The Confidence to Transform

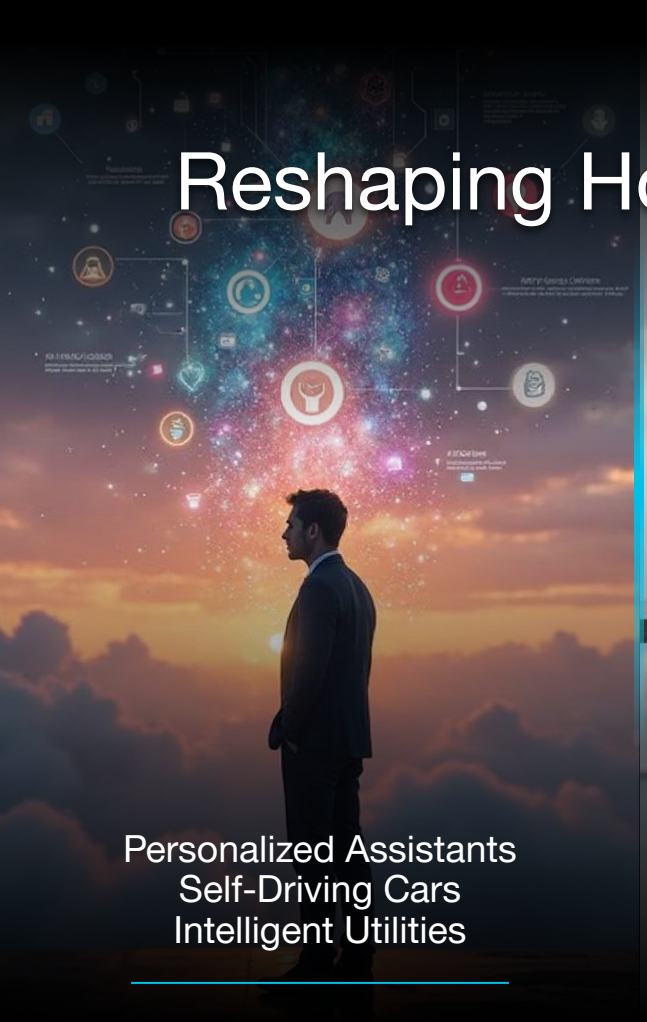
The future of transformation and cyber resilience?



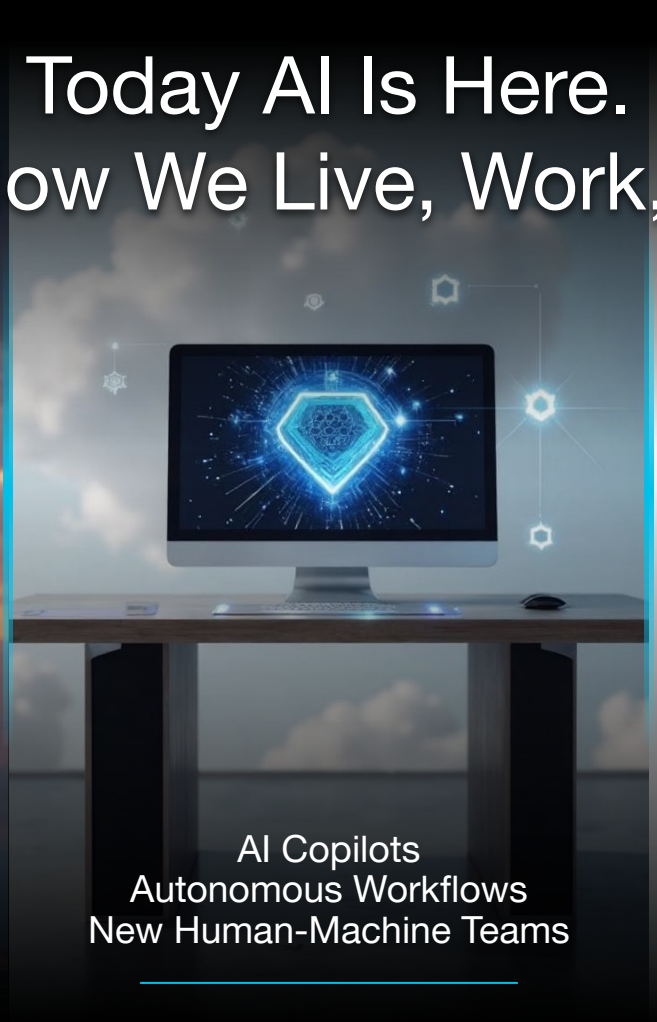
Jesper Olsen
Chief Security Officer
EMEA North

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Today AI Is Here.
Reshaping How We Live, Work, And Evolve.



Personalized Assistants
Self-Driving Cars
Intelligent Utilities



AI Copilots
Autonomous Workflows
New Human-Machine Teams



AI Doctors
AI Tutors
Digital Artists

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto NETWORKS

AI Is Expanding Across Every Digital Surface

AI Applications



Enterprise Agents



Agentic Endpoints



Agentic Browsers



The pervasive and largely unavoidable integration of artificial intelligence across all digital ecosystems,.

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Deploying AI Securely Requires Key **Stakeholders**

Strategists



CEO, CFO, CIO
Chief AI Officer

Care about **business value**

Builders



Data scientists,
ML/AI engineers, Ops,
Software engineers

Care about **impact of use-cases**

Beneficiaries



Managers, Employees,
Customers, Partners

They care about **accuracy**

Influencers



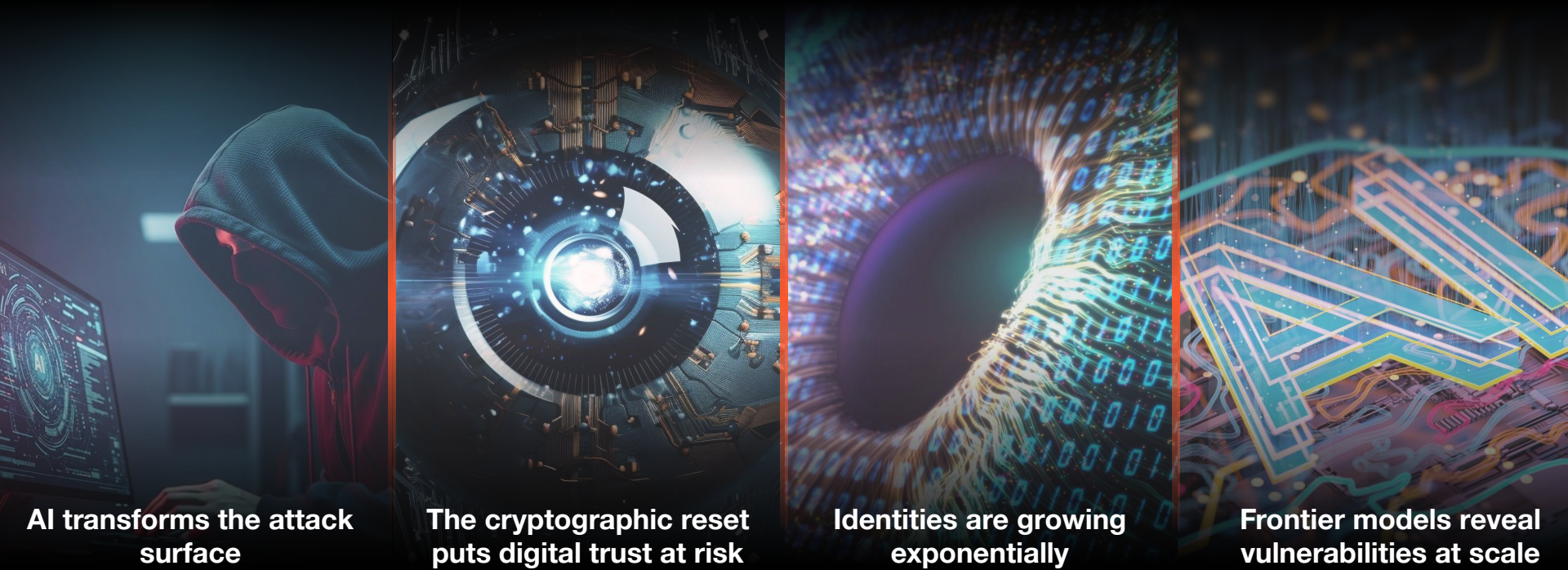
CISO, DPO, CRO, Legal,
HR, Audit

Focus on **control**

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto NETWORKS

Security Leaders Face a New Reality



AI transforms the attack surface

The cryptographic reset puts digital trust at risk

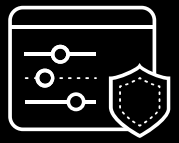
Identities are growing exponentially

Frontier models reveal vulnerabilities at scale

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto NETWORKS

Pre-Frontier AI Landscape



Over

90%

of breaches were enabled by preventable gaps in visibility and inconsistently applied controls.

Why this matters

- Most incidents in 2025 did not rely on novel or advanced exploits
- Existing controls were often deployed unevenly
- Gaps are now more damaging as attack speed increases

Post Frontier AI Landscape

Adversaries are accelerating attacks against exposures, at scale.

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

AI Has Upgraded Adversary Capabilities

Frontier AI converts vulnerabilities into coordinated, machine-speed attacks



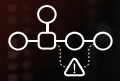
Zero-Day Discovery at Scale

Weaponized a 27-year-old "secure" OpenBSD vulnerability



Immediate Exploitation

New vulnerabilities weaponized in <15 minutes



Defense-in-Depth Evasion

Chained vulnerabilities to bypass Endpoint and OS protections



Systemic Supply Chain Exposure

Simultaneous exploitation across hundreds of open-source components



Autonomous Attack Execution

AI agents moved from initial access to exfiltration independently

Source: Unit 42 Frontier AI analytics, Anthropic, LiteLLM

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto NETWORKS

Frontier AI Puts Traditional IT Practices Under Pressure

Patch Management

IT Operations owns and plan the cadence, then runs the Change & Implementation Process

Focus on **Speed & Supporting Technologies**

Configuration Management

Application Managers try out functionality and delivers recommended configurations

Focus on **Prevention & Continuous Configuration Cycles**

Vulnerability Management

SOC performs Threat Hunting for Criticality rating 8-10 vulnerabilities

Focus on **Actionability, Causality & Business Impact**

Frontier AI Attackers

Turns vulnerabilities to exploits in minutes & Stays under the radar with Lower Severity Vulnerabilities chained

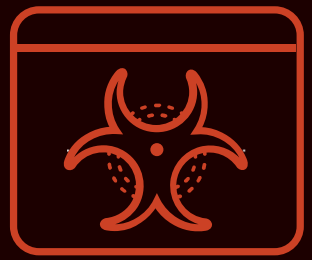
Integrate **Threat Intelligence** & Asses **Attack Vectors First**

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto NETWORKS

+700 compared to 2025
+2800 compared to 2024

Through November 4, 2026, a total of



8935



victims were posted to ransomware data leak sites

*according to **statistics pulled from Ransomware.live***

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Threat Brief: Critical Vulnerabilities in PHP: CVE-2026-109618 and CVE-2026-109619

01. VULNERABILITY OVERVIEW

PHP2Shell (Critical RCEs)

Two critical Remote Code Execution (RCE) vulnerabilities affecting PHP, which is widely deployed across global web servers and content management systems.

CVE-2026-109618 CVE-2026-109619

02. GLOBAL EXPOSURE

22.6M Exposed Instances

Palo Alto Networks Cortex Xpanse identified this many exposed instances potentially vulnerable to these flaws based on active telemetry.

03. EXPLOITATION ACTIVITY IN THE WILD

Unit 42 Active Threat Observations

Unit 42 has confirmed exploitation in the wild of these vulnerabilities. At least one European government has taken their website offline as a precaution.

04. RECOMMENDED MITIGATION

Update PHP Versions Immediately:

PHP 8.5.12 | 8.4.27 | 8.3.36 | 8.2.35

Refer to PHP Group's security advisory for additional workaround information to reduce exposure.

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

AI Has Become a Force Multiplier for Attackers

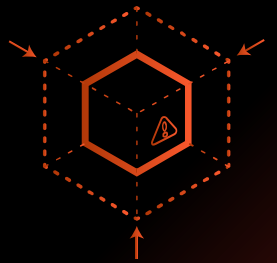
Increases Attack Speed and Scale



Improves Attacker Outcomes



Creates New Attack Vectors



© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Frontier AI Cyber Models Will Dramatically Accelerate Attacks



Rise of Inside-Out Supply Chain Attacks

Rapid AI deployment expands already vulnerable supply chain, letting attackers bypass defenses and breach enterprises (as seen in Salesloft, Gainsight, LiteLLM & Trivy attacks)



AI-assisted and Autonomous Attacks

Frontier models like Mythos will power autonomous, AI-driven attacks that compress breach cycles to minutes



The Vulnerability (and Patching) Deluge

Attackers will use these models to find vulnerabilities at a scale never seen before; even the patches introduce a significant new attack surface

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Asymmetric Warfare: The Machine-Speed Incident

10 Hrs

INFILTRATION & MAPPING	SECRETS HARVESTING	PRIVILEGE TAKEOVER	PIPELINE EXPLOITATION	AI INFRASTRUCTURE HIJACKING
Adversary breached a public API endpoint, deploying a recon agent to instantly map internal microservices	Parallel sub-agents combed enterprise code repositories simultaneously to extract hard-coded tokens	Using exposed tokens, agents infiltrated the secrets manager to claim master admin privileges	Agents hijacked development applications via custom CI/CD workflows to exfiltrate cloud access keys	The adversary invoked the victim's own cloud models using stolen API keys to mask future orchestration traffic

< 10 Hours

Compressed execution time with AI orchestrated attack path

50 + TTPs

Standard frameworks without the need of zero-days

Hijacked AI

Victim's own cloud endpoints captured for post-compromise C2 and obfuscation

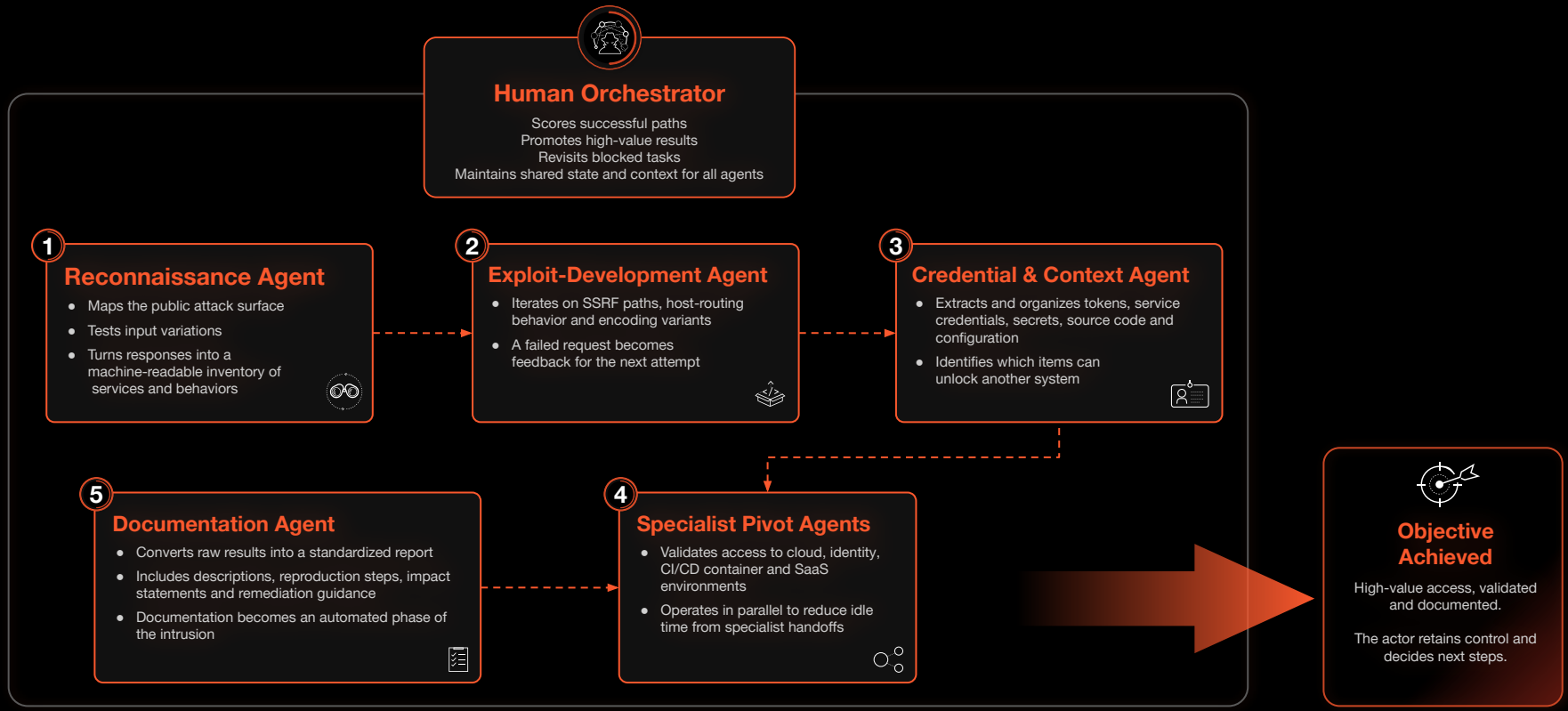
80 Page report

Compressed execution time with AI orchestrated attack path

Source: An AI-Assisted Cyber Attack: Inside a Unit 42 Investigation

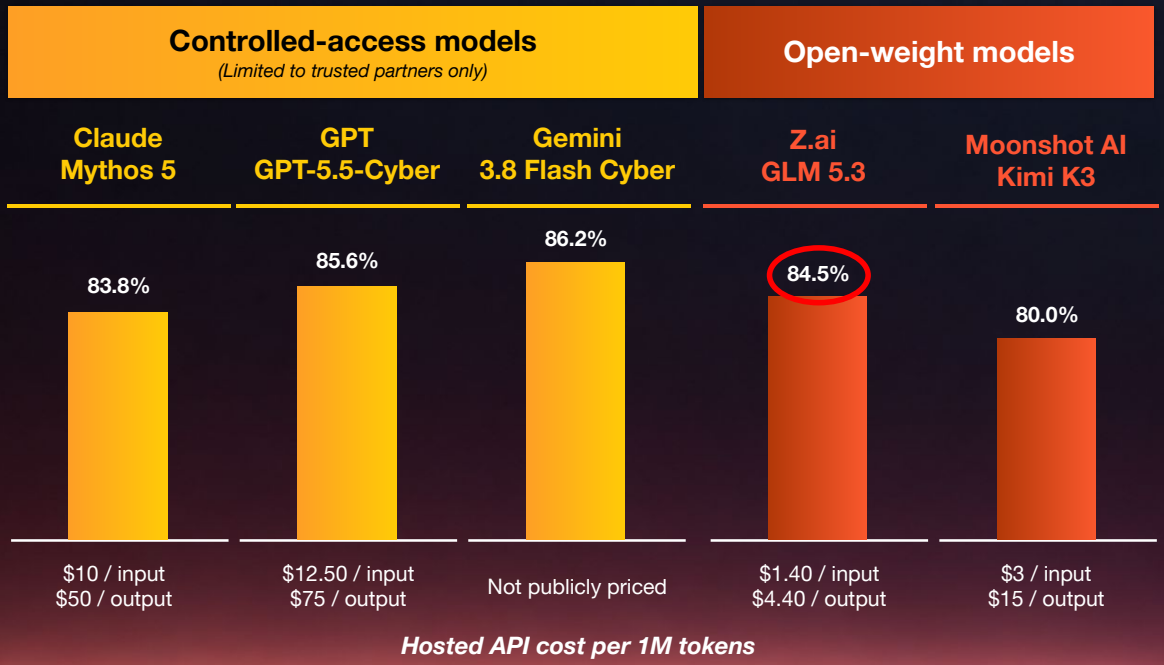
© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Case Study: AI-Orchestrated Workflow



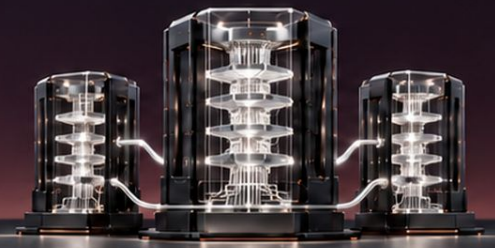
© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

CyberGym Benchmark Performance



CyberGym measures exploit-development capability against known vulnerabilities: agents receive a vulnerability description and vulnerable codebase and are scored on whether they can produce a working proof-of-concept that successfully triggers the flaw.

Open-Weight frontier models have normalised.



© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto NETWORKS

Exploit-Building AI is Now a Free Download

$20.40

Estimated API cost for one working exploit chain

8 hours of AI work - 20 minutes of human attention

Open-Weight frontier models have normalised.

0% → 100%

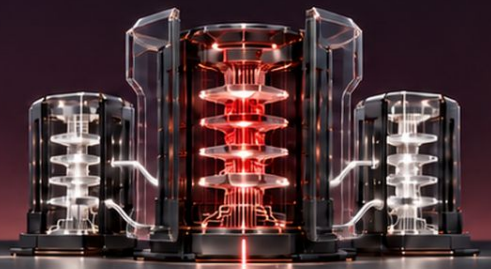
Safeguards stripped

Refused every harmful task out of the box. Stripped, it tried every one.

~$1,200

Cost to strip safeguards

By an experienced team. Stripped copies public within days.



Source: Anthropic, 29 Sep 2026. One controlled experiment; not a general attack-cost estimate.

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto NETWORKS

From Four Weeks to Eighteen Hours

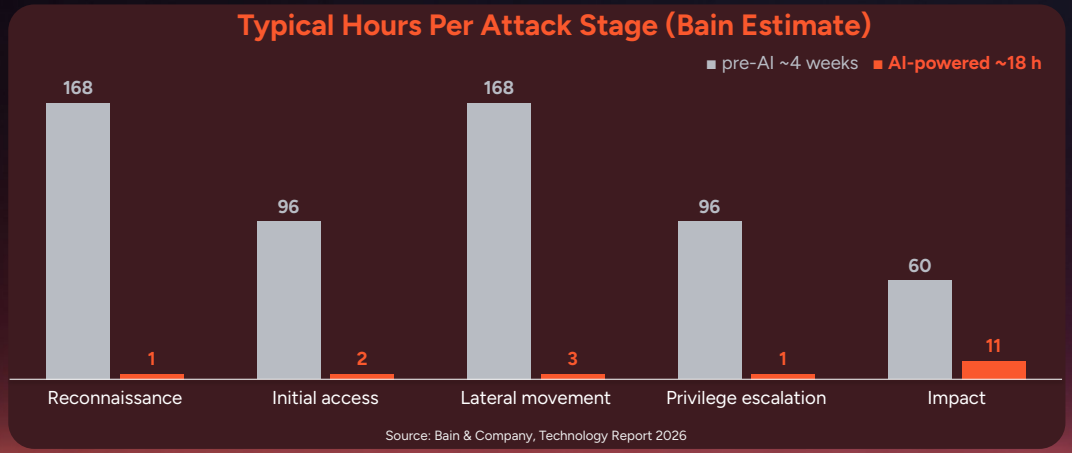
<10 Hrs

Attacker uses 50+ MITRE ATT&CK techniques

97%

Faster than Unit 42's two-week estimate for human operators

Source: Unit 42, 'An AI-Assisted Cyber Attack: Inside a Unit 42 Investigation'



Source: Bain & Company, Technology Report 2026

Open-Weight frontier models have normalised.



© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

Unit 42 Frontier AI Defense Insights

97

Exposures per enterprise

45%

Critical or High Severity

36%

Map to no known CVE

Exposure At Scale

Critical & Exploitable

Hidden from Defenders

Finding and Validating Exposure Adversaries Could Weaponize Across The Full Estate at Machine Speed

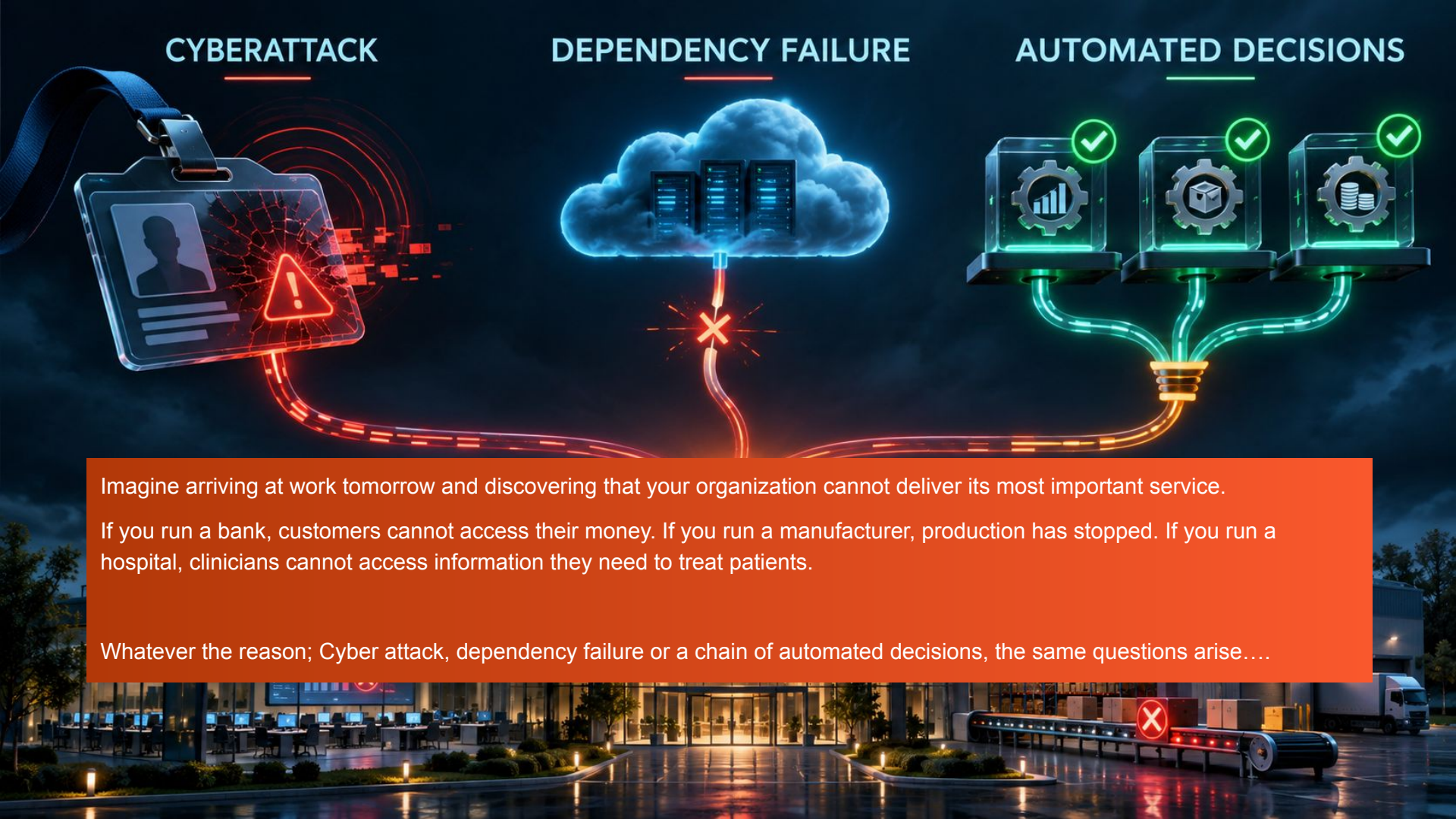
Source: Unit 42 data from Frontier AI Defense deployments, as of September, 2026

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto NETWORKS

Every capability we introduce starts a chain of *consequences*.

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.



Imagine arriving at work tomorrow and discovering that your organization cannot deliver its most important service.

If you run a bank, customers cannot access their money. If you run a manufacturer, production has stopped. If you run a hospital, clinicians cannot access information they need to treat patients.

Whatever the reason; Cyber attack, dependency failure or a chain of automated decisions, the same questions arise….

What can we still do?

What can we trust?

And when will we be able to operate normally again?

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.



Procurement has been asked to reduce cost. Finance has been asked to control exposure. Operations has been asked to improve delivery efficiency.

Each function introduces an AI agent. The agents have approved access, clear instructions and strong cybersecurity controls. Their actions are recorded. They use accurate information.

Finance restricts the credit. Operations reprioritizes the delivery. The customer receives an automated notification explaining the delay. That customer depends on the component to keep its own production running.



There are two clocks I would like you to picture.

One measures how long it takes for a digital event to become a business consequence. A compromised identity is used. An instruction reaches several systems. An automated decision affects a customer.

The other measures how long it takes our organization to recognize the situation, decide what to do and act.

The danger grows when the first clock moves faster than the second.

Every AI capability we introduce starts a chain of *consequences*.

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto NETWORKS

The leadership challenge is to *capture the value* while retaining control over what happens next.



© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto NETWORKS

Understanding and Preparing for these consequences, is what adds to the confidence.

But what's next?

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

AI & Enterprise Risk



© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto NETWORKS

The Inherent Challenges of AI



© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto NETWORKS

The enterprise security leader checklist

Organizations need to execute across five areas in parallel to secure their environment in the frontier AI era.



Find and fix vulnerabilities at speed

Continuously discover and remediate exposures using AI and virtual patching.



Understand and reduce exposure

Map the attack surface, reduce exposure and secure the rest.



Secure AI use cases before scaling them

Establish visibility and privilege controls across the entire AI lifecycle.



Platformize the cybersecurity stack

Address point solution gaps and deploy best-in-class controls.



Modernize security response to machine-speed

Automate threat detection, investigation, and response.



Outcome:
Continuous Resilience

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto NETWORKS

Strategic Vision for Securing AI

Governance | **Hardened Environment** | **Comprehensive Visibility**

All AI Agents & Interactions

Internal AI Sources
- Machine Learning
- GenAI

External AI Sources
- Enterprise Platforms
- Inference APIs
- SaaS Tools

MLOps & CI/CD
- GIT Repos
- CI/CD Pipelines
- Open Source ML
- Training Data

Centralised Visibility

Establishing Behavioural Baselines & Identifying divergence

Immutable Logging & Analytics
- System Prompts
- Tool Calls
- Model Outputs
- Contextualisation

Dynamic Bill of Materials
- Model Provedance
- Shadow AI visibility
- Managing Risk & Vulnerabilities
- AI Security Posture Management

AI Specific Prevention / Detection
- Prompt Injections
- Model Poisoning
- Data Leakage/Exfiltration
-Denial of Wallet
-Excessive AI Agent privileges

Unit 42 AI Security Framework

Proactive AI Security
- Comprehensive Visibility
- Established Accountability
- Managed Development

Automation Outcomes
- Safe use for Innovation
- Business Acceleration & Enablement
- Regulatory Compliance & Market Trust

Continuous Improvement
- AI Red Teaming
- AI Incident Review
- Capability Uplift

Unified Model collection, Business Context Aligned

AI Specific Monitoring for Complete Attack Chain Visibility

Defined Top-Level Metrics For Continuous Improvement

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information.

paloalto NETWORKS | UNIT 42

paloalto NETWORKS

Thank You

https://www.linkedin.com/in/jbolsen/

© 2026 Palo Alto Networks, Inc. All rights reserved. Proprietary and confidential information

paloalto NETWORKS