Outpacing the Adversary

Securing AI Innovation, Before It's Too Late

Haider Pasha
Chief Security Officer
EMEA & LATAM

Does your organization use AI today (Applications, Models, or Datasets)?

A We are using it today

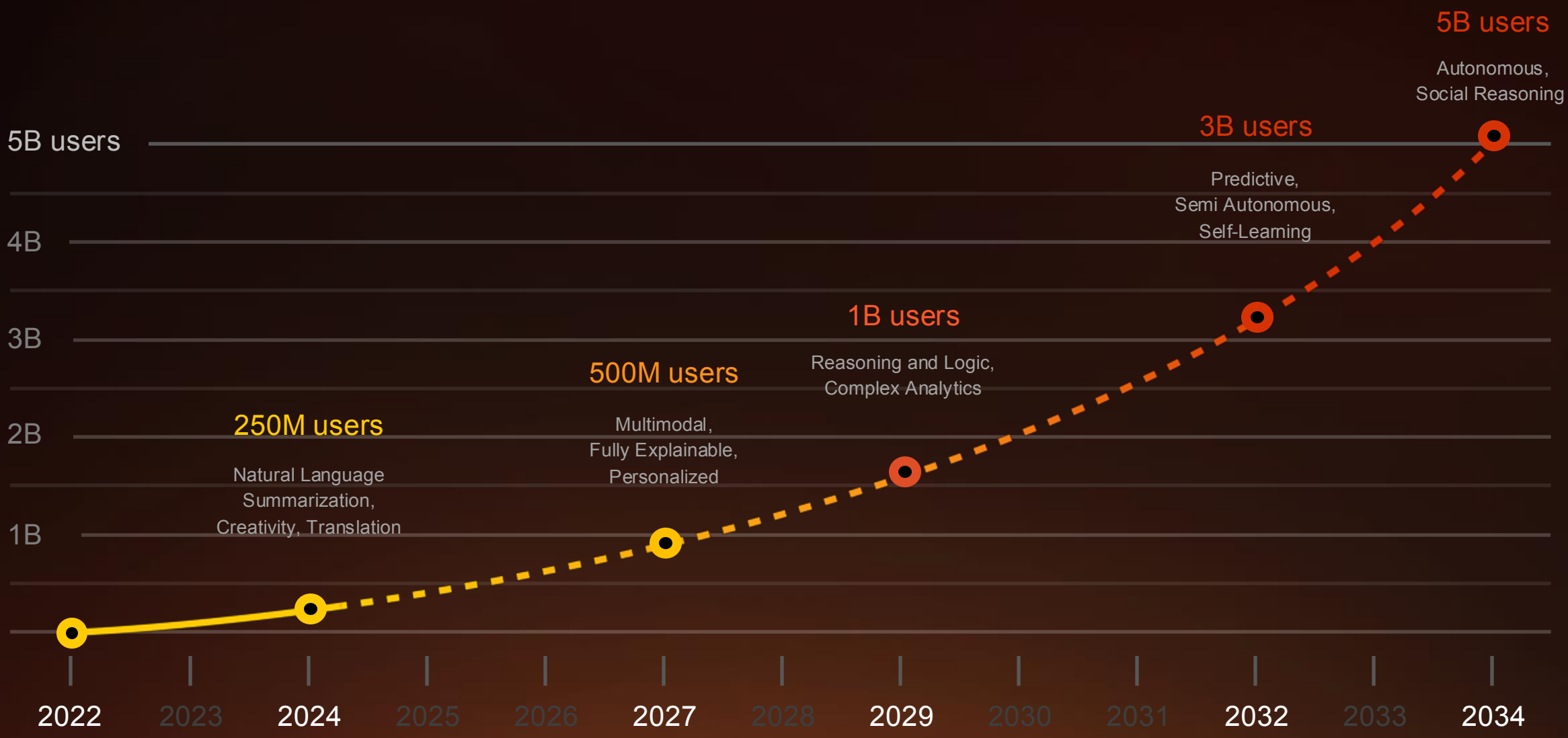
B Plan to Use it within 12 Months

C Considering to use it longer-term

D No Plans to use AI

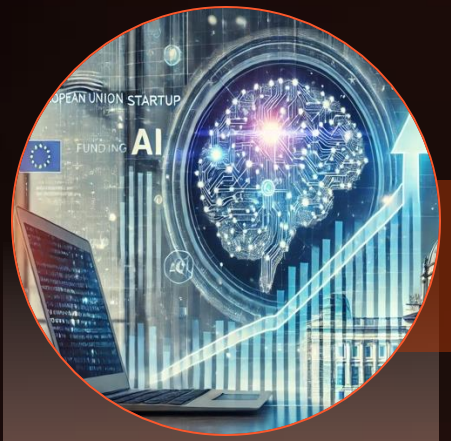
paloalto NETWORKS

We Are Just at the Start of the AI Journey



paloalto NETWORKS

The EU is Leading AI Innovation



$1.9Bn

Total Funding Created by EU AI Startups in 2024

500+ AI Startups and 8 Unicorns

250k

Size of AI Workforce in the EU

20% Higher Salaries for AI Workers

€30Mil

Fines for Non-compliance to the AI Act

70% of High Risk AI Systems Requiring Human Oversight

$1.8tn

Projected AI Market Size in the EU by 2030

Representing 9.5% of EU's Economy

paloalto NETWORKS

What do you find to be the biggest obstacle to AI innovation for your organization?

A. Budget Constraints

B. Complexity of legacy systems

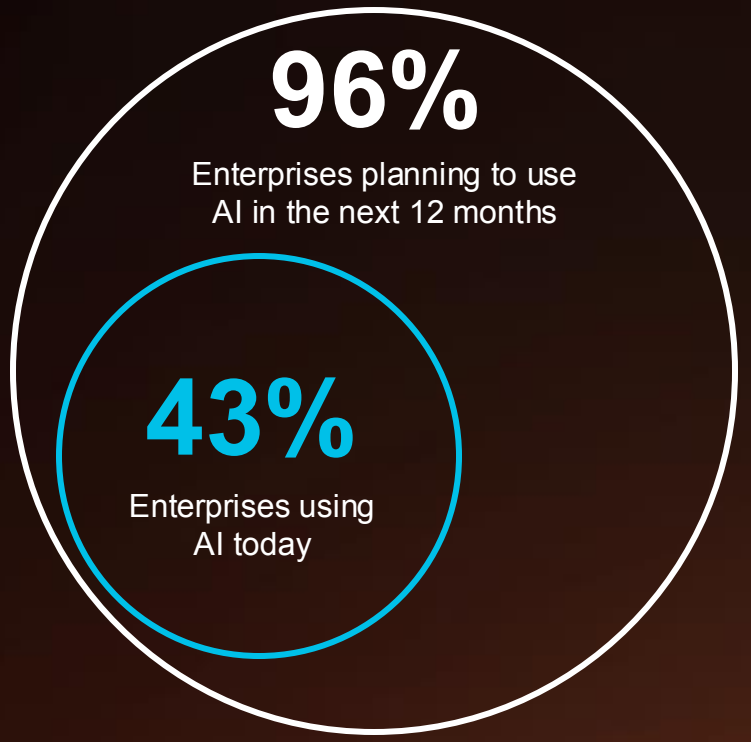
C. Lack of skilled personnel

D. Difficulty in balancing security & agility

paloalto NETWORKS

AI Projects Bring New Risks For Businesses

AI will be ubiquitous



And will require a new stack with a new set of challenges

TYPICAL LARGE ENTERPRISE

AI Applications

100s of sanctioned AI apps

AI Model Infrastructure

1000s of LLM, SLMs, ML scripts

AI Datasets

10s of PB of training & vector data

MILLIONS of prompts annually

50%
of employees using AI do it without permission

80%
of public models can be jailbroken

100+
malicious models available in the wild

Sources: AI will be ubiquitous (EY Reimagining Industry Futures Study 2024, Lenovo Global CIO Report 2024), Typical Large Enterprise (Salesforce survey of IT leaders July 2023, Estimate of prompts based on typical large enterprise size and expected AI app usage per employee, Qumolo blog on data usage by Enterprises July 2020), 50% of Employees using AI do it without permission (Salesforce Generative AI Snapshot Research Series), 80% of public Models can be Jailbroken (SCMedia Article July 28 2023, Research paper: Universal and Transferable Adversarial Attacks on Aligned Language Models July 2023), 100+Malicious Models available in the wild (Jfrog Blog Feb 27 2024).

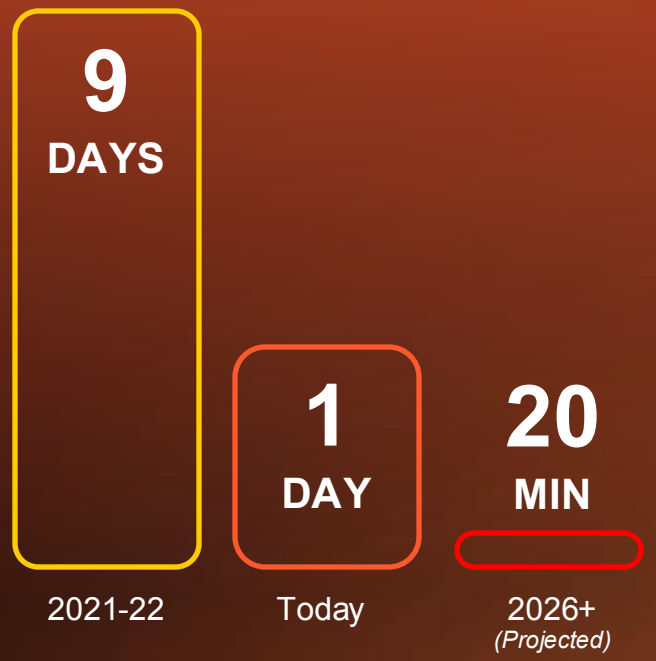
paloalto NETWORKS

AI is Turbocharging the Speed and Scale of Cyber Attacks

Build Ransomware

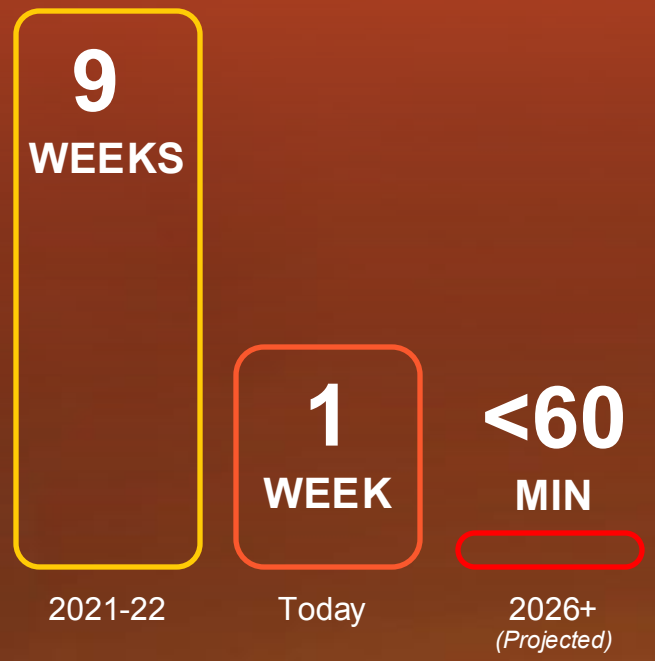
$2B impact from attack on a US health insurer in 2024

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:
1. 56% increase in exploited Zero Days in 2023 (Year-on-Year increase based on Google Cloud Blog March 26 2024),
2. 73% increase in Ransomware attacks in 2023 (SANS Blog Jan 15 2024),
3. 78% increase in data breaches and leaks in 2023 (WSJ Article March 15 2024),
4. Most companies need >2-3 days to resolve an incident (XSIAM customer interviews and XSIAM product telemetry for customers)

paloalto NETWORKS

Given the pace of innovation in cybersecurity, threat actors are adopting AI unlike anything we have seen before.

CYBERSCOOP

Cyber firm KnowBe4 hired a fake IT worker from North Korea

The security awareness training company said in a blog post that the software engineer used stolen U.S. credentials and an AI-enhanced photo.

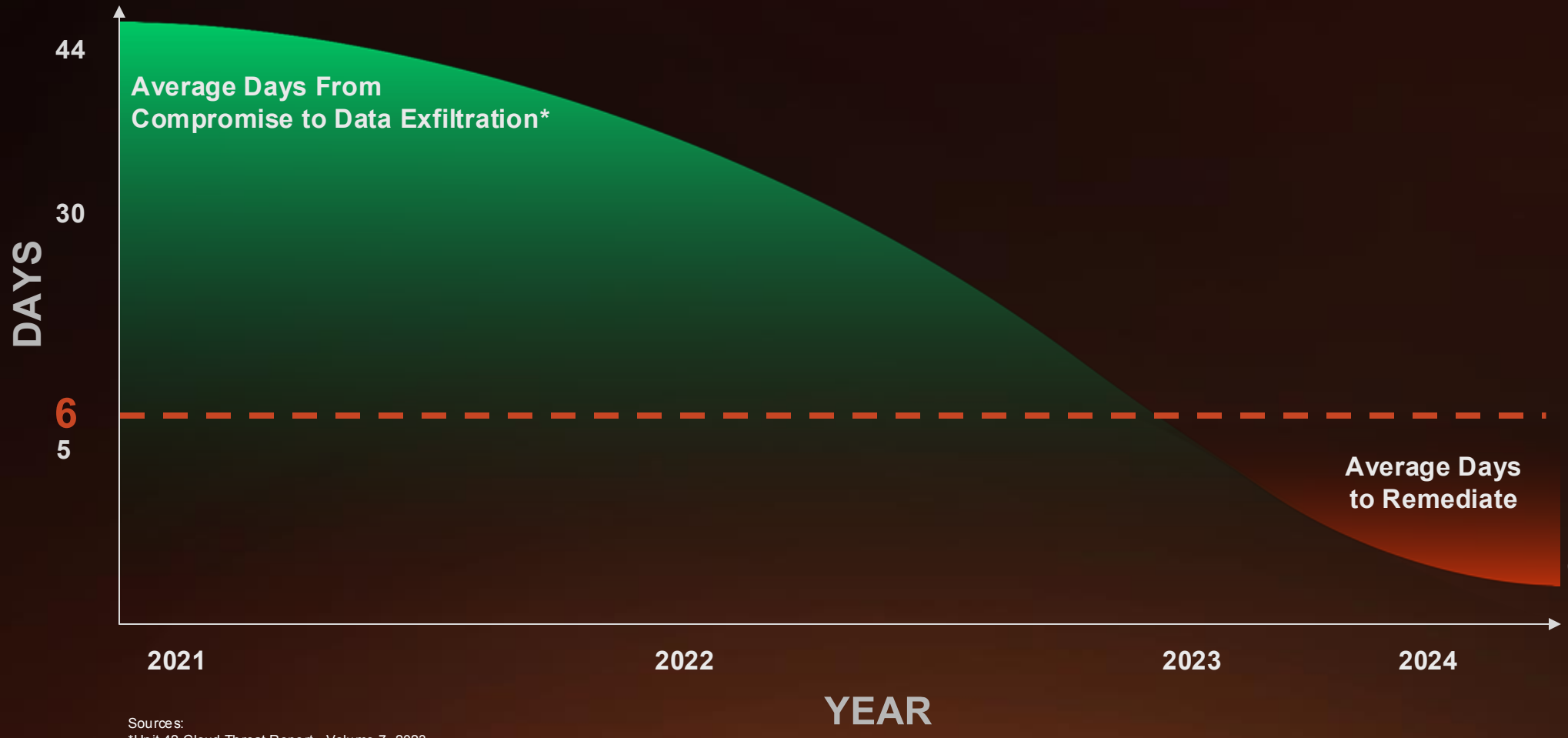
BY MATT BRACKEN • JULY 24, 2024

The original stock picture (left) and an AI fake (right) used by a North Korean threat actor who posed as a U.S.-based software engineer and was hired by the cyber firm KnowBe4. (Photo credit: KnowBe4)

https://cyberscoop.com/cyber-firm-knowbe4-hired-a-fake-it-worker-from-north-korea/

paloalto NETWORKS

The Average Organization Can No Longer Stop a Breach



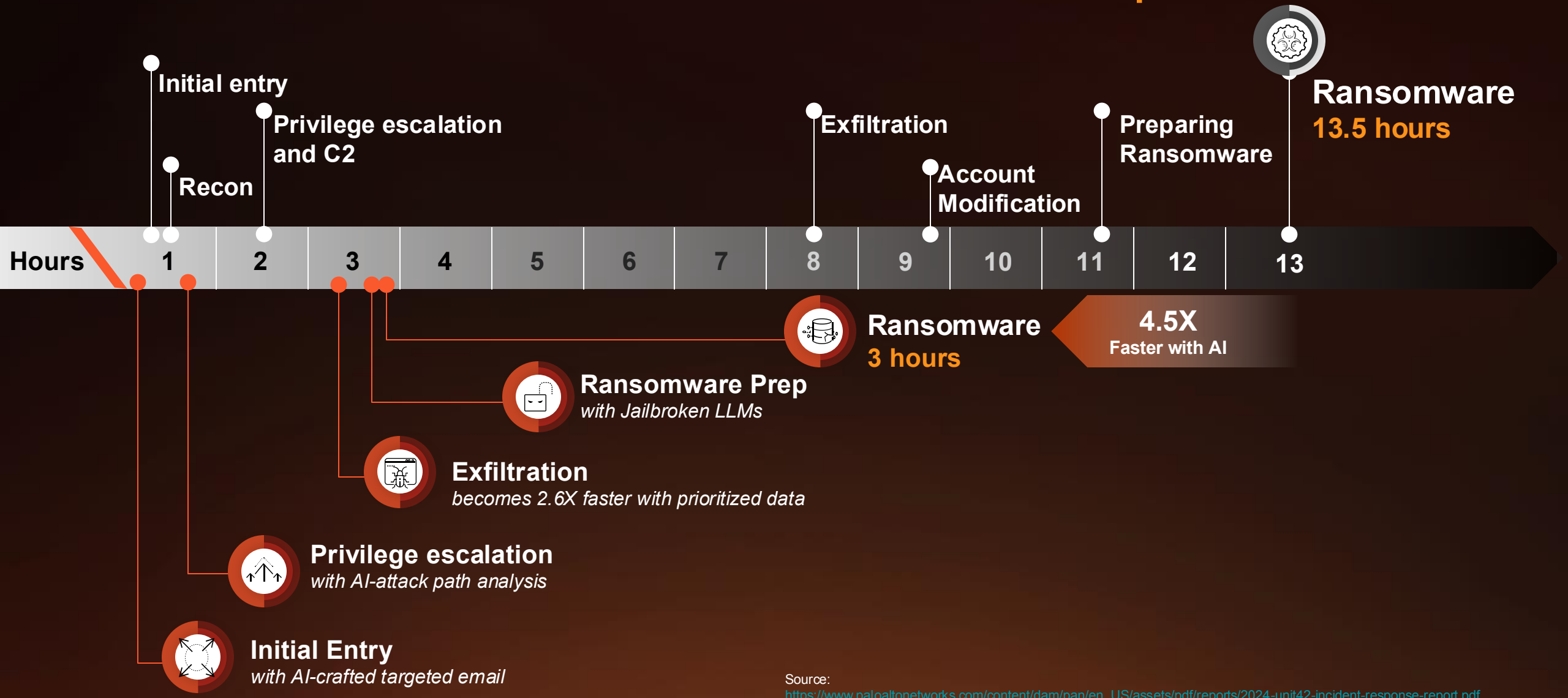
$4.45M
Average cost of a data breach**

Sources:
*Unit 42 Cloud Threat Report - Volume 7, 2023
**Ponemon Institute, Cost Of A Data Breach 2023

paloalto NETWORKS

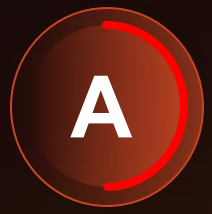
Real-World Attack Analysis

Unit 42 Casefile: ‘Black Basta’ Attack Group



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

How would you rate your organization's readiness to defend against AI-driven cyberattacks?



Well Prepared

Somewhat Prepared

Not Prepared

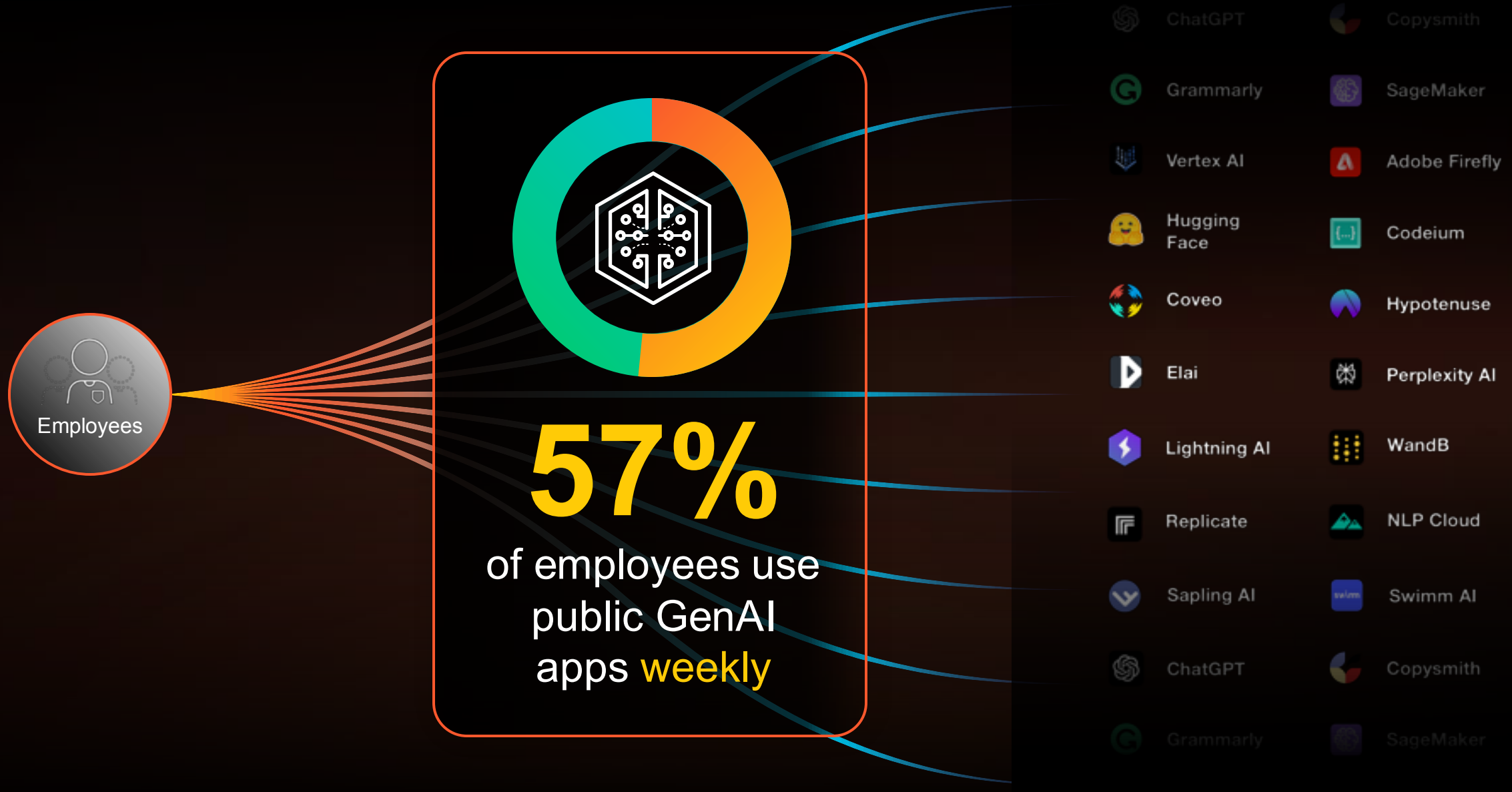
Not Sure

paloalto NETWORKS

AI Use-Cases

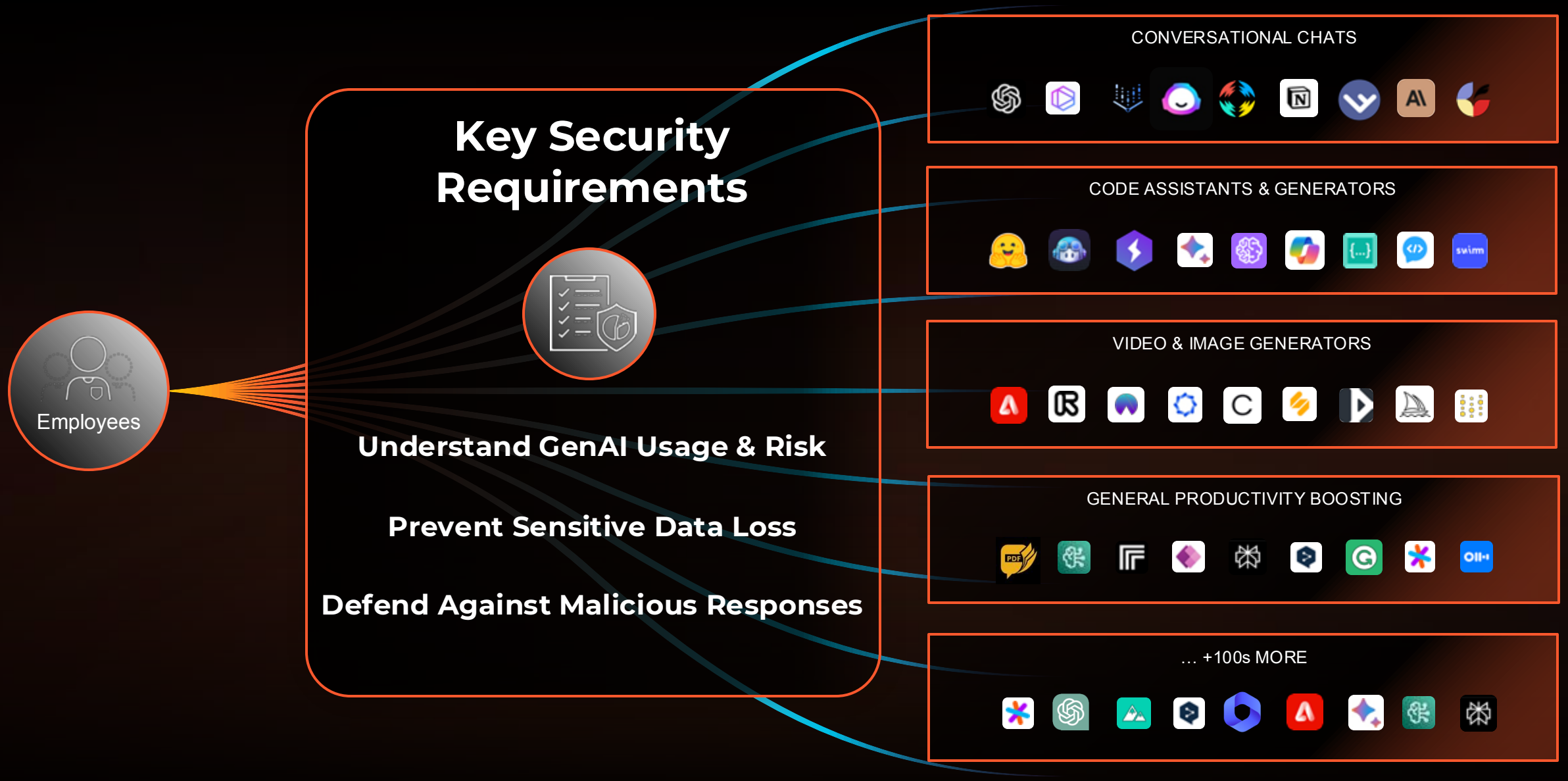
Employees Using GenAI Applications

Building Our Own AI Applications



Source: ZDNet, Feb. 2024

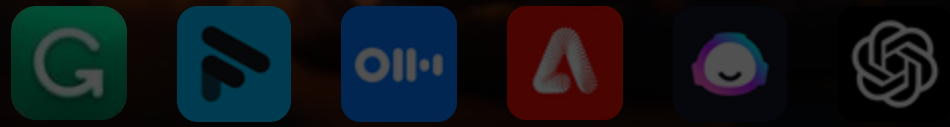
paloalto NETWORKS



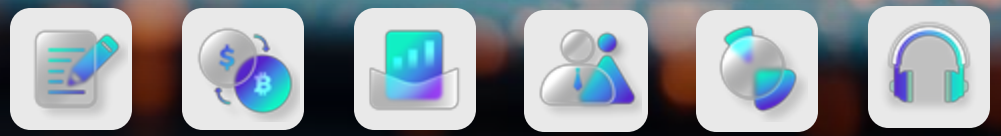
paloalto NETWORKS

AI Use-Cases

Employees Using GenAI Applications

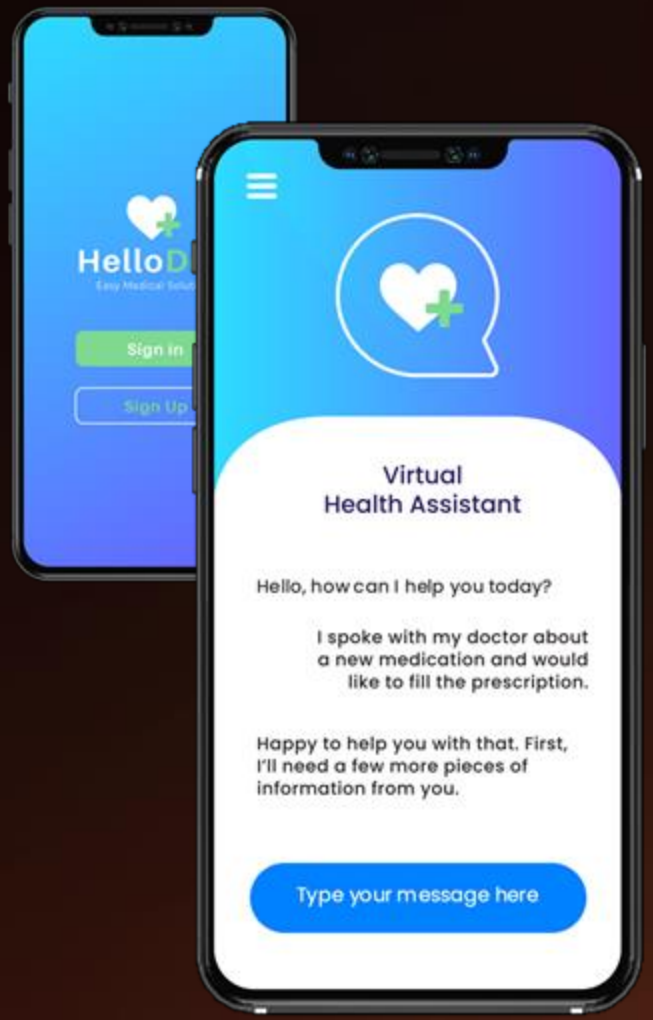


Building Our Own AI Applications



paloalto NETWORKS

Enterprise AI Applications Use a Specialized Tech Stack



AI Infrastructure

- Insecure Prompt Templates
- Corrupt AI/ML Libraries

AI Models

- Model Vulnerabilities
- Model Trained on Proprietary Data
- Model Misconfig

47%

Executives worry that their companies' own adoption of generative AI will lead to new security pitfalls

PWC 2023 Trust Survey, 500 business execs

Datasets

- Publicly Writable Dataset
- Sensitive Data Exposure
- Obscure Data Lineage

Plugins & Agents

- Excessive Permissions

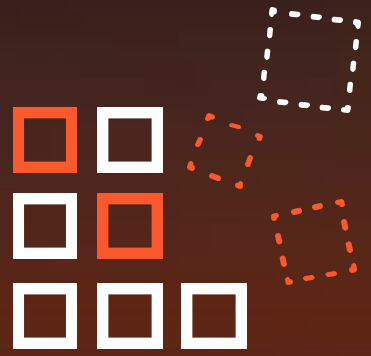
How can organizations Secure their AI Innovations?

1

AI Innovation needs to be secure

...by design

2



Organizations need to change their approach

...to platformization

3

Security Platforms must embed AI to deliver

...real time and autonomous outcomes

paloalto NETWORKS

1

Securing AI by Design

Track and monitor AI usage for every employee

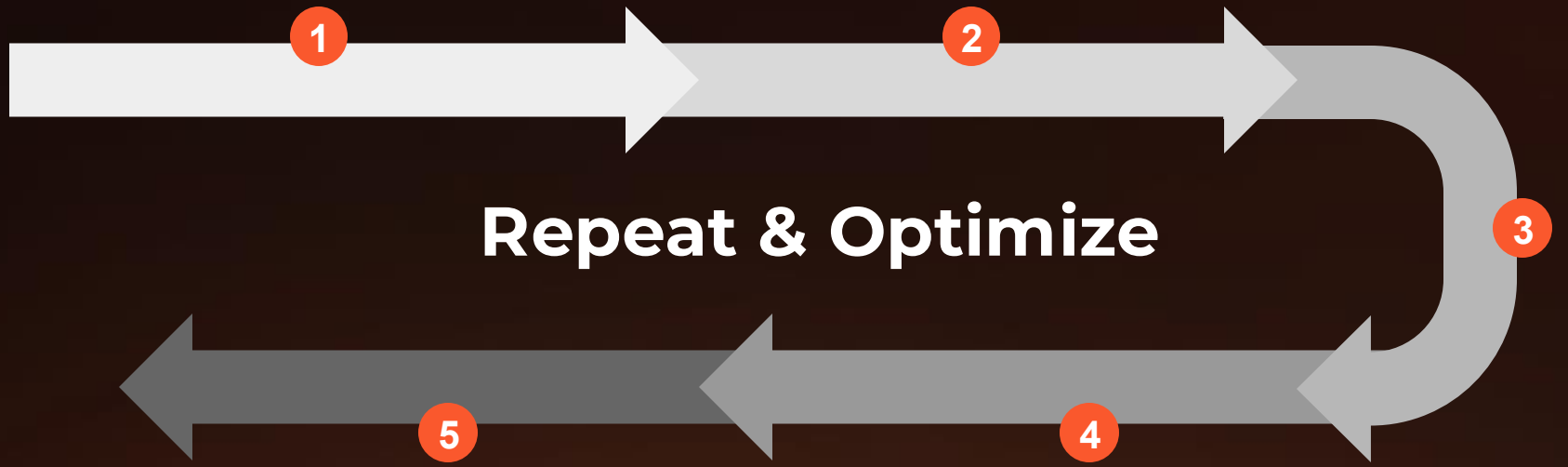
Secure every step of AI app development lifecycle and supply chain

Protect AI data from unauthorized access and leakage at all times

Delivered as an Extension of Existing Cybersecurity Solutions

paloalto NETWORKS

Secure AI Requires Specific Visibility & Controls



Establish visibility into AI activity
Leverage endpoint, network, and cloud data to create inventory of AI Models and Plug-ins

Reduce the Exposure
Block AI Models and Plug-ins that are not approved

Secure CI/CD
Uniform Security by only deploying AI Models within Secure CI/CD process

Assess AI Risk
Scan each AI Model and infra for vulnerabilities, configurations and risks using AI-SPM. Monitor Malicious input/outputs of ML Models

Implement AI DLP & SOC
Establish playbooks to automate incident remediation

paloalto NETWORKS

Example: How we Secure AI by Design

AI Access Security

Full real-time visibility of AI usage

Comprehensive data protection

Access control at the fingertips

AI Runtime Security

AI Security Posture Management

Full discoverability of your entire AI ecosystem

Real-time assessment & identification

AI App, Data, & Model Protection

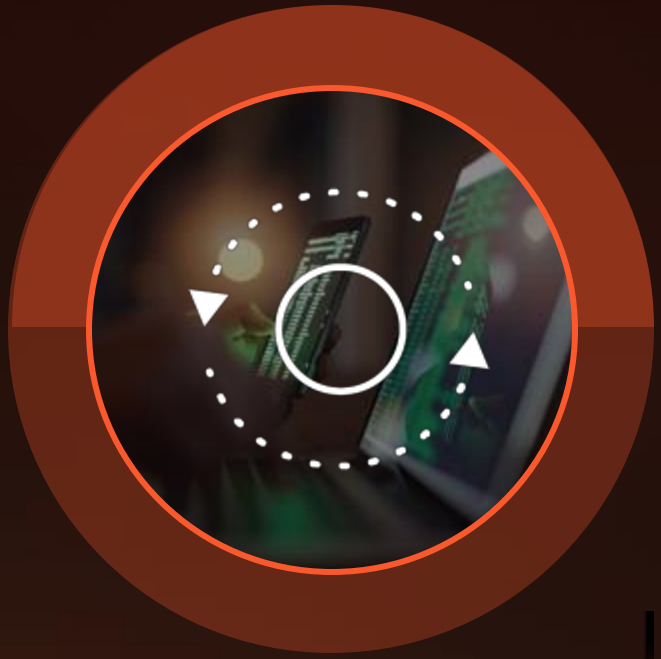
paloalto NETWORKS

2

Platforms are Built on Three Core Principles

Native Integration

Innovative Tech

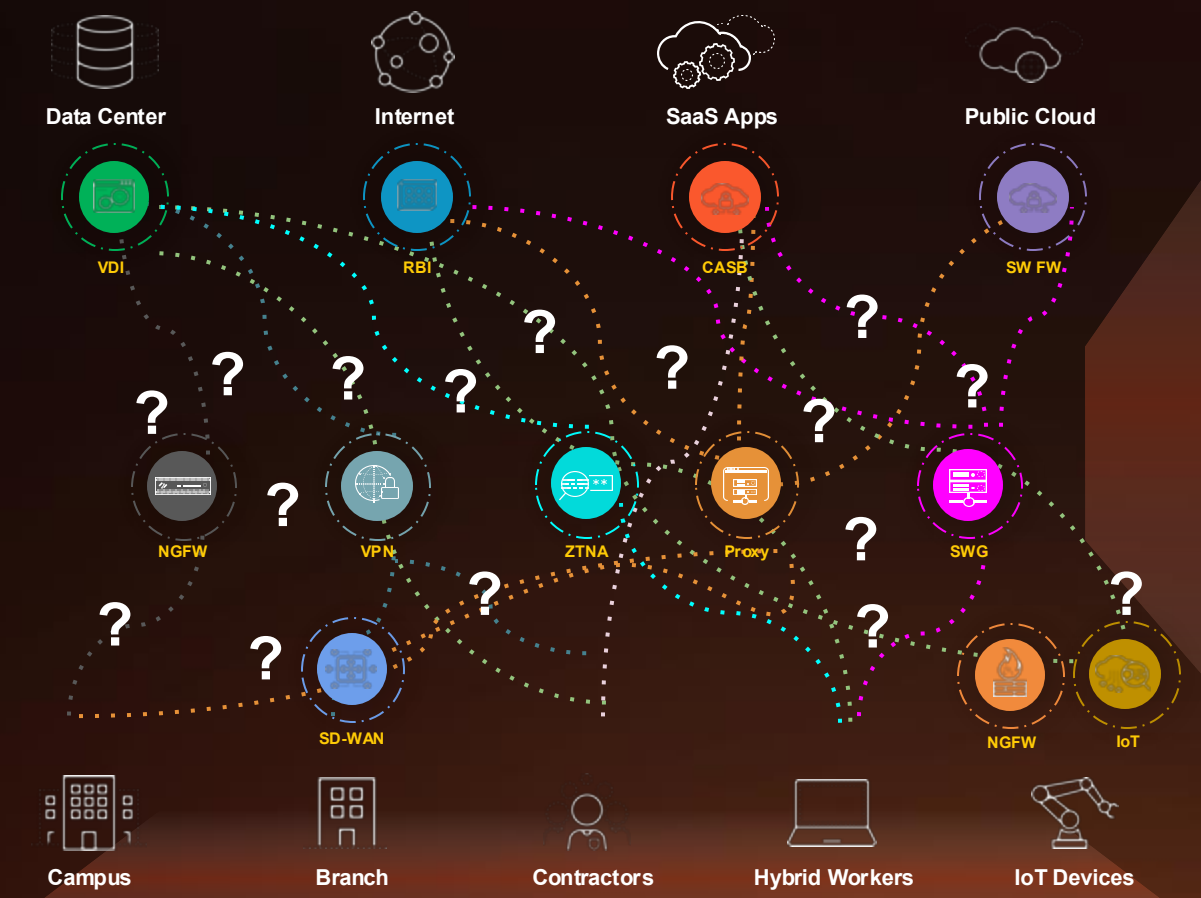


The Right Data

Lowered TCO with Improved Risk Profile

paloalto NETWORKS

Increased Organizational Interconnectedness is Leading to Worsening Impacts, Affecting Innovation



Where would you put…

Security for Gen AI app access?

AI app development & supply chain Security?

Runtime Security for custom AI apps?

paloalto NETWORKS

Is your organization considering consolidating cybersecurity tools in the next 12-18 months?

A Yes, we have started

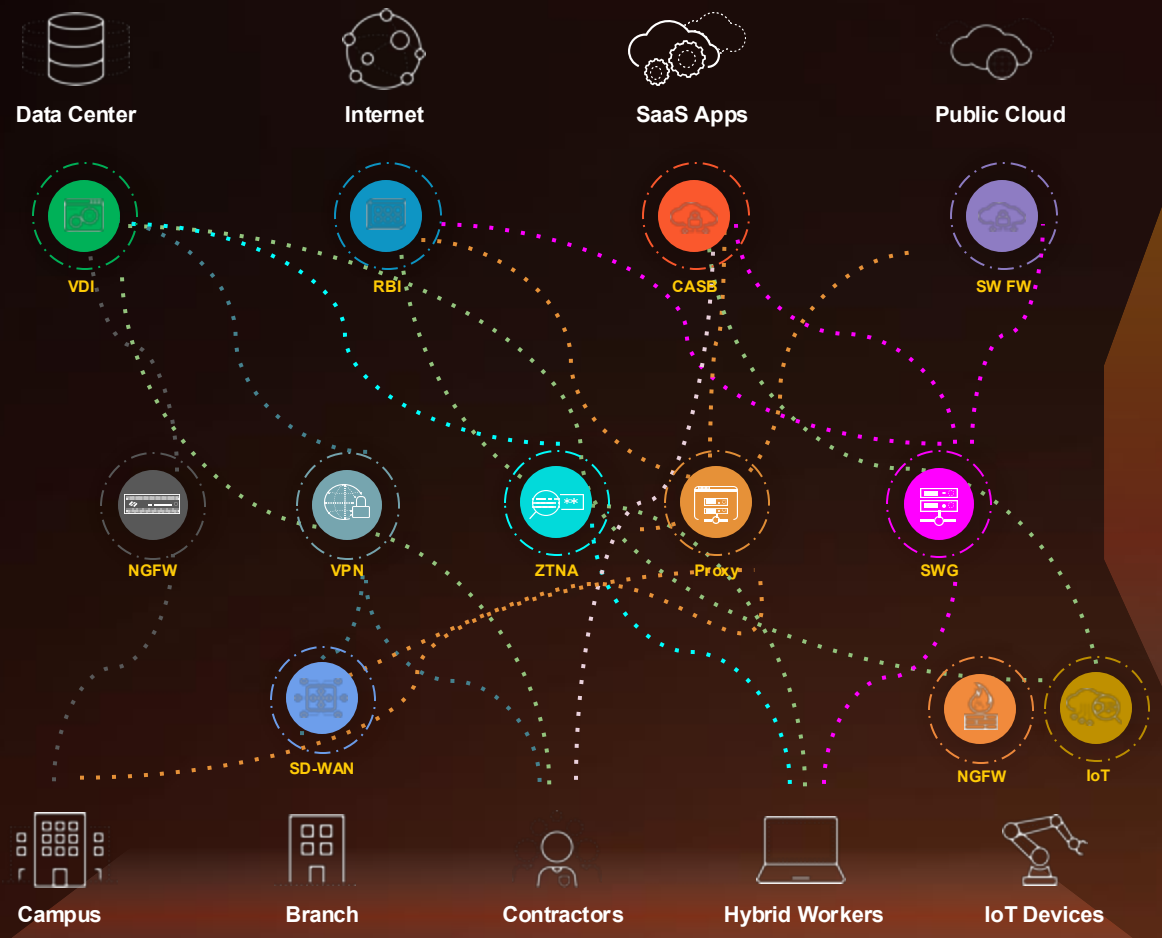
B We are planning to, but not started yet

C No, not considering yet

D Not sure

Example: Comprehensive AI Adoption via a Platform

Months or Years to Deploy Across the Enterprise



Simple Enterprise-Wide Security Activation

paloalto NETWORKS

3 Embed AI to Achieve Real-Time & Autonomous Outcomes

The difference between 90% accuracy and inaction
vs. 100% confidence and real-time response

paloalto NETWORKS

Precision AI | Embedded Across our Platforms

STRATA

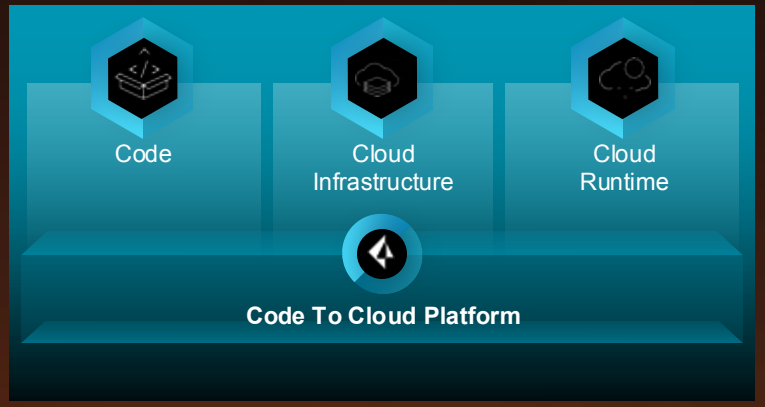
ZERO TRUST PLATFORM

Inspect connections and block attacks with Precision AI

PRISMA CLOUD

CODE TO CLOUD PLATFORM

Identify and remediate cloud security issues at scale with Precision AI



CORTEX

AI-DRIVEN SOC PLATFORM

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

paloalto NETWORKS

Example: Our Approach to SOC Platformization

Fighting AI with Precision AI

11.3B Attacks blocked inline daily

2.3M New and unique attacks identified daily

>7.6PB of data ingested

4.6B New events analyzed daily by 4400+ ML Models

Consolidate with Proven TCO Benefits

Before	SOC Platformization	After
Too Many Alerts	-$2M per year Operating Optimizations	Cortex XSIAM
5 SOC Vendors	-$2.5M per year Risk Reduction	Full Coverage
Missing Coverage	-$3.5M per year Consolidation Benefits	Faster Response
$17M per year		Proactive SOC
		$9M per year

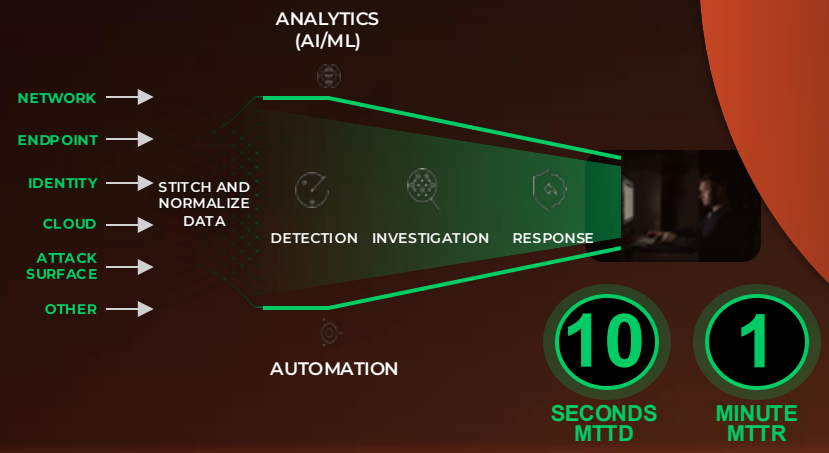
Better Cybersecurity Outcomes

Real-Time & Autonomous

Cost Effective

Native Integration

Innovative Leadership



Our Latest Innovations

- AI Access Sec
- AI Runtime Sec
- CDR
- Enterprise Browser
- DSPM
- App Accel
- ADV DNS
- AI SPM

Drive Simplicity Across Tech Stack

Validated by 24 Magic Quadrants & Waves

paloalto NETWORKS

Example: Our Approach to SOC Platformization

Fighting AI with Precision AI

INGESTED DATA (Per day) — 4x Data

INCIDENTS (Per day) — 65

INCIDENT CLOSE-OUT RATE — 100%

MTTR
14 mins to 2 hours

Consolidate with Proven TCO Benefits

Before	SOC Platformization	After
Too Many Alerts	-$2M per year Operating Optimizations	Cortex XSIAM
5 SOC Vendors	-$2.5M per year Risk Reduction	Full Coverage
Missing Coverage	-$3.5M per year Consolidation Benefits	Faster Response
$17M per year		Proactive SOC
		$9M per year

Real-Time & Autonomous

Cost Effective

Better Cybersecurity Outcomes

Native Integration

Innovative Leadership

10 SECONDS MTTD

1 MINUTE MTTR

Our Latest Innovations

- AI Access Sec
- AI Runtime Sec
- CDR
- Enterprise Browser
- DSPM
- App Accel
- ADV DNS
- AI SPM

Drive Simplicity Across Tech Stack

Validated by 24 Magic Quadrants & Waves

paloalto NETWORKS

Call to Action: A CxO's Roadmap to Securing AI Innovation

Understand Business Context for AI

Exec support, Specific Problem to Solve, Feasibility, Training for Skill-Set Development and Metrics to measure

Ensure AI Visibility & Employee Use

Sanctioned v Unsanctioned Apps, User Permissions, AI Risk Register

Protect AI Supply-Chain

Catalog and Secure … infrastructure, models, data and agents/plugins

Align to Regulations and Laws

Multiple Jurisdictions, Data Classification and Sovereignty, IP Considerations, Introduce Guardrails

Evolve company-wide AI policy

Develop a comprehensive AI policy, monitor, iterate, learn and update

paloalto NETWORKS

Thank You

paloaltonetworks.com