paloalto NETWORKS | Cybersecurity Partner of Choice

Secure AI By Design

WITH PALO ALTO NETWORKS

AI Is Quickly Becoming The Most Disruptive Technology Since Cloud

The A.I. Revolution Will Change Work. Nobody Agrees How.

The tally of how many jobs will be "affected by" world-changing technology is different depending on who you ask.

May 23, 2023 - Economy & Business

Elon Musk: AI will change human race 'a lot'

How unbelievably realistic fake images could take over the internet

AI image generations like DALL-E and Midjourney are getting better and better at fooling us.

By Sara Morrison I sara@vox.com I Mar 30, 2023, 6:30am EDT

Vox

Generative AI is poised to change everything. Is your company ready?

CNBC

Marc Andreessen - e/acc
@pmarca

AI is bringing a sudden rush of new young tech super geniuses out of woodwork. Makes me proud to be a technology brother.
💪💻

1:40 PM - Mar 13, 2023

Outcry Against AI Companies Grows Over Who Controls Intern's Content

Websites like Reddit and writers including James Patterson and Sarah Silverman demand compensation for work they suspect was used to train new artificial-intelligence technology

WSJ

AI Can Now Write Code That's Better Than Humans

Devin Coldewey
@techcrunch / 10:04 AM PST - February 2, 2022

THE SHIFT

How ChatGPT Kicked Off an A.I. Arms Race

Even inside the company, the chatbot's popularity has come as something of a shock.

Elon Musk
@elonmusk

Replying to @Scobleizer
Some of the AI art is incredible & it keeps getting better!

1:02 PM - Apr 2, 2023

TECH - ARTIFICIAL INTELLIGENCE

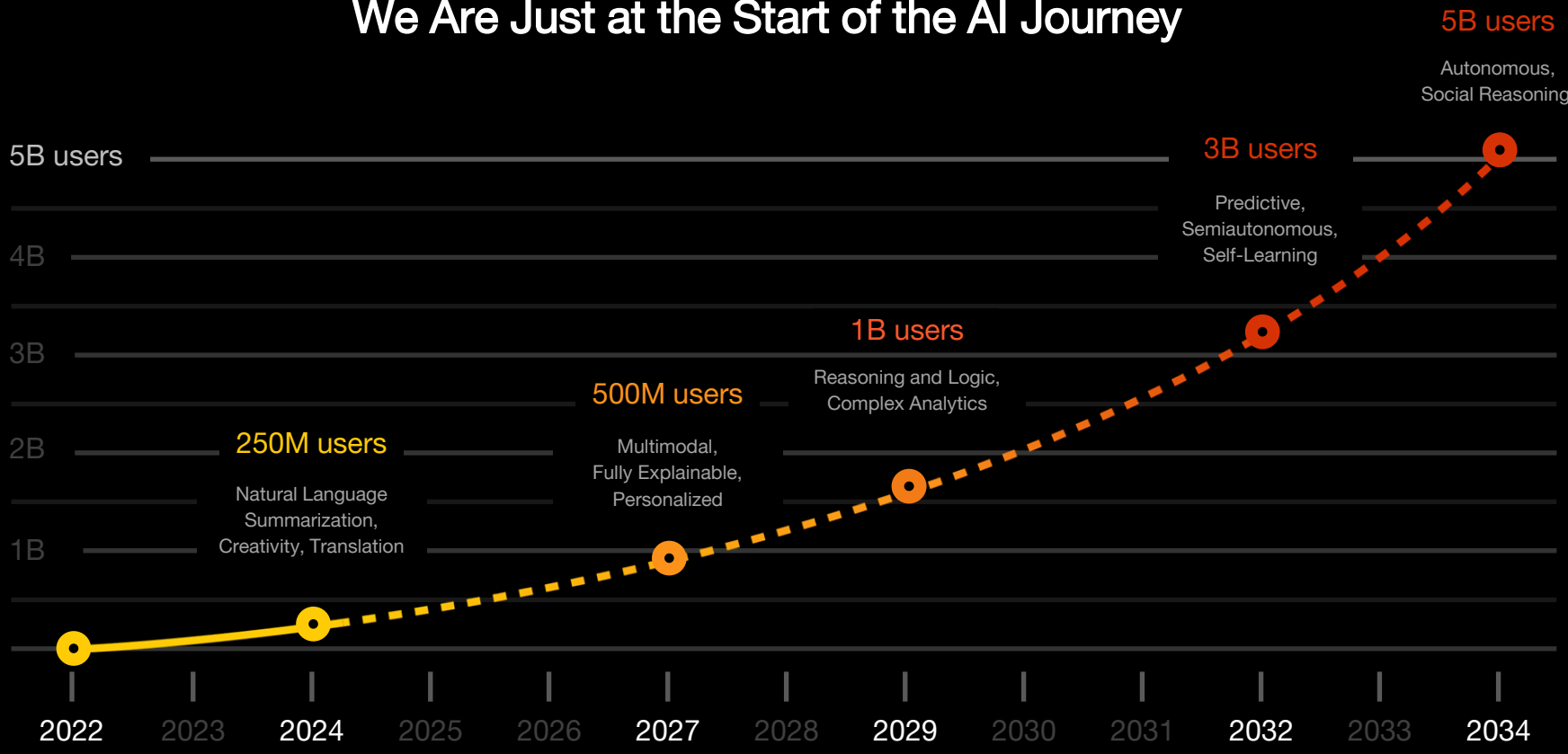
The AI Arms Race Is Changing Everything

TIME

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

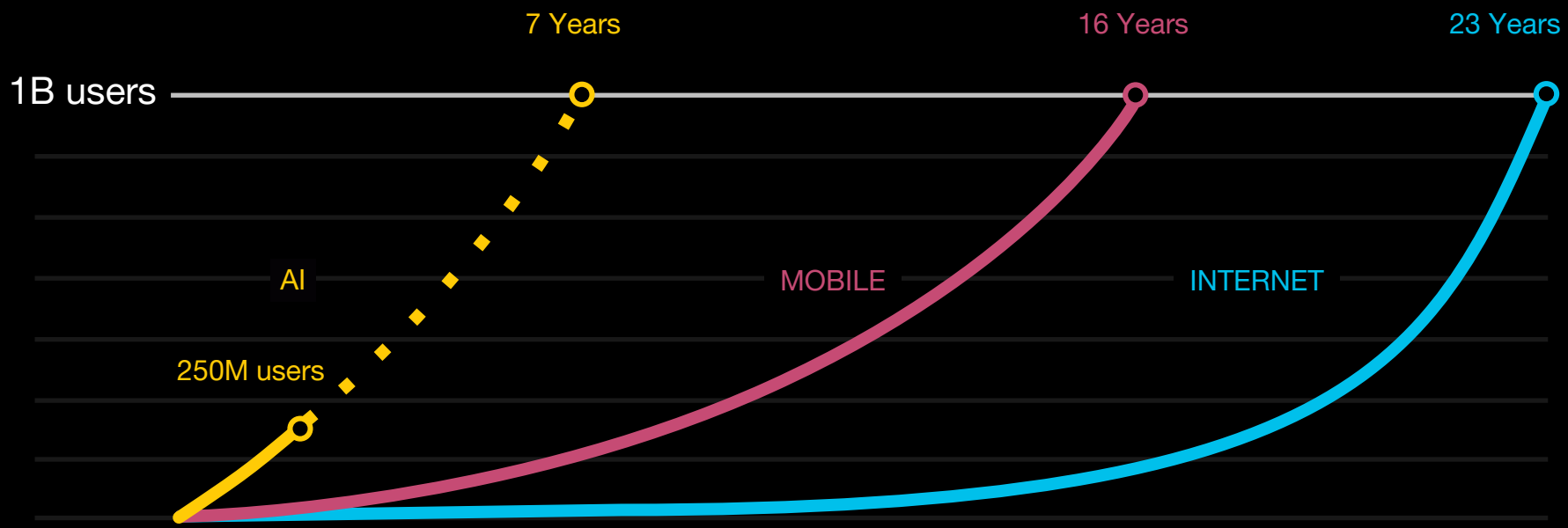
paloalto NETWORKS

We Are Just at the Start of the AI Journey



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

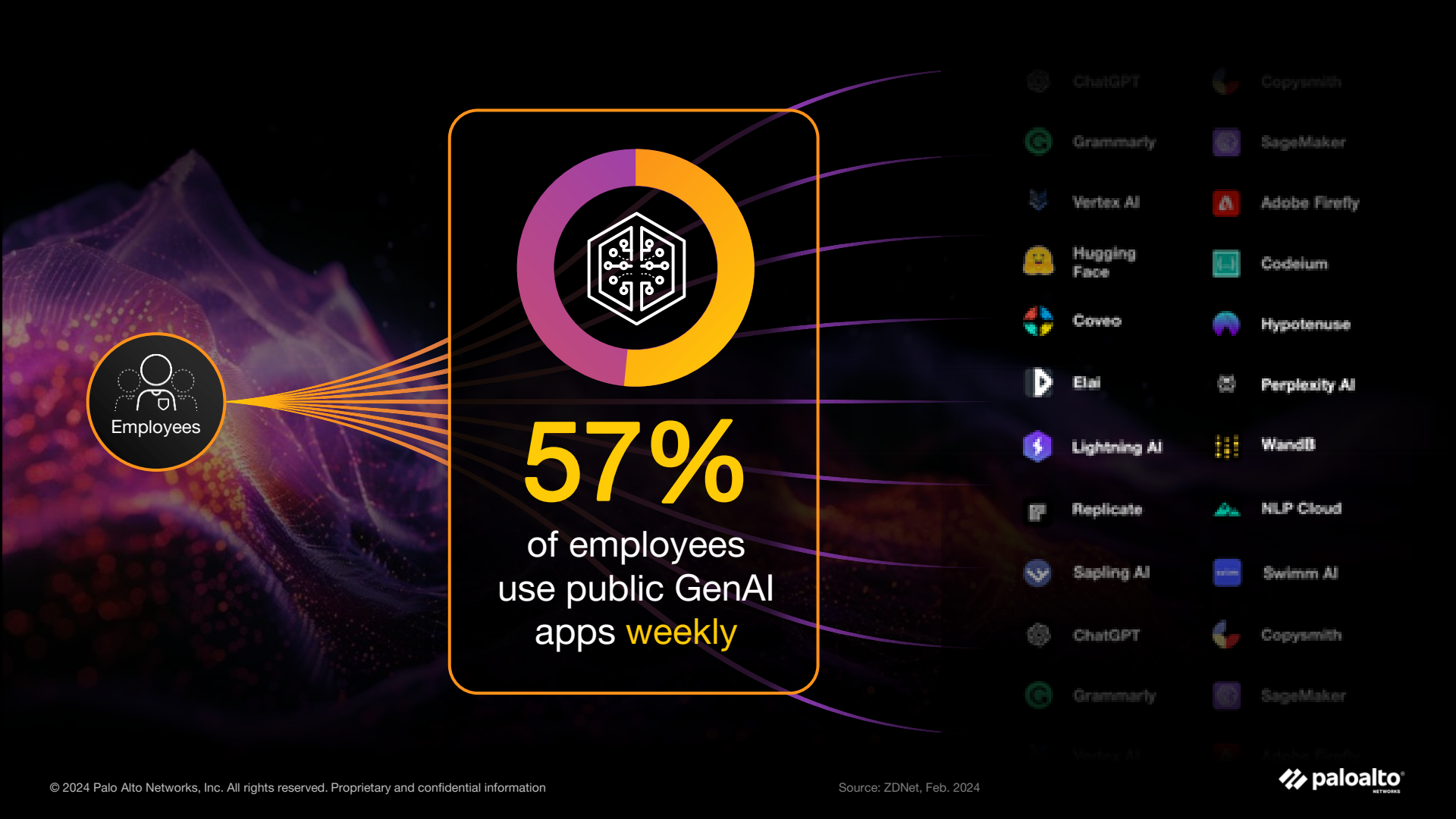
AI Is Already the Fastest-Growing Technology in Our History



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

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

paloalto NETWORKS



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

Source: ZDNet, Feb. 2024

paloalto NETWORKS

And Adversaries See the Same Promise in AI

Speed

Hours

From Compromise to Exfiltrate Data[1]

THE WALL STREET JOURNAL.

AI Is Generating Security Risks Faster Than Companies Can Keep Up

Scale

Ransomware

Volume to surge[2]

TechTarget

NCSC Says AI will Increase Ransomware, Cyber Threats

Scope

Prompt Injection

Generative AI's Biggest Flaw[3]

DARKREADING

Forget Deep Fakes or Phishing: Prompt Injection is GenAI's Biggest Problem

1. Unit 42 Cloud Threat Report - Volume 7, 2023, Unit 42 Engagement Experience
2. https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat
3. https://www.wired.com/story/generative-ai-prompt-injection-hacking/
4. https://owasp.org/www-project-top-10-for-large-language-model-applications/assets/PDF/OWASP-Top-10-for-LLMs-2023-v1_1.pdf

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

paloalto NETWORKS

AI Is Expanding the Horizons of What's Possible for Cyberthreats

If the SolarWinds attack used AI, victim count could have been 1,000s

Imagine it taking <4 hours from compromise to exfiltration

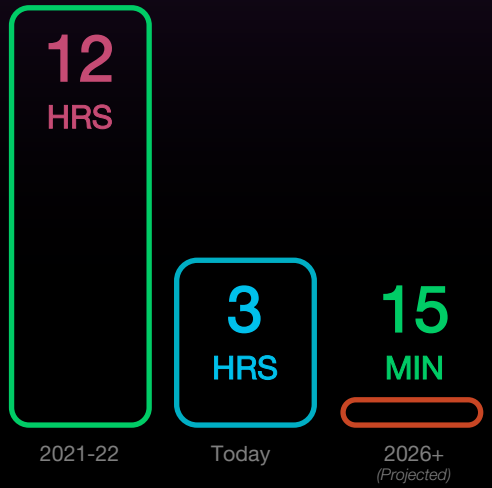
With AI, every attack could be a novel attack

Sources: Palo Alto Networks Unit 42 Research

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

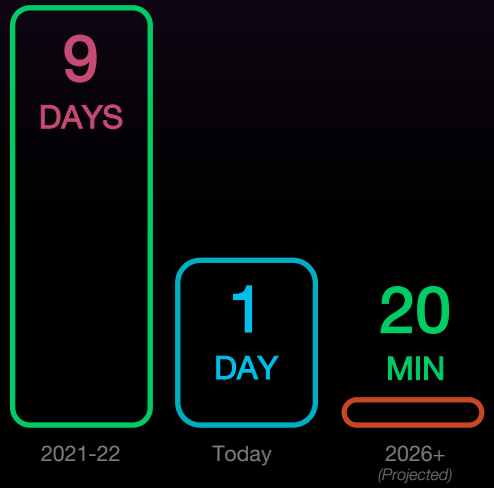
AI Is Turbocharging the Speed and Scale of Attacks

Build Ransomware



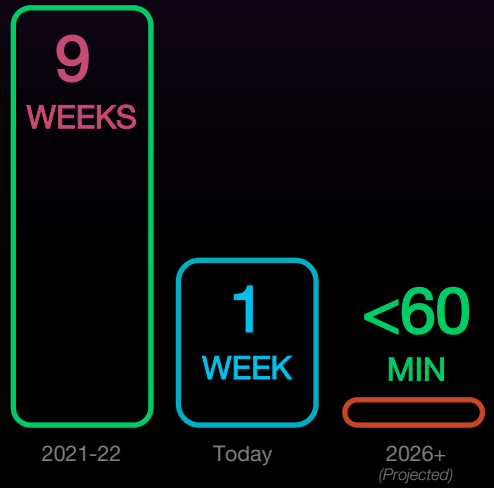
$2B impact from attack on a US health insurer in 2024

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)

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

We Are Ready to Help You Win the Fight

Embedding AI Across Your Security Stack

Securing AI by Design

Radically Simplifying Cybersecurity

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

paloalto NETWORKS

We Believe Enterprises Need to Secure AI by Design

Track and monitor AI usage for every employee

Secure every step of AI app development lifecycle and supply chain

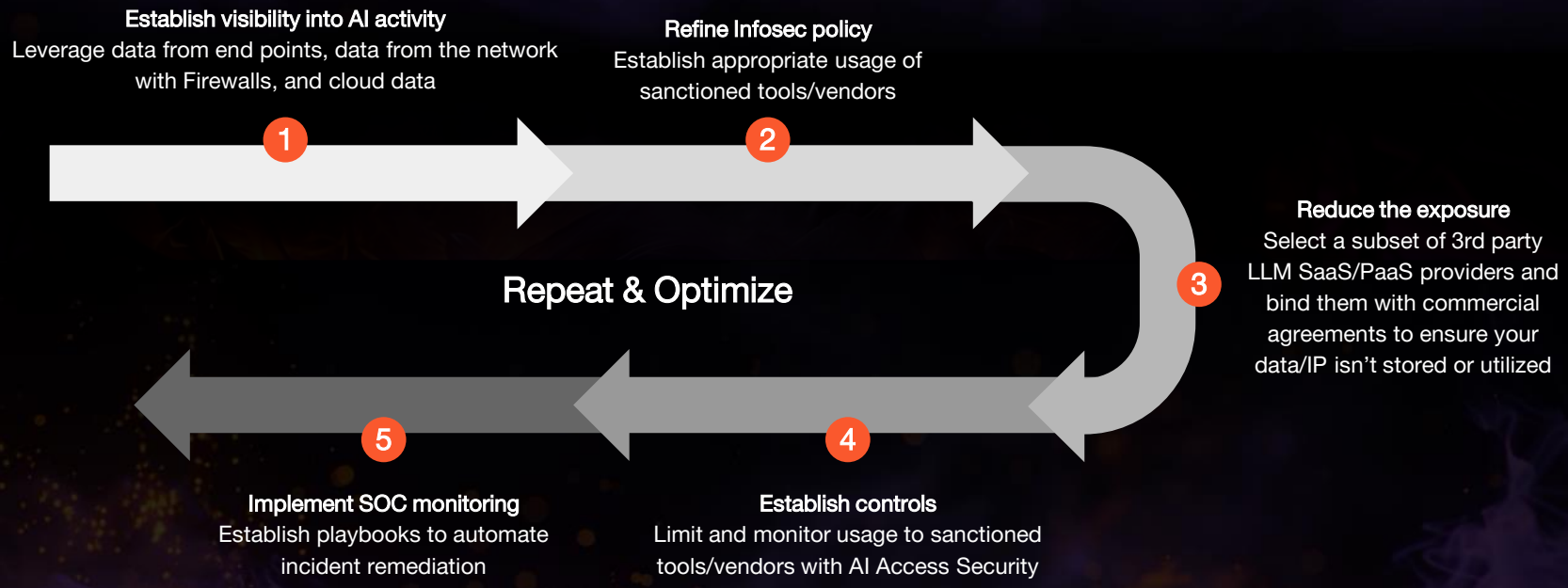
Protect AI data from unauthorized access and leakage at all times

Delivered as an extension of existing cybersecurity solutions

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

paloalto NETWORKS

Secure AI requires specific visibility and controls



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

To Secure AI by Design,
We have a comprehensive Set of Solutions

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

paloalto NETWORKS

AI Access Security to Enable Safe AI Adoption to Employees

Full real-time visibility of AI usage

View what AI apps are used and by whom

Comprehensive data protection

Scan what data, secrets & IP are shared

Access control at your fingertips

Block unsanctioned apps, apply infosec policies and protect data

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

paloalto NETWORKS

Securing Enterprise AI Applications

Automatically discover entire AI application ecosystem

AI Security Posture Management

Reduce AI supply chain and infrastructure security risk; identify data exposure

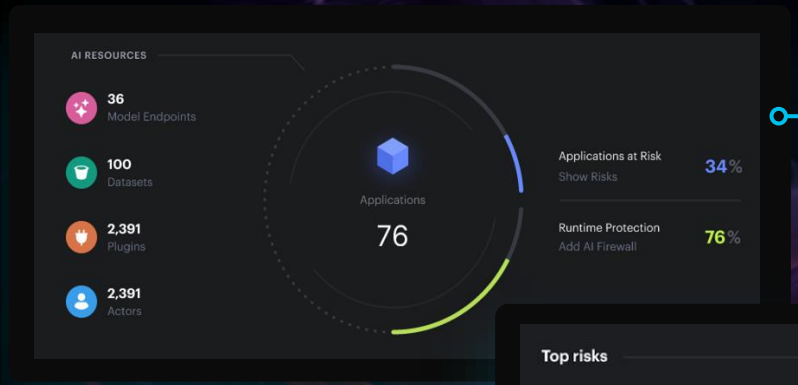
AI Runtime Security

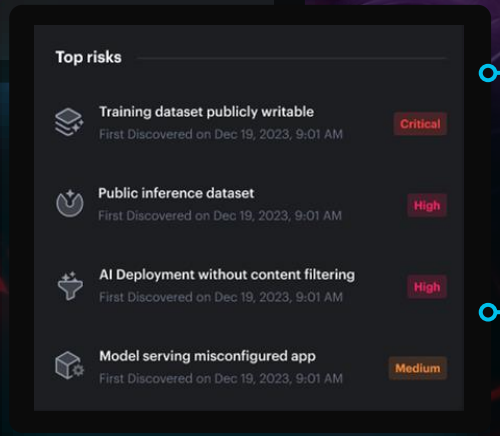
Protect enterprise AI applications, models, and data from AI and foundational threats in runtime

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

paloalto NETWORKS

AI-SPM to Protect AI Apps from Malicious Building Blocks





Full discoverability of your entire AI ecosystem

View AI models, infra, datasets, and agents

Real-time assessment & identification

Analyze risk continuously with extensive threat intelligence

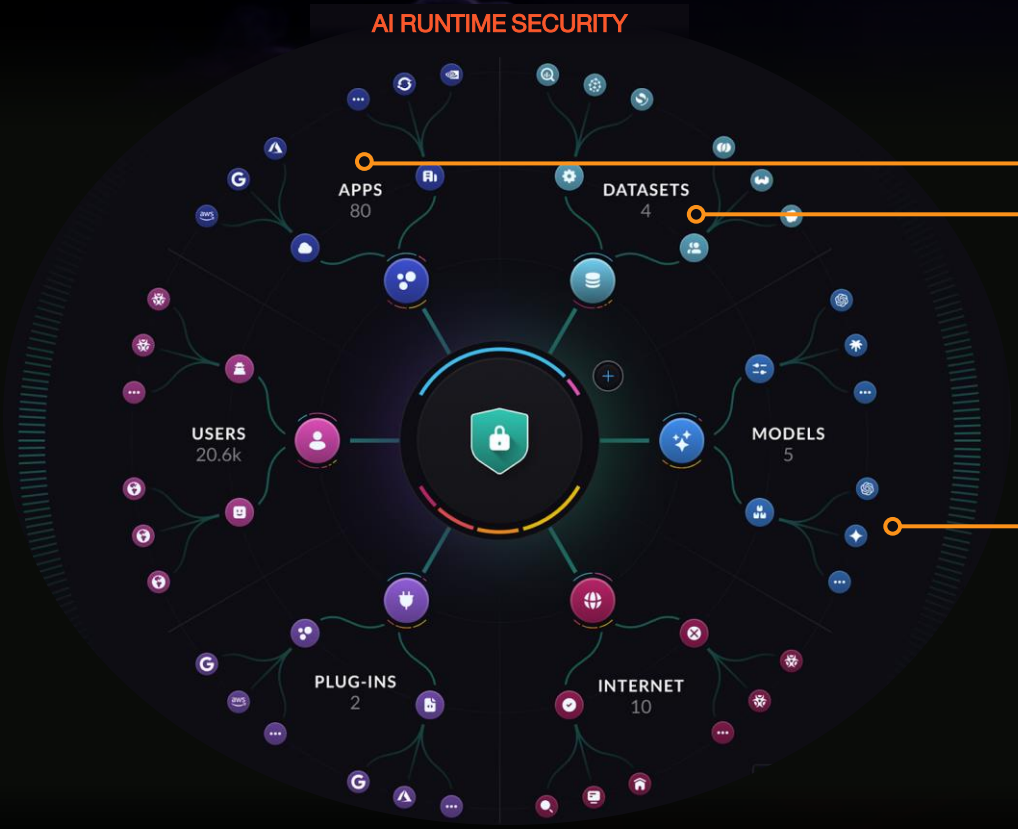
Prioritization and recommendation

Generate actionable insights and guided remediations

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

paloalto NETWORKS

AI Runtime Security to Protect Apps, Models, and Data



AI App Protection
Stop zero-day threats in zero time

AI Data Protection
Protect sensitive data from being leaked

AI Model Protection
Safeguard AI models from misuse and attacks

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

paloalto NETWORKS

Thank You

paloaltonetworks.com

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