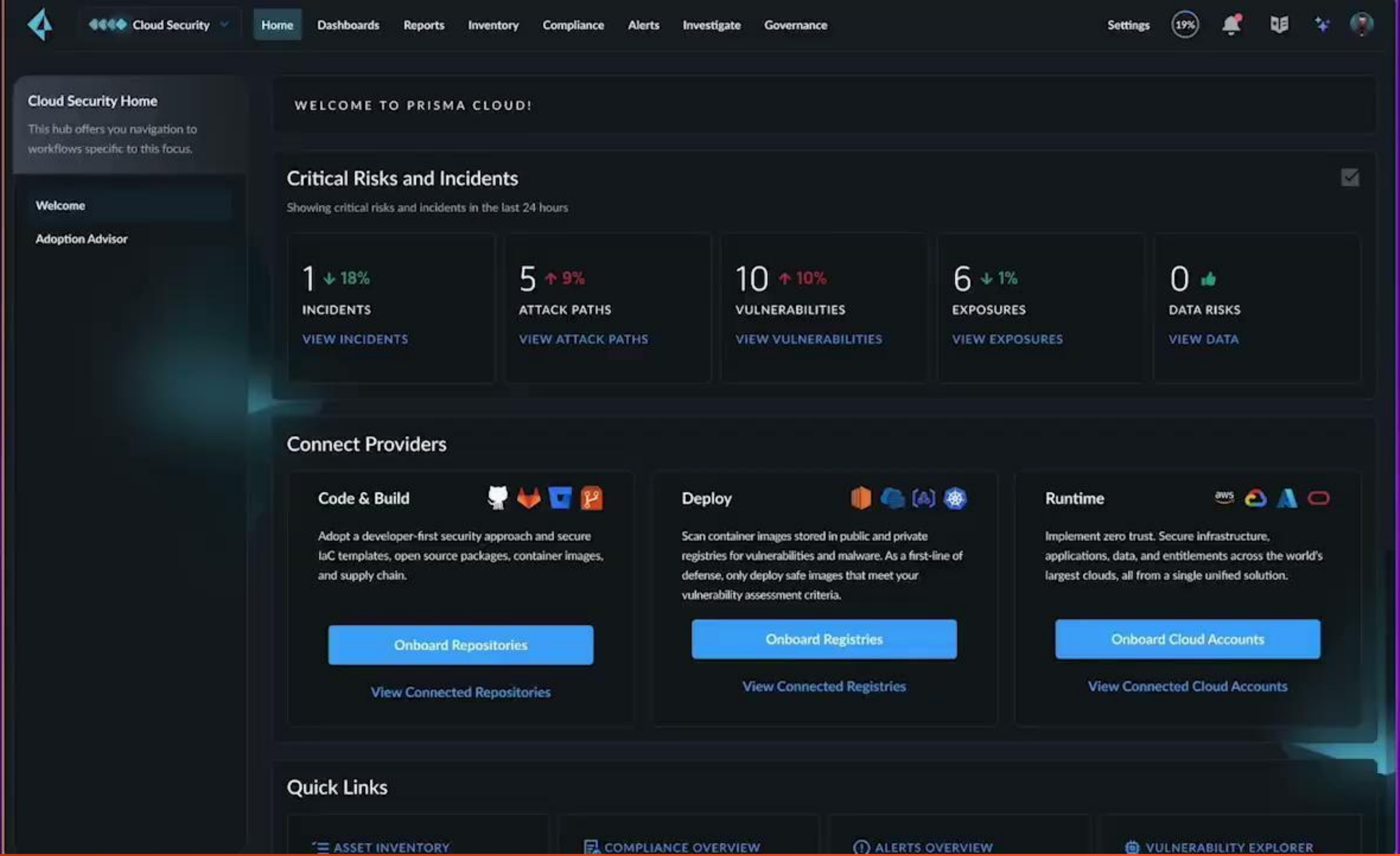
Unmatched visibility: Applications, Workloads, Data, Identity, Services, APIs, Unsanctioned Clouds
CSPM, CIEM, DSPM, CDEM

Secure The Infrastructure

Runtime Protection

Proactive Runtime Detection and Prevention:
CWPP, WAAS, CNS

Secure The Runtime



Cloud Security Home

This hub offers you navigation to workflows specific to this focus.

WELCOME TO PRISMA CLOUD!

Critical Risks and Incidents

Showing critical risks and incidents in the last 24 hours

1 ↓ 18%	5 ↑ 9%	10 ↑ 10%	6 ↓ 1%	0
INCIDENTS	ATTACK PATHS	VULNERABILITIES	EXPOSURES	DATA RISKS
VIEW INCIDENTS	VIEW ATTACK PATHS	VIEW VULNERABILITIES	VIEW EXPOSURES	VIEW DATA

Connect Providers

Code & Build

Adopt a developer-first security approach and secure IaC templates, open source packages, container images, and supply chain.

Onboard Repositories

View Connected Repositories

Deploy

Scan container images stored in public and private registries for vulnerabilities and malware. As a first-line of defense, only deploy safe images that meet your vulnerability assessment criteria.

Onboard Registries

View Connected Registries

Runtime

Implement zero trust. Secure infrastructure, applications, data, and entitlements across the world's largest clouds, all from a single unified solution.

Onboard Cloud Accounts

View Connected Cloud Accounts

Quick Links

CORTEX®

BY PALO ALTO NETWORKS

CORTEX

Cortex XDR | Cortex XSOAR | Cortex XPANSE | Cortex XSIAM

A Holistic Platform For Delivering SOC Services

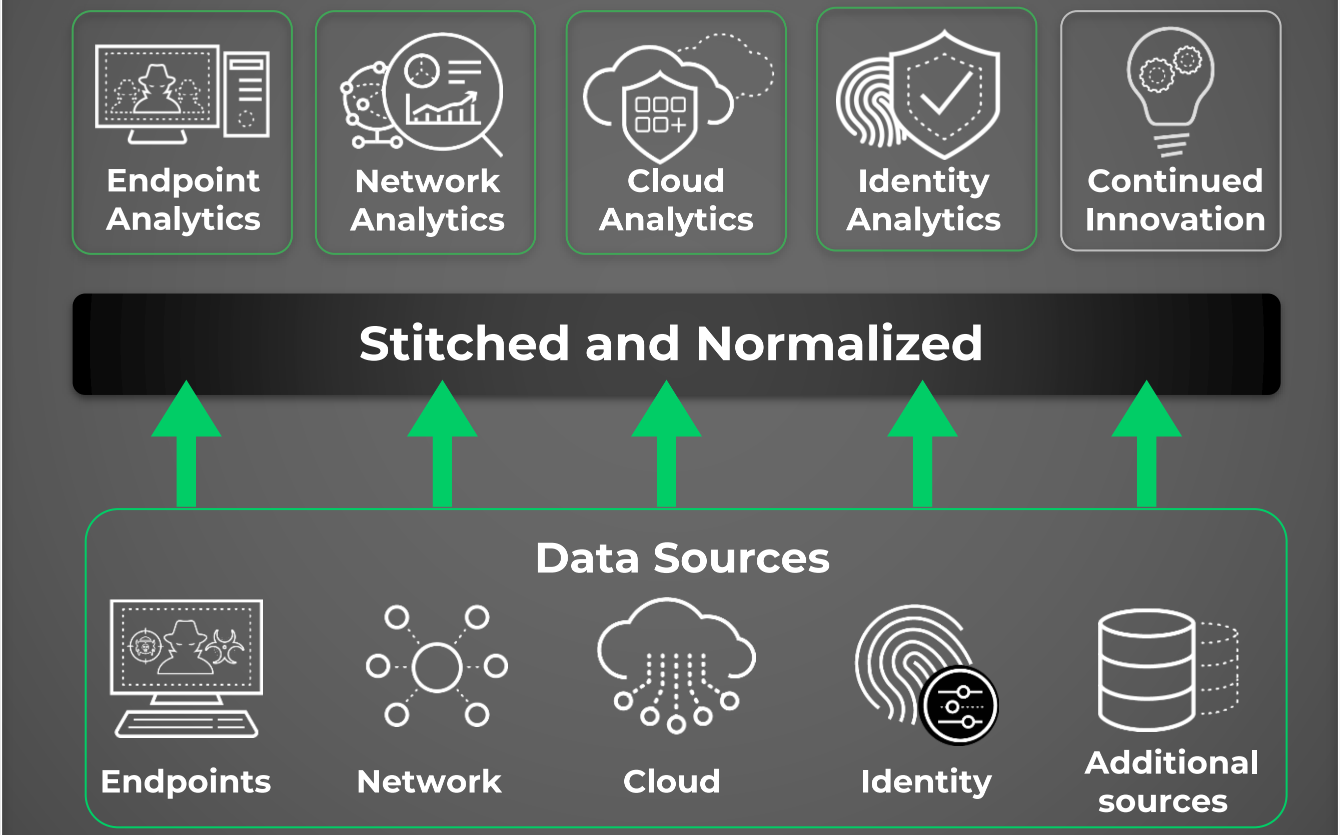
Cortex XPANSE

Discovers and reduces the entire **attack surface**

Cross correlates **internal view of assets with outside-in** mapping

Understands exposure to new attacks and how attacks have unfolded (including **supply chain exposures** and nation-state vulnerabilities)

Cortex XDR



Endpoint Analytics

Network Analytics

Cloud Analytics

Identity Analytics

Continued Innovation

Stitched and Normalized

Data Sources

Endpoints

Network

Cloud

Identity

Additional sources

Cortex XSOAR

Scales and accelerates security operations with automaton

Reduces manual steps in your incident response workflow by up 10 100%

Easily deploy new automation cases via **extensive SOAR marketplace**

Unified SecOps Platform

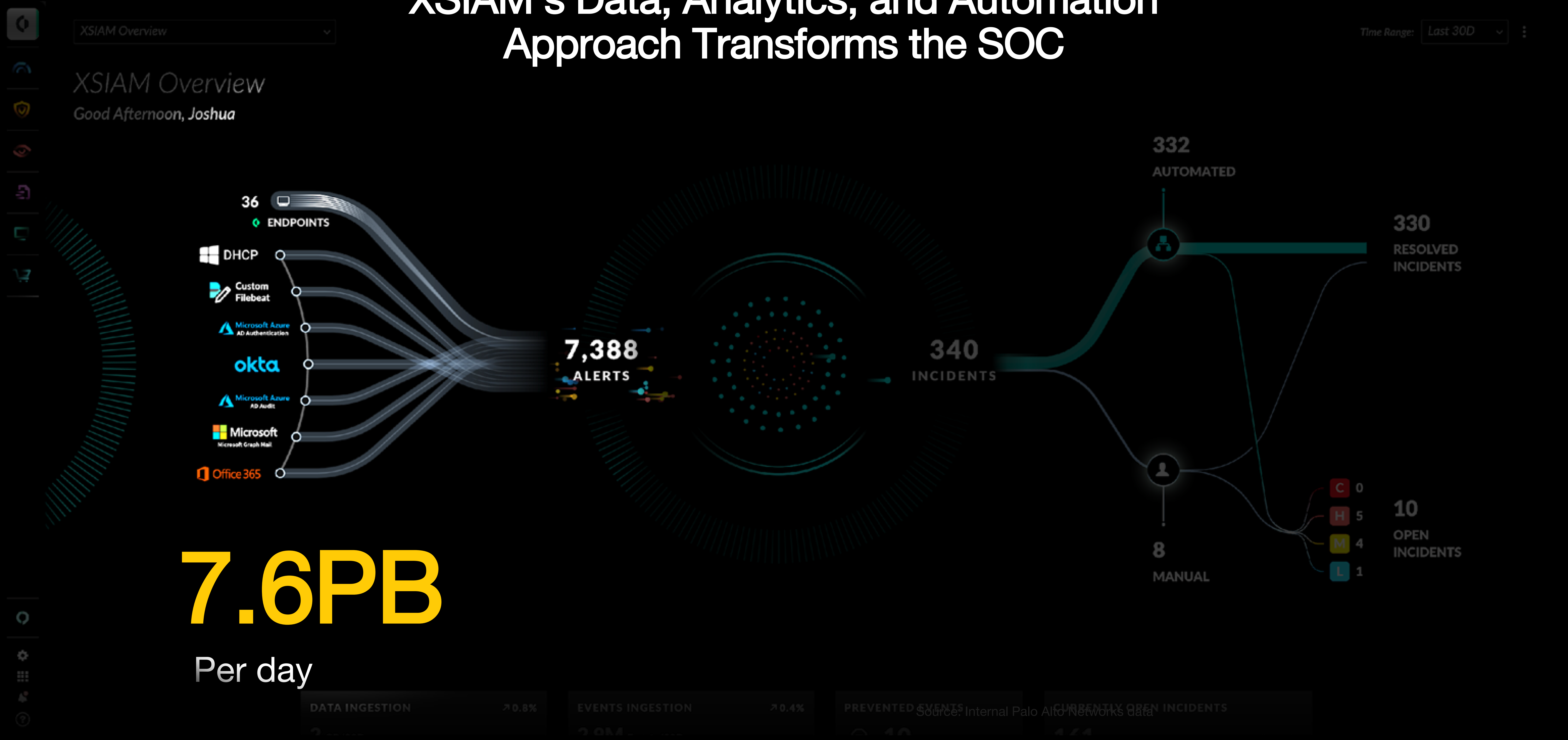
XSIAM

Cortex XSIAM

Unify SOC Operations with an integrated AI-driven platform

End-to-end workflow automation for security operations

XSIAM's Data, Analytics, and Automation Approach Transforms the SOC



XSIAM Overview

Time Range: Last 30D

XSIAM Overview

Good Afternoon, Joshua

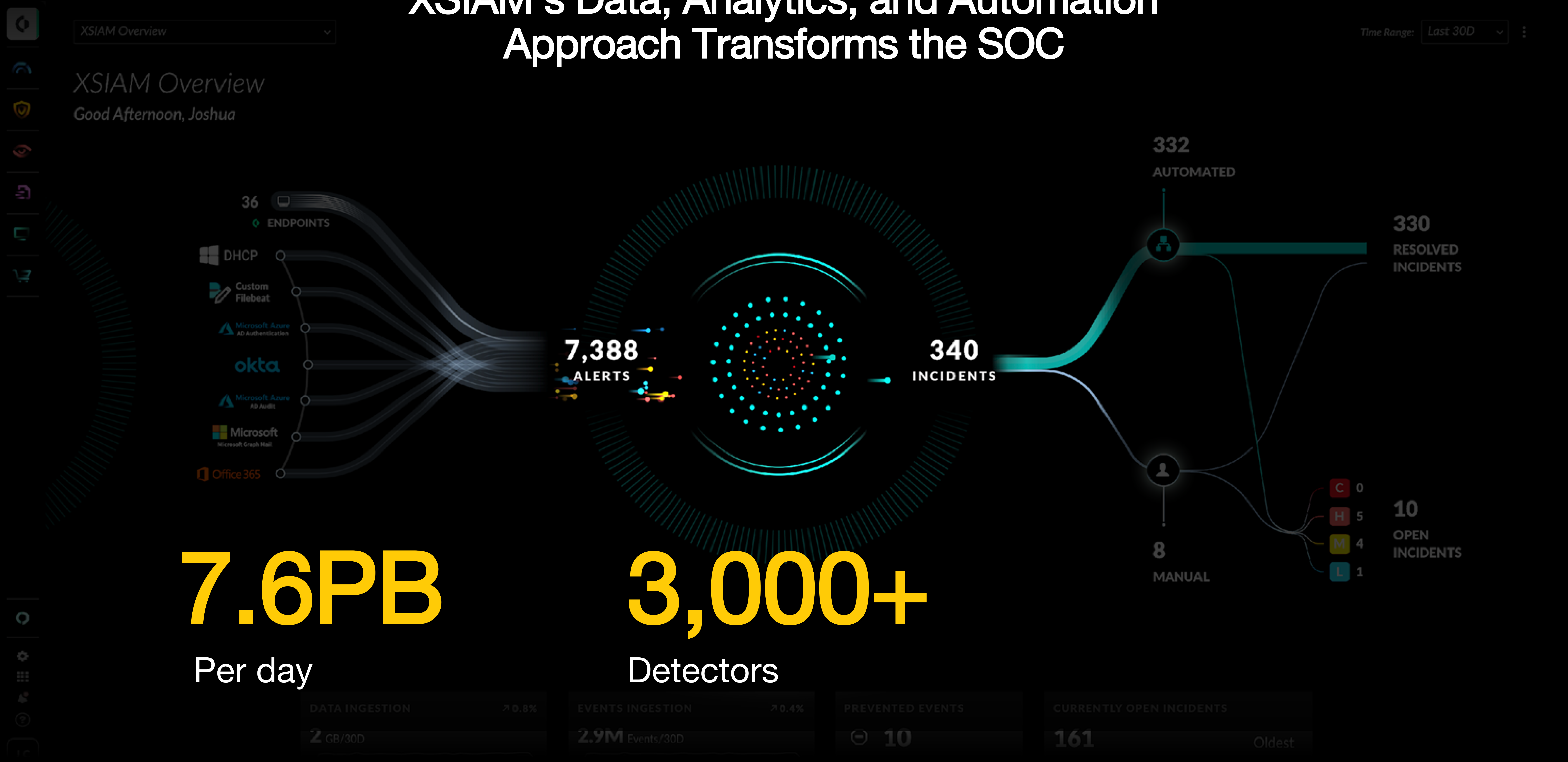
7.6PB

Per day

Source: Internal Palo Alto Networks data

All sources: Internal Palo Alto Networks data

XSIAM's Data, Analytics, and Automation Approach Transforms the SOC



7.6PB

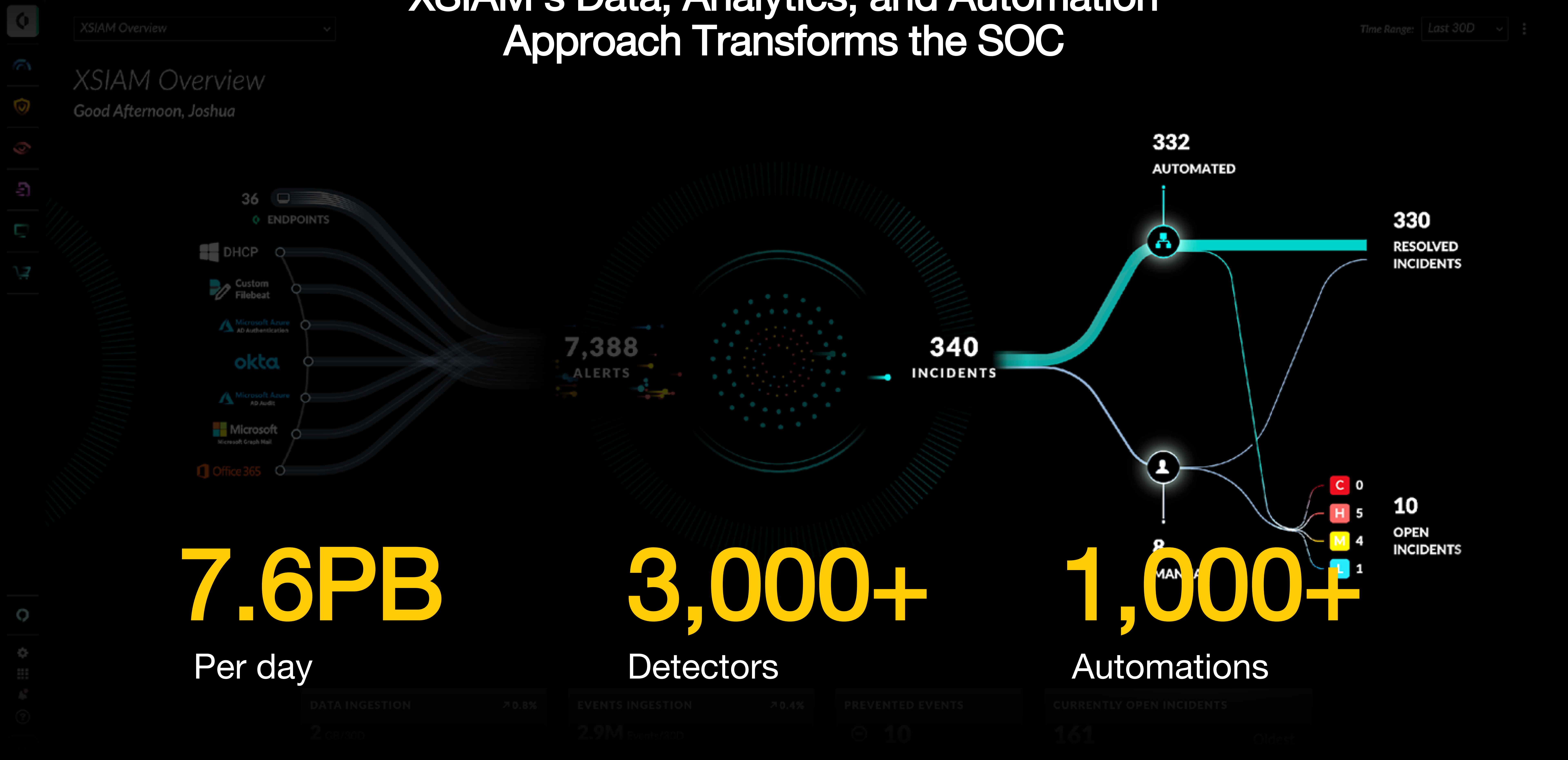
Per day

3,000+

Detectors

All sources: Internal Palo Alto Networks data

XSIAM's Data, Analytics, and Automation Approach Transforms the SOC



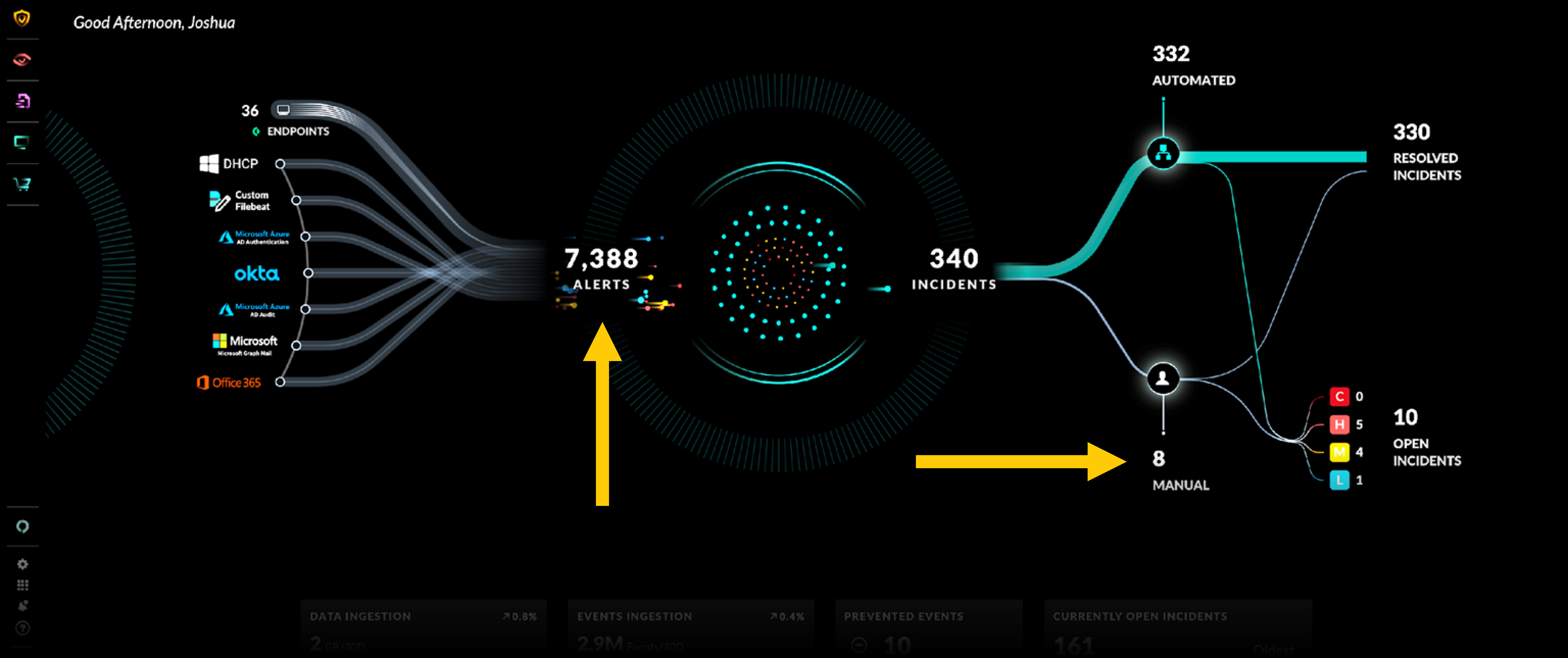
7.6PB
Per day

3,000+
Detectors

1,000+
Automations

All sources: Internal Palo Alto Networks data

XSIAM's Data, Analytics, and Automation Approach Transforms the SOC



DATA INGESTION ↗0.8%
2 GB/30D

EVENTS INGESTION ↗0.4%
2.9M Events/30D

PREVENTED EVENTS
10

CURRENTLY OPEN INCIDENTS
161 Oldest

Precision AI

We're Ready for the AI Fight

STRATA™

ZERO TRUST PLATFORM

Inspect connections and block attacks with Precision AI

ADV TP | ADV URL | ADV WF | ADV DNS

DLP | GP | NG CASB | IoT

PRISMA® CLOUD

CODE TO CLOUD PLATFORM

Identify and remediate cloud security issues at scale with Precision AI

CSPM | CIEM | VM-Series

DPSM | CWP | WAAS

CORTEX®

AI-DRIVEN SOC PLATFORM

Real-time detection, investigation, and remediation with Precision AI

SIEM | EDR | SOAR | NTA

ASM | ITDR | TIM | CDR

Thank You

paloaltonetworks.com