CORPORACIÓN FONAFE

Dejando Huella

FONAFE TECH

Innovación y Tecnología:
Transformando las Empresas del Estado

CORPORACIÓN FONAFE

Dejando Huella

FONAFE TECH

Jesús Cruz

Senior Systems Engineer
Palo Alto Networks

CORPORACIÓN FONAFE

Dejando Huella

FONAFE TECH

Ciberseguridad en la nueva era de IA. ¿Realmente mi información corre riesgo?

Ciberseguridad en épocas de IA

¿Realmente mi información corre riesgo?

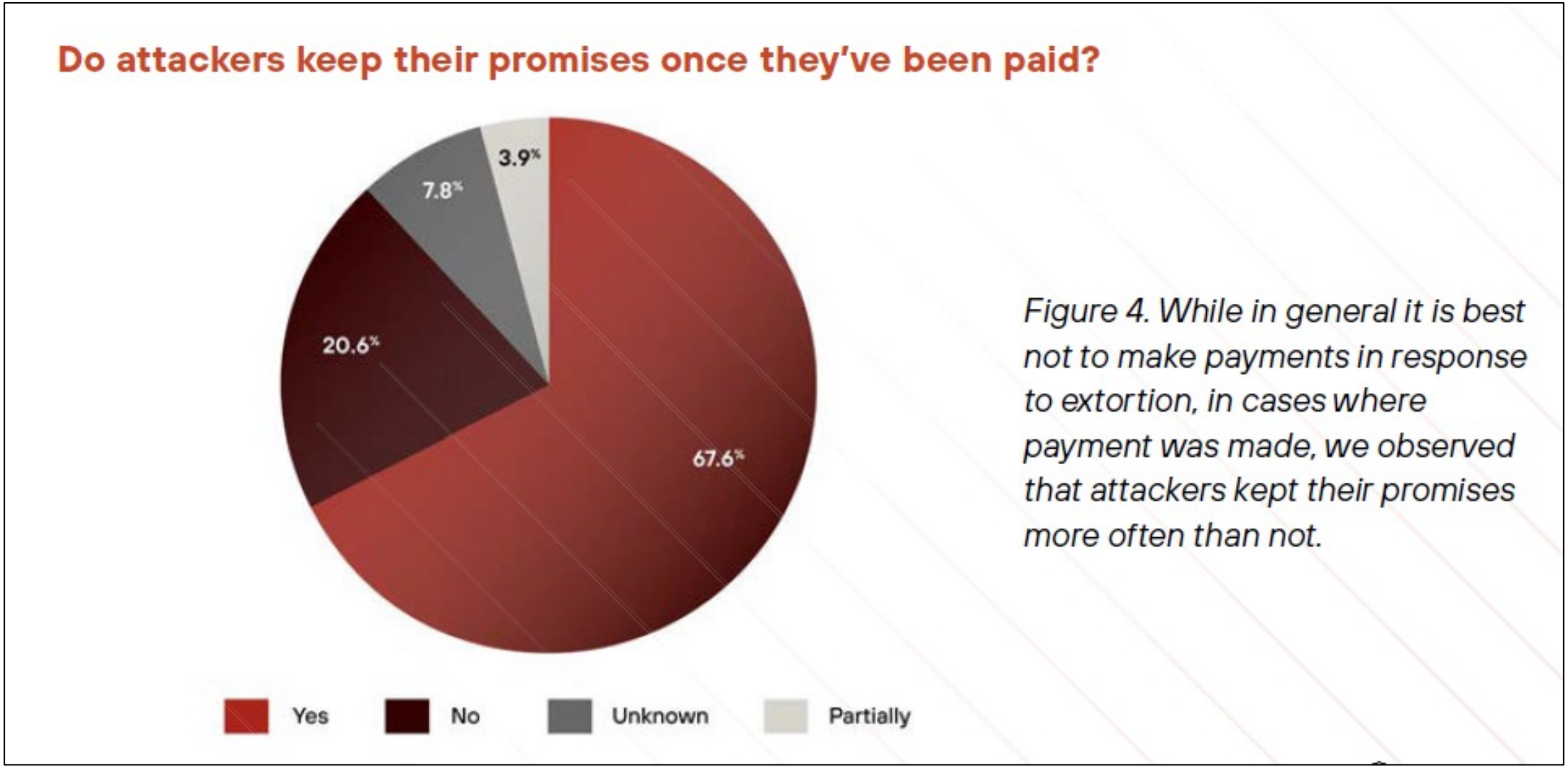
Jesús Arturo Cruz Ortiz
Systems Engineer

Ciberataques 2023

	Incidents				Breaches			
Industry	Total	Small (1–1,000)	Large (1,000+)	Unknown	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	30,458	919	1,298	28,241	10,626	617	986	9,023
Accommodation (72)	220	16	9	195	106	16	9	81
Administrative (56)	28	7	7	14	21	6	4	11
Agriculture (11)	79	5	0	74	56	4	0	52
Construction (23)	249	17	6	226	220	12	5	203
Education (61)	1,780	82	630	1,068	1,537	56	618	863
Entertainment (71)	447	16	2	429	306	10	1	295
Finance (52)	3,348	75	122	3,151	1,115	54	87	974
Healthcare (62)	1,378	54	21	1,303	1,220	41	18	1,161
Information (51)	1,367	79	62	1,226	602	49	19	534
Management (55)	22	4	1	17	19	4	1	14
Manufacturing (31–33)	2,305	102	81	2,122	849	62	49	738
Mining (21)	30	1	2	27	20	1	1	18
Other Services (81)	462	13	5	444	417	8	5	404
Professional (54)	2,599	205	102	2,292	1,314	124	73	1,117
Public Administration (92)	12,217	56	115	12,046	1,085	39	27	1,019
Real Estate (53)	432	35	5	392	399	29	2	368
Retail (44–45)	725	90	47	588	369	55	32	282
Transportation (48–49)	260	21	38	201	138	17	12	109
Utilities (22)	191	17	11	163	130	12	6	112
Wholesale Trade (42)	76	22	21	33	54	17	14	23
Unknown	2,243	2	11	2,230	649	1	3	645
Total	30,458	919	1,298	28,241	10,626	617	986	9,023

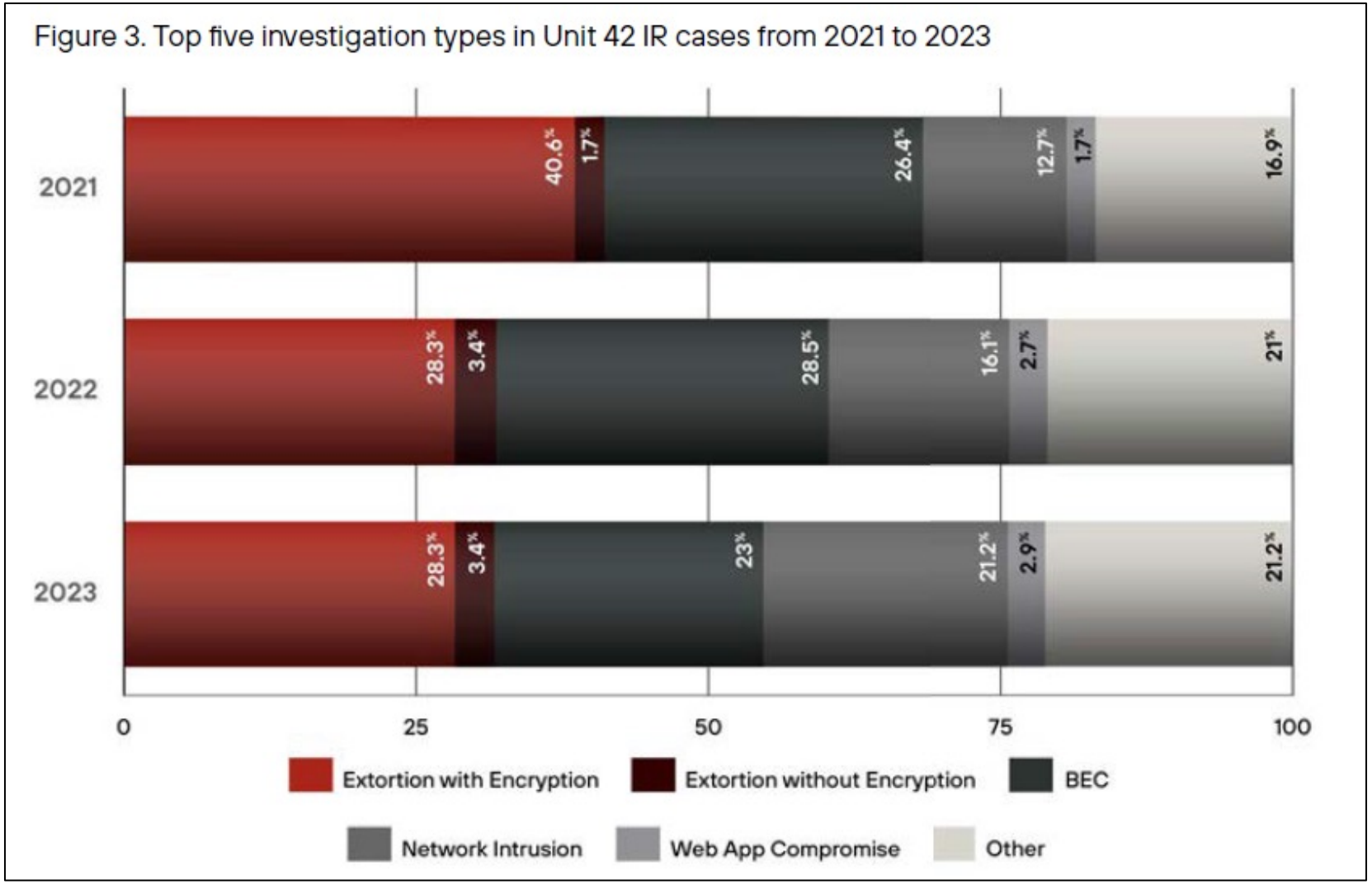
Fuente: 2024 Data Breach Investigations Report (Verizon)

¿El atacante cumple su promesa?



Fuente: 2024 Incident Response Report (Palo Alto)

Tipos de incidentes investigados



Fuente: 2024 Incident Response Report (Palo Alto)

Actores involucrados en un ataque

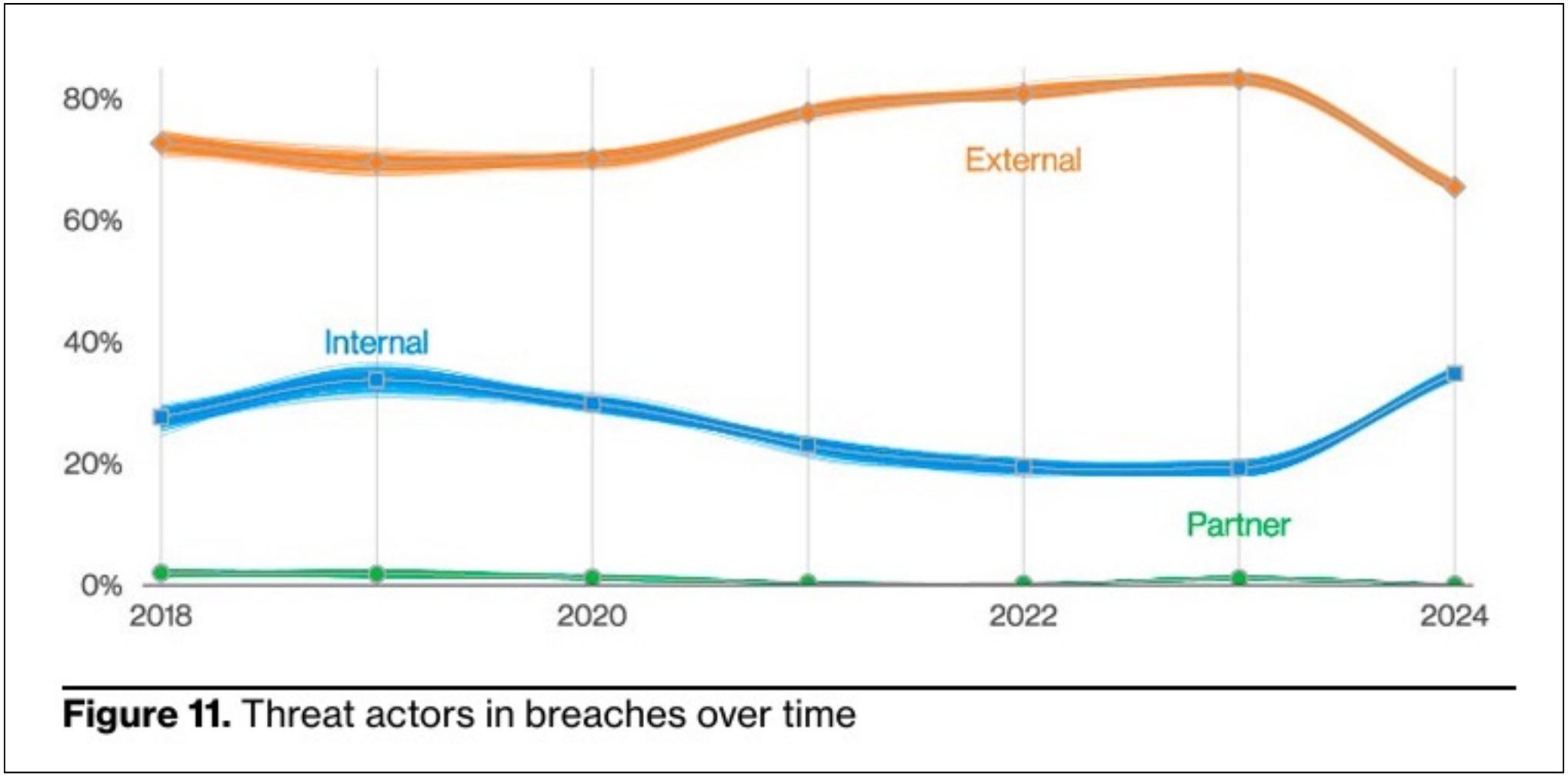


Figure 11. Threat actors in breaches over time

Fuente: 2024 Data Breach Investigations Report (Verizon)

Vectores de ataques comunes: Sector Financiero

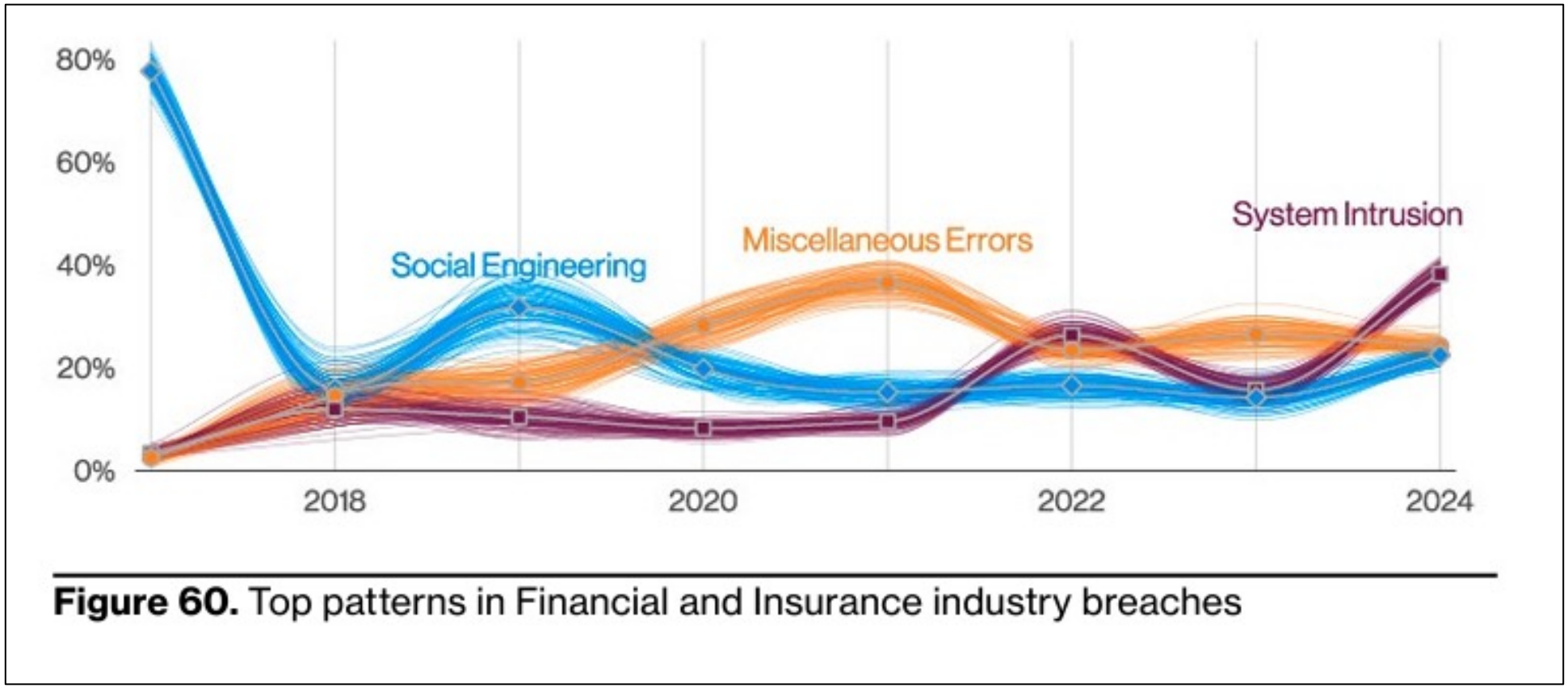


Figure 60. Top patterns in Financial and Insurance industry breaches

Fuente: 2024 Data Breach Investigations Report (Verizon)

Vectores de ataques comunes: Sector Público

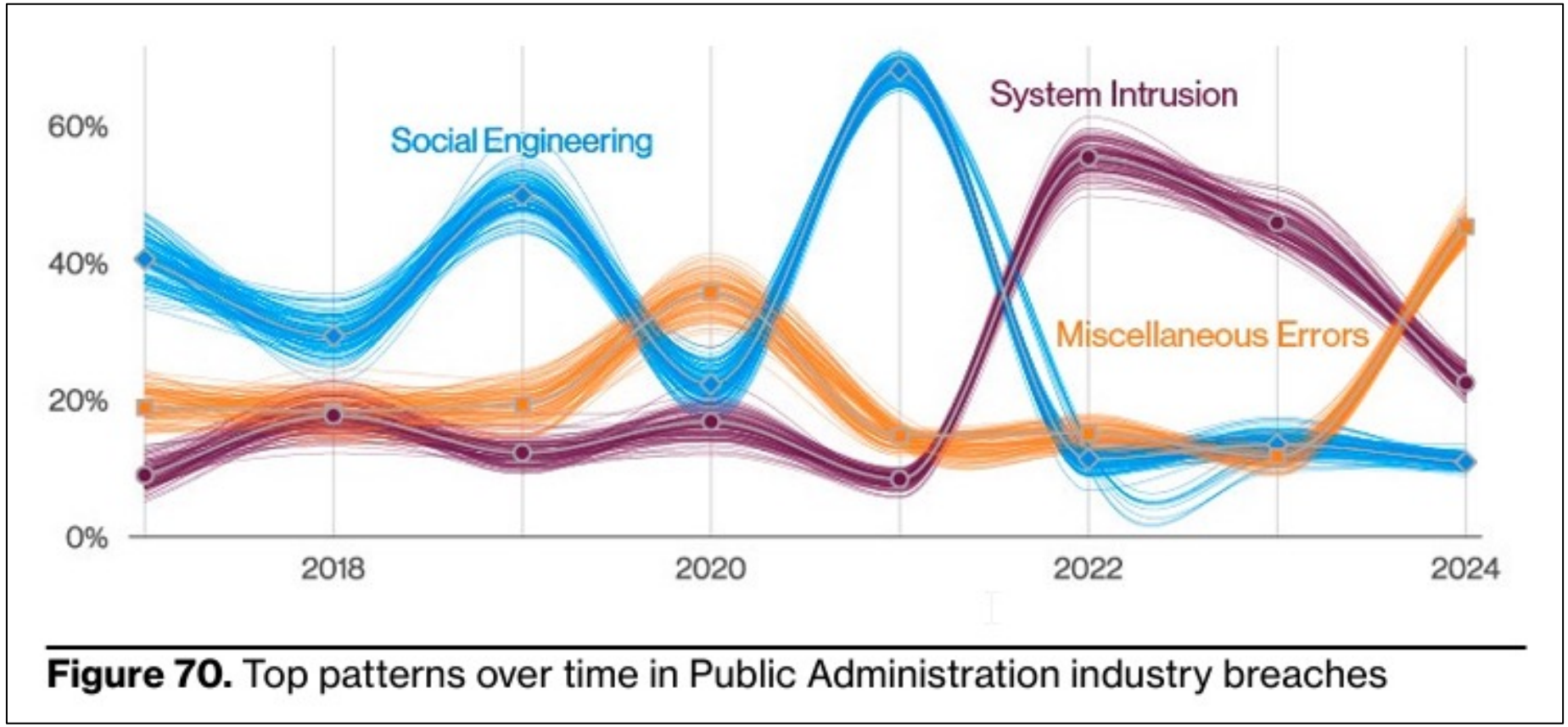
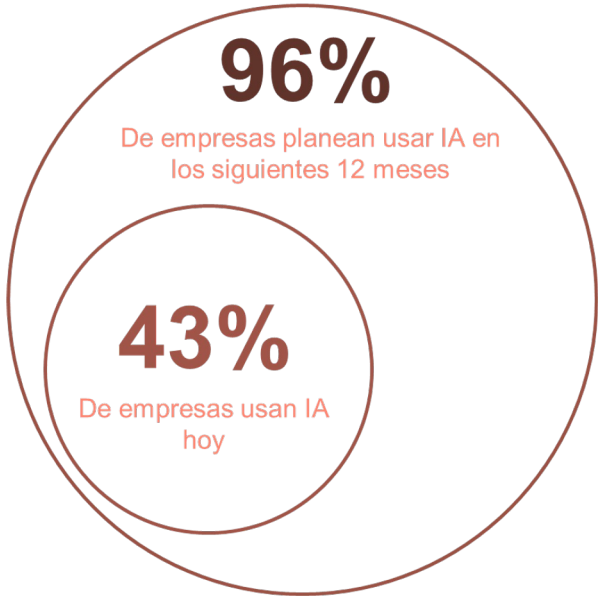


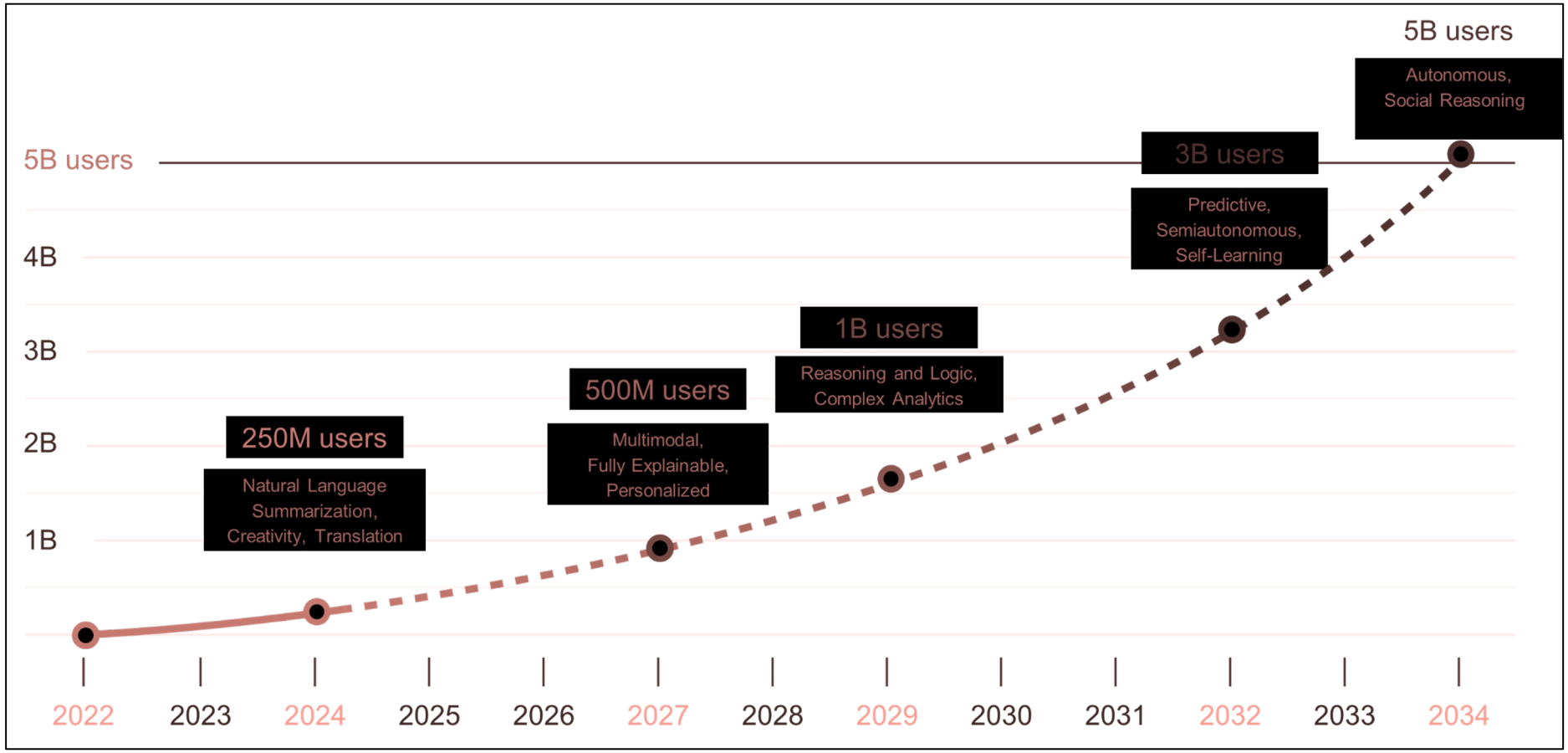
Figure 70. Top patterns over time in Public Administration industry breaches

Fuente: 2024 Data Breach Investigations Report (Verizon)

¿Como va la IA en esto?

La IA estará en todos lados





Uso de la IA para ejecutar ciberataques

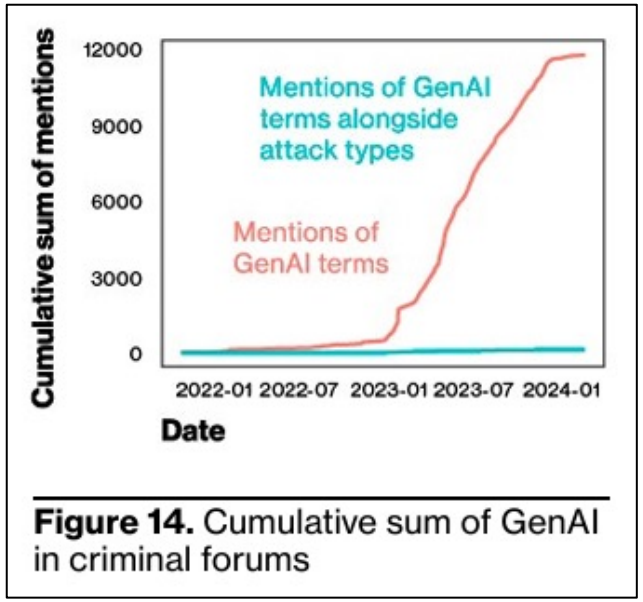
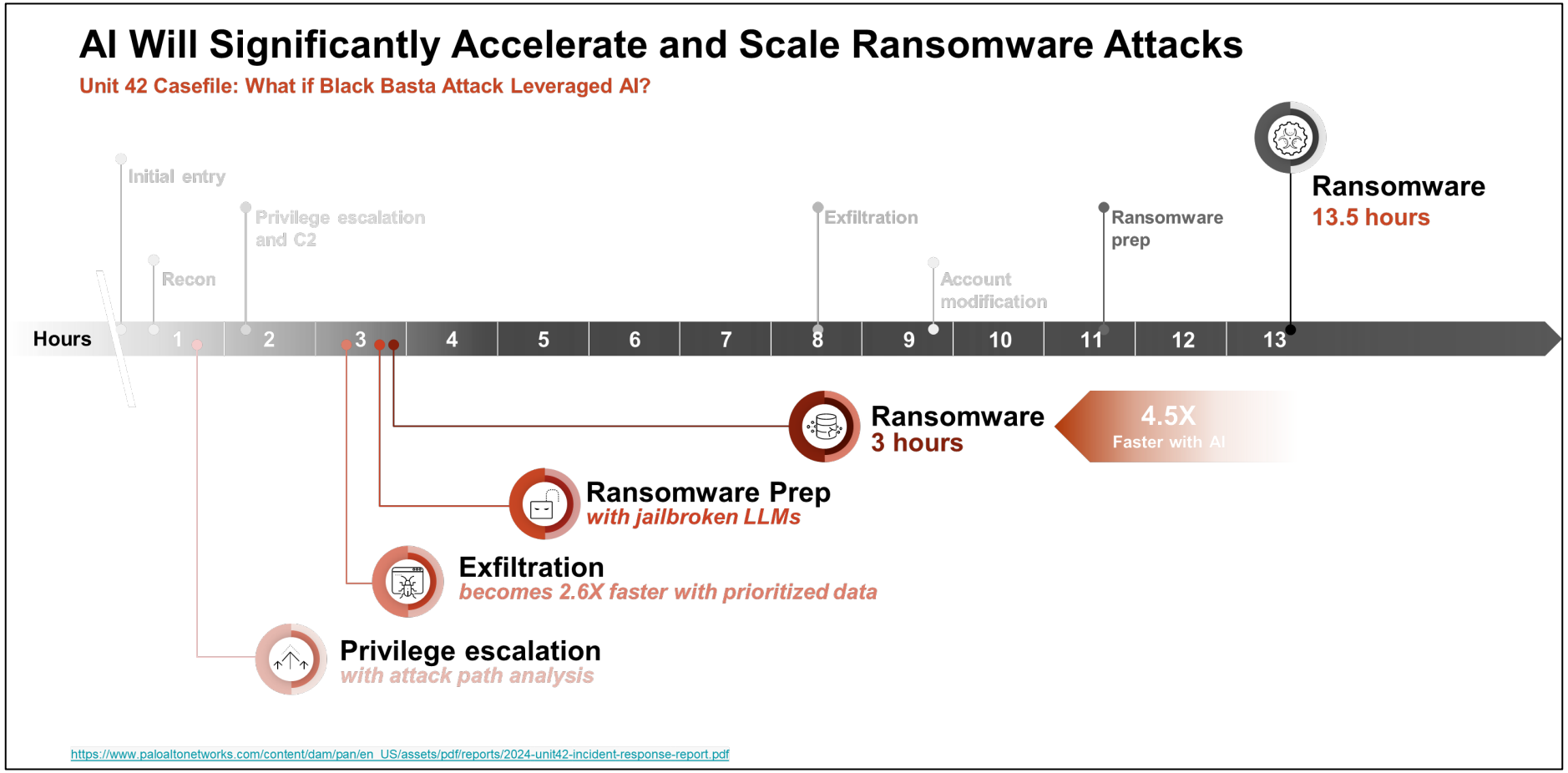
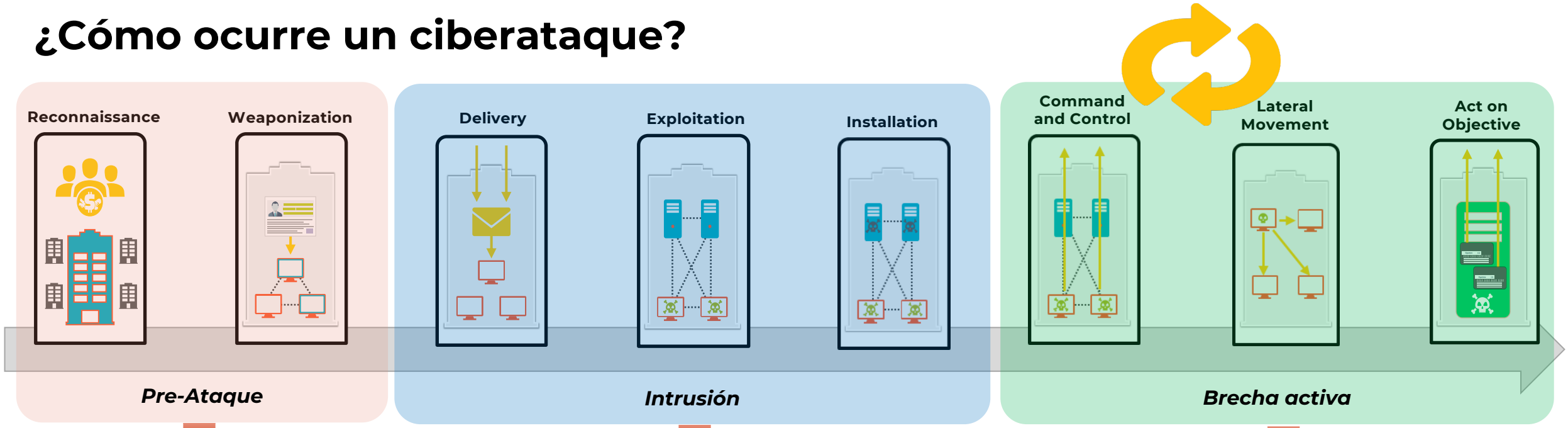


Figure 14. Cumulative sum of GenAI in criminal forums

Fuente: 2024 Data Breach Investigations Report (Verizon)



¿Cómo ocurre un ciberataque?



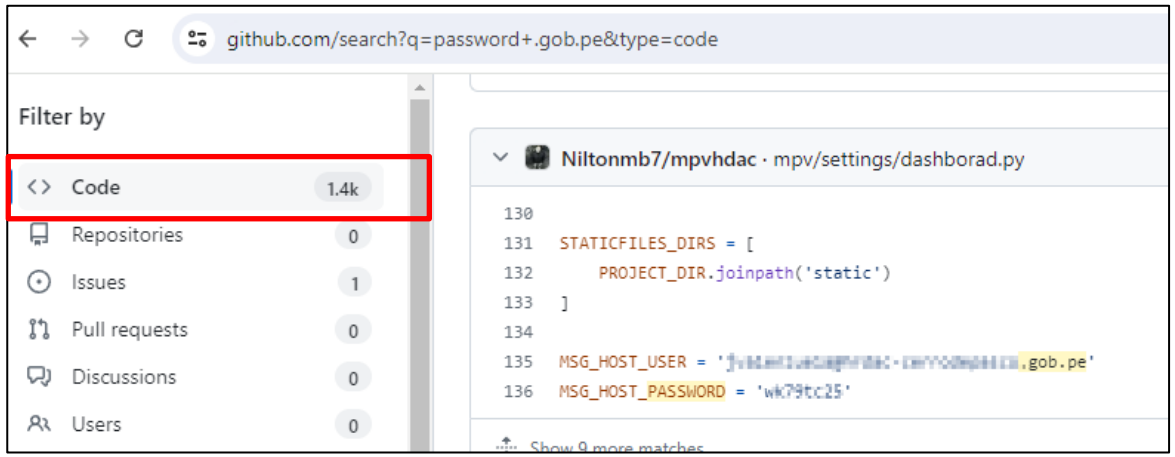
Horas a meses

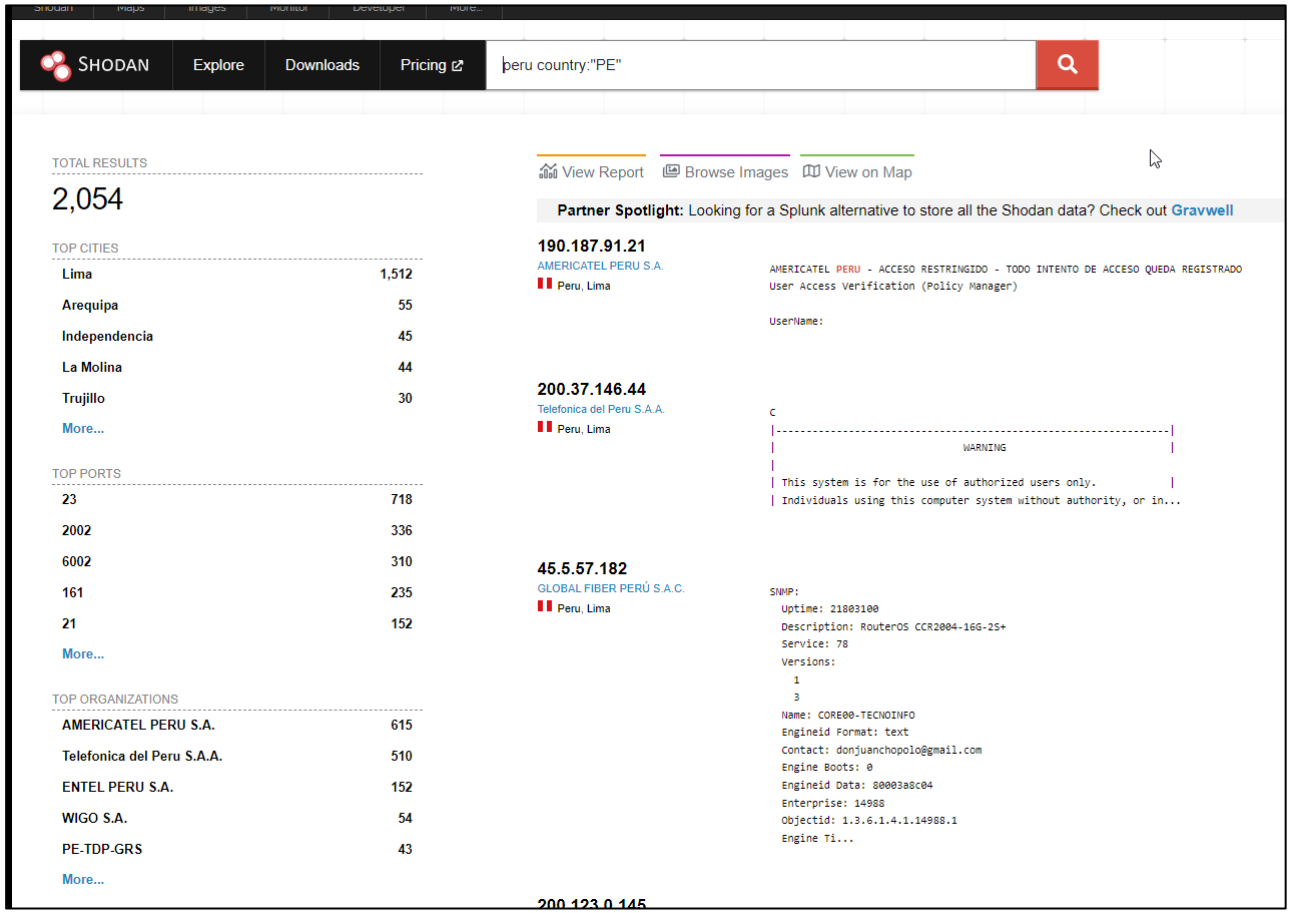
Segundos

- *1° RDP*
- *2° Phishing / Ing. Social*
- *3° Exploits*
- *4° Credenciales comprometidas*

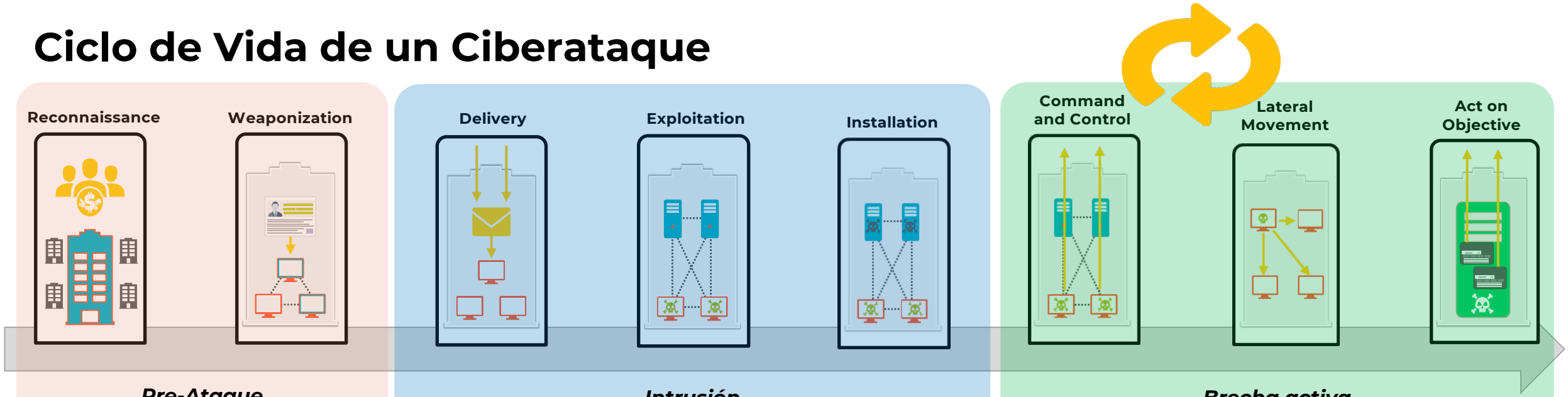
Meses

La información esta desperdigada





Ciclo de Vida de un Ciberataque



Horas a meses

Segundos

Meses (promedio 270 días)

NGFW WAF Antispam Sandbox CWP Antimalware Hardening

Controles **PREVENTIVOS**

Controles **DETECTIVOS**

IOC TTPs Threat Hunting Anomalías

Controles **CORRECTIVOS**

Mejor continua

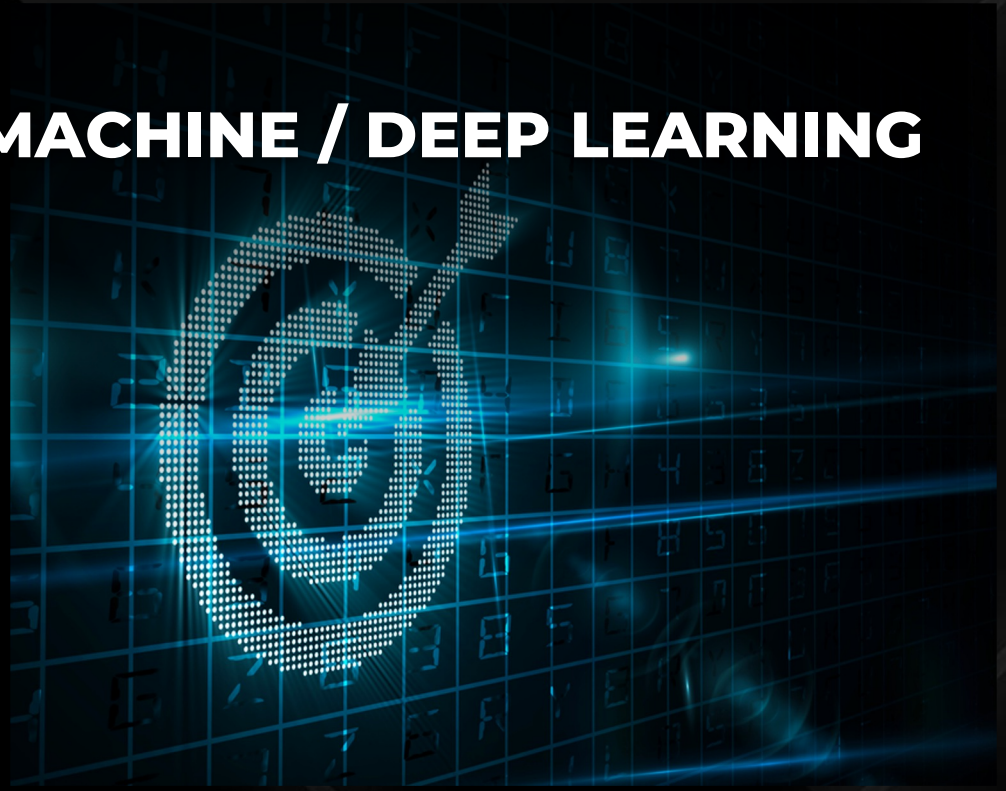
¿Qué tools usan los grupos de Ransomware?

- Cobalt Strike
- Mimikatz
- Bloodhunt
- Metasploit

- 7zip
- Anydesk / Teamviewer
- Onedrive / GDrive
- Powershell
- Systernals
- Putty
- AWS / Azure
- WinSCP
- DNS

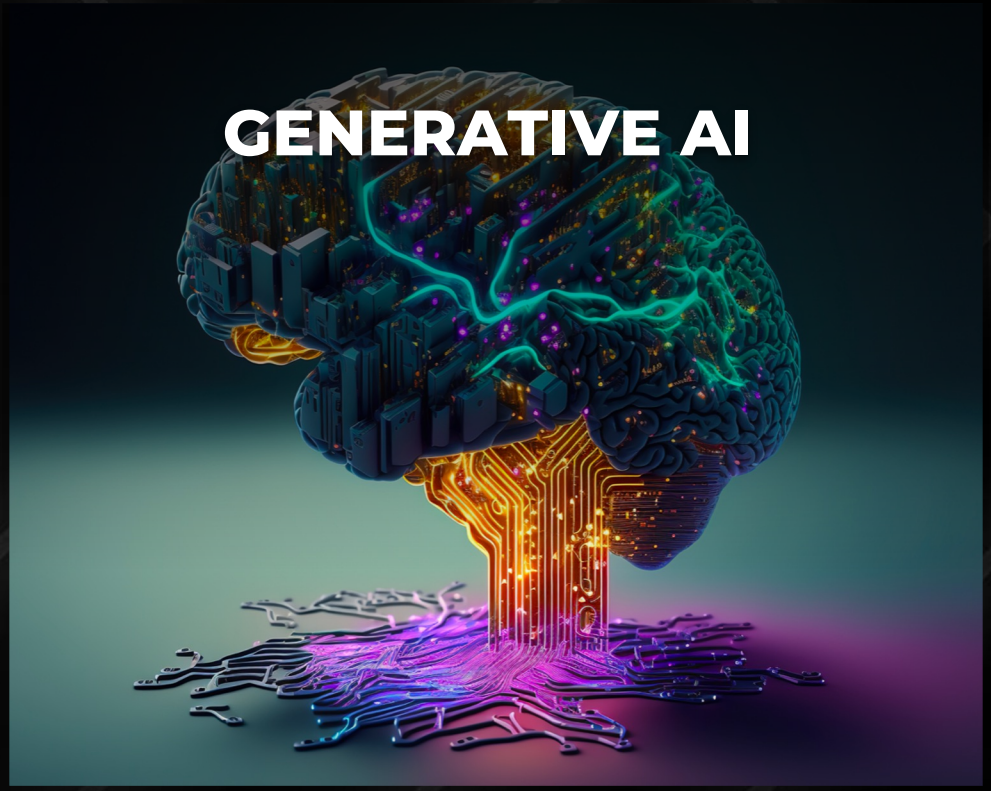
COMO DEFENDERNOS CON IA

MACHINE / DEEP LEARNING



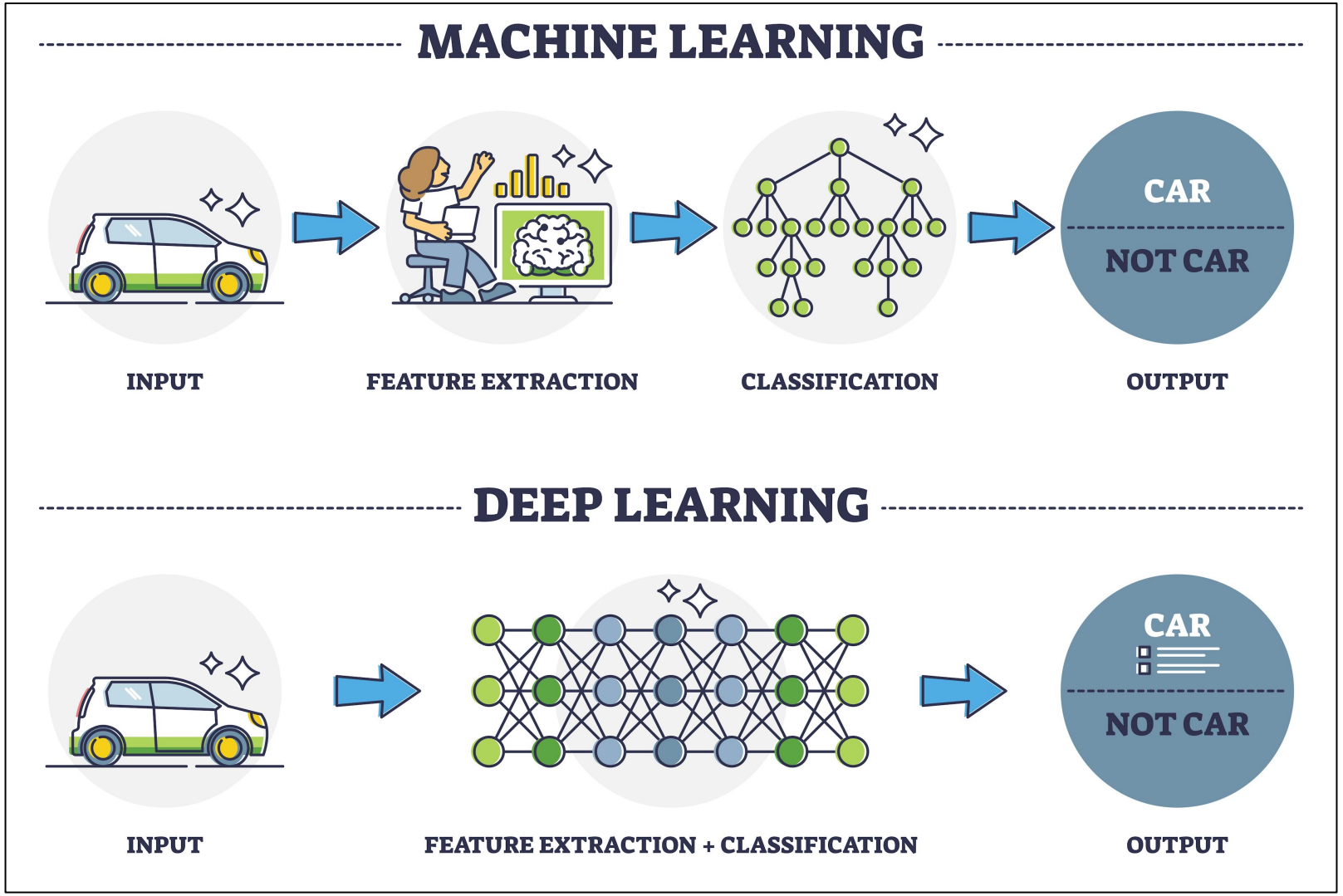
Deterministic models focused on **targeted, well-defined tasks** requiring high accuracy & precision

GENERATIVE AI

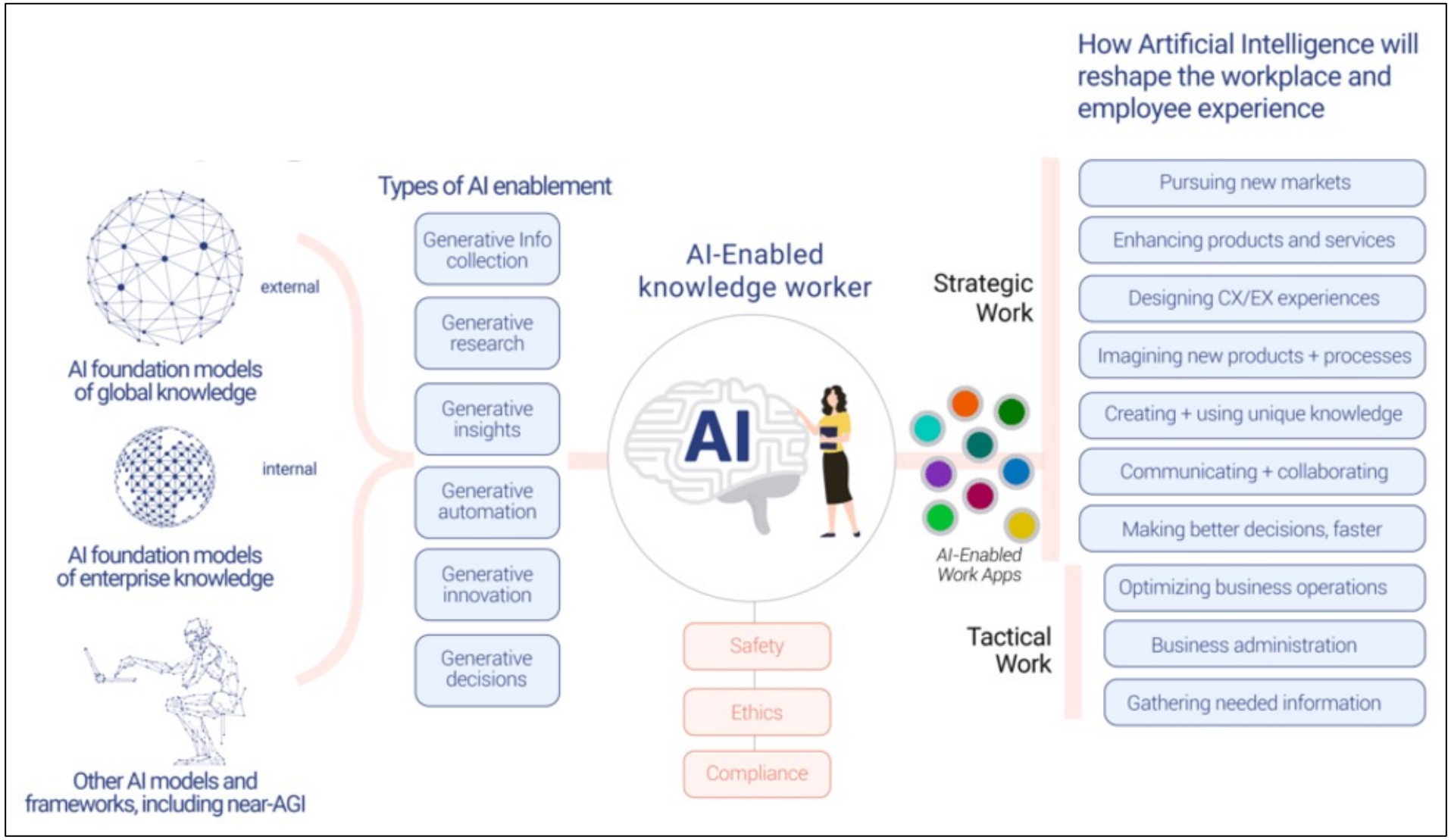


General-purpose, versatile models for **generating creative & non-deterministic content** from human language prompts

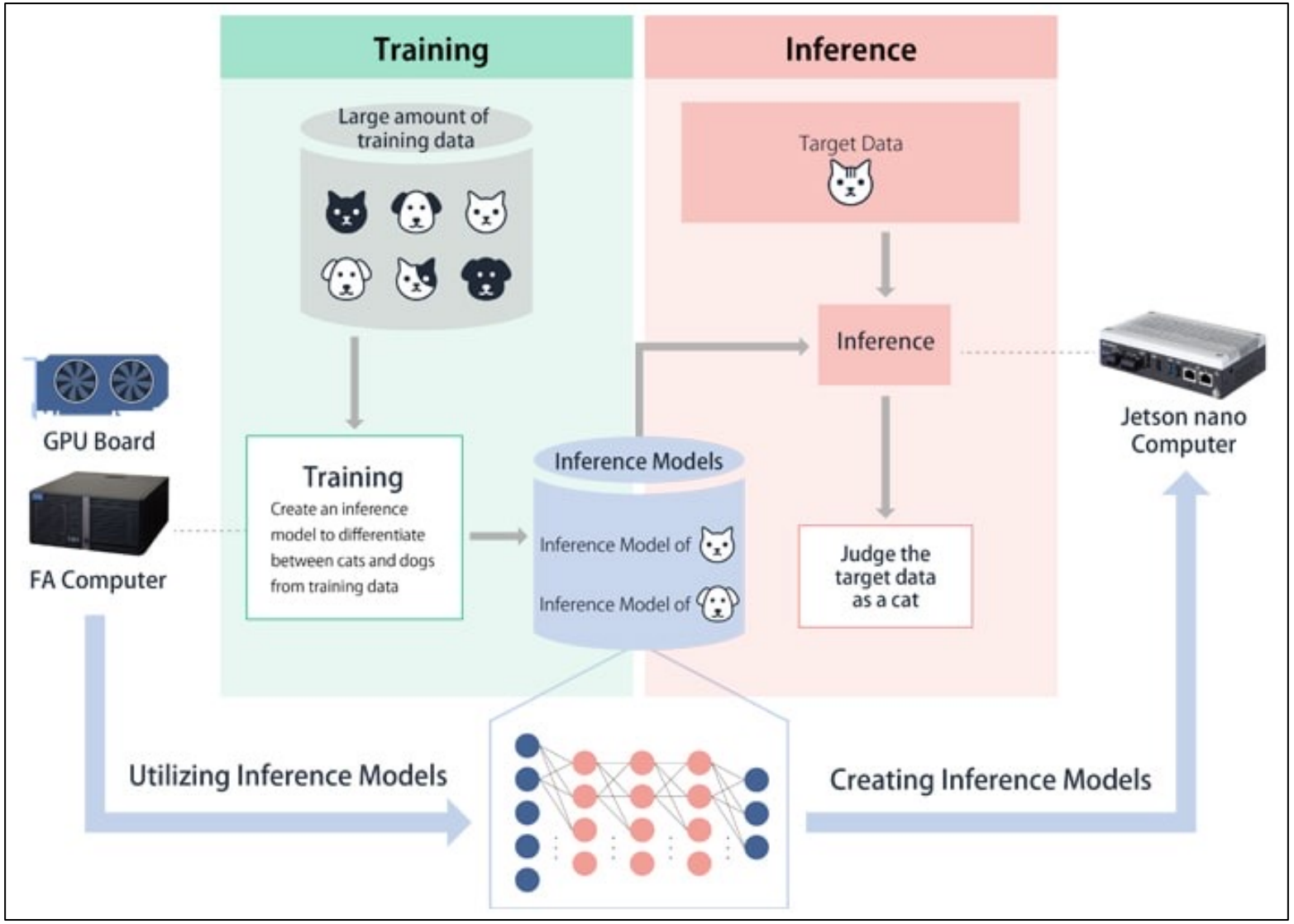
Machine / Deep Learning



IA Generativa



Training e Inferencia

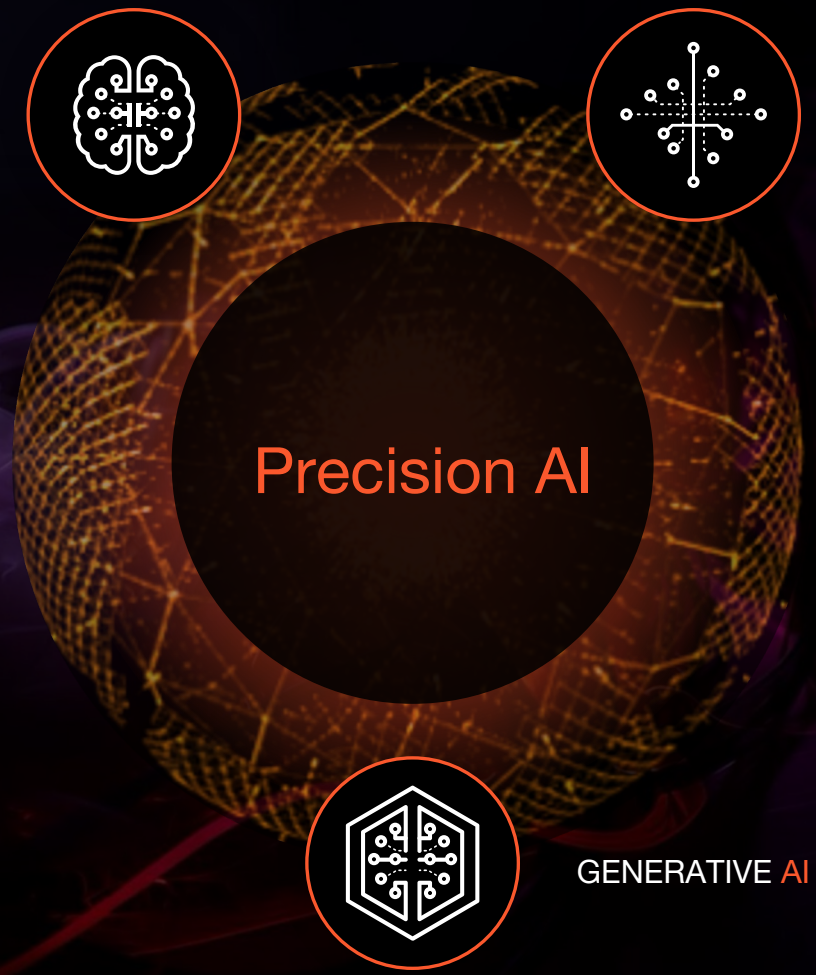


¿Qué se necesita para hacer una buena Ciberseguridad usando IA?

1. Muchísima data
2. Data de muy buena calidad
3. Alto nivel de I+D para desarrollar los algoritmos

Precision AI™

Inteligencia Artificial propietaria de Palo Alto Networks



Precision AI está entrenada con toda la data recolectada por Palo Alto Networks a nivel global

Cada día en nuestros más de **85,000** clientes

>7.6EB

de data ingestada

11.3B

ataques bloqueados en línea

2.3M

nuevos ataques identificados

1T rillon

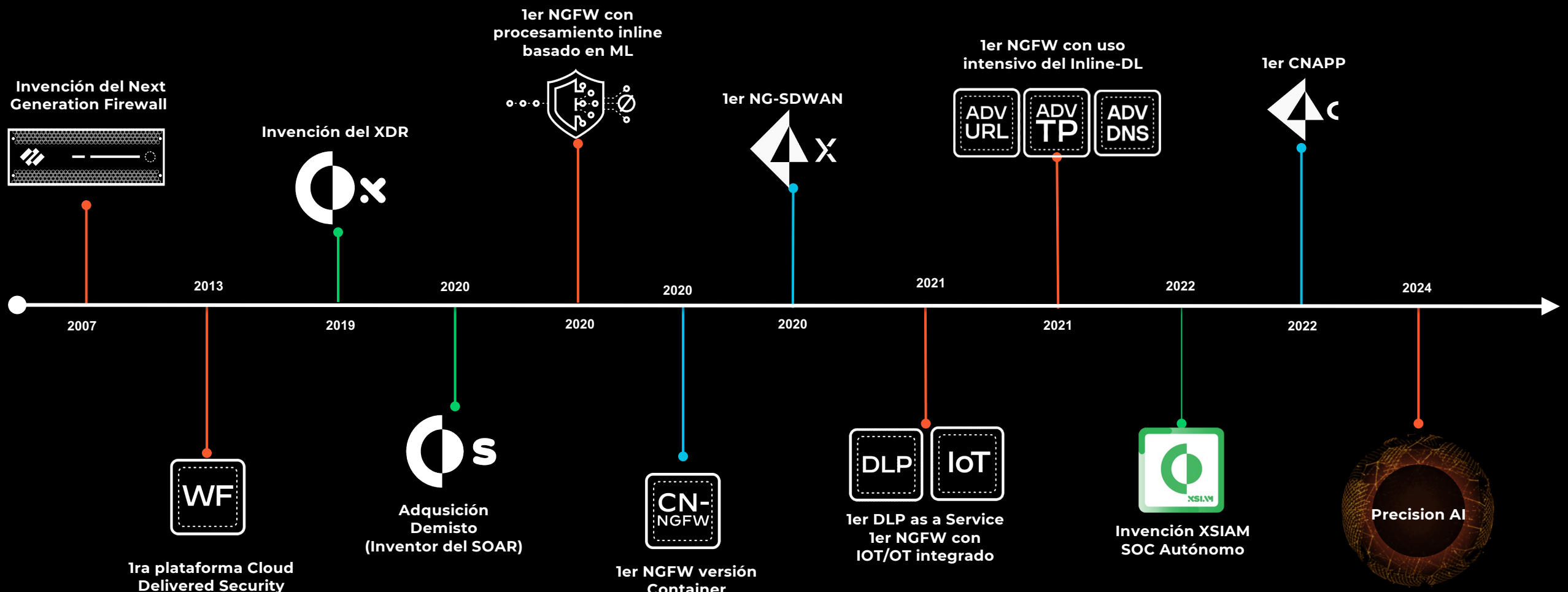
eventos cloud procesados

Data de Red, Endpoint y Nube

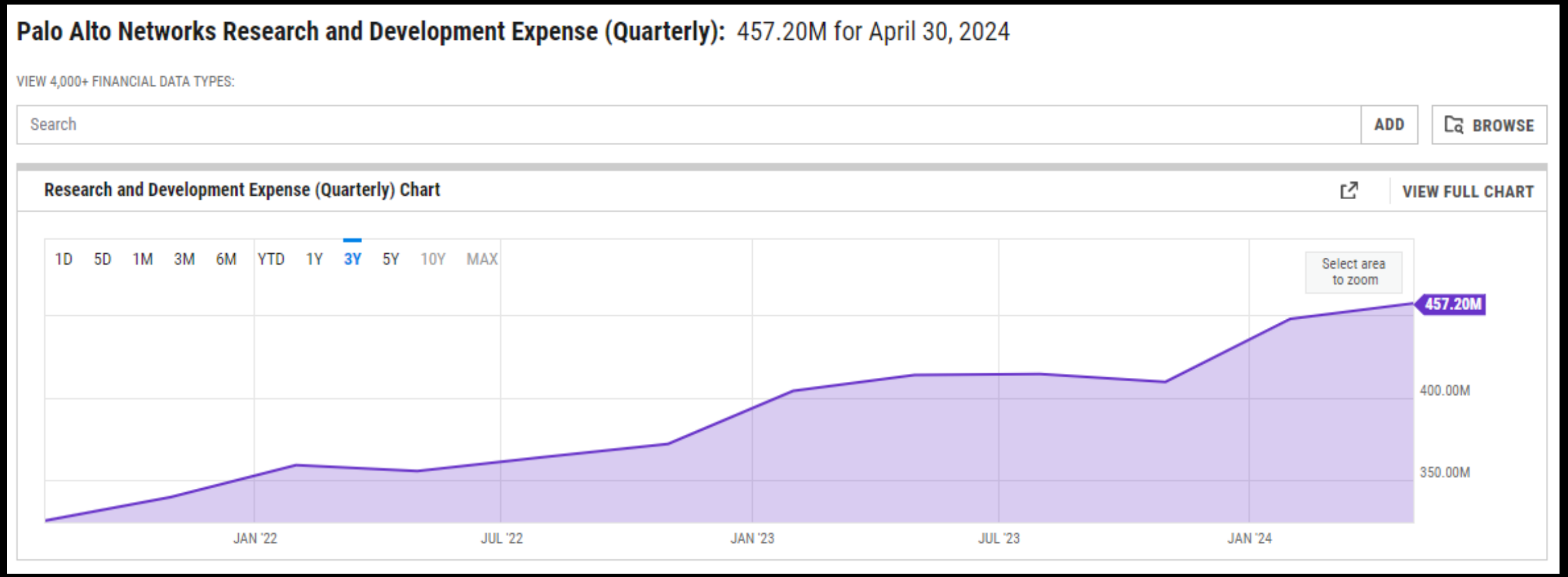
2 a 4 veces más de data colectada por cualquier otro vendor de ciberseguridad

paloalto NETWORKS

Nuestro ADN: Innovación y Desarrollo



La empresa de Ciberseguridad con mayor inversión en I+D



Fuente: https://ycharts.com/

La empresa de Ciberseguridad más grande del mundo

- Más de 19,000 empleados
- 13 Data Center a nivel global
- Presencia en 80% de las Global 2000
- Presencia en 94 de las Fortune 100
- Fundada el año 2007

SIMPLIFY SECURITY WITH OUR BEST OF BREED PLATFORMS

SUB-CATEGORY	NETWORK SECURITY PLATFORM
Firewall	Network Security Platform
Intrusion Prevention	
URL Filtering	
Sandbox	
DNS Security	
IoT / OT Security	
Data Loss Prevention (DLP)	
Cloud Access Security Broker	
Remote Browser Isolation	
Enterprise Browser	
Secure Web Gateway	
SD-WAN	
Remote Access	
Digital Experience Monitoring	
Posture and Health Management	

SUB-CATEGORY	CLOUD SECURITY PLATFORM
Cloud Security Posture Management	Prisma Cloud
Cloud Workload Protection	
Identity & Access Management	
Code Security	
Web Application / API Security	

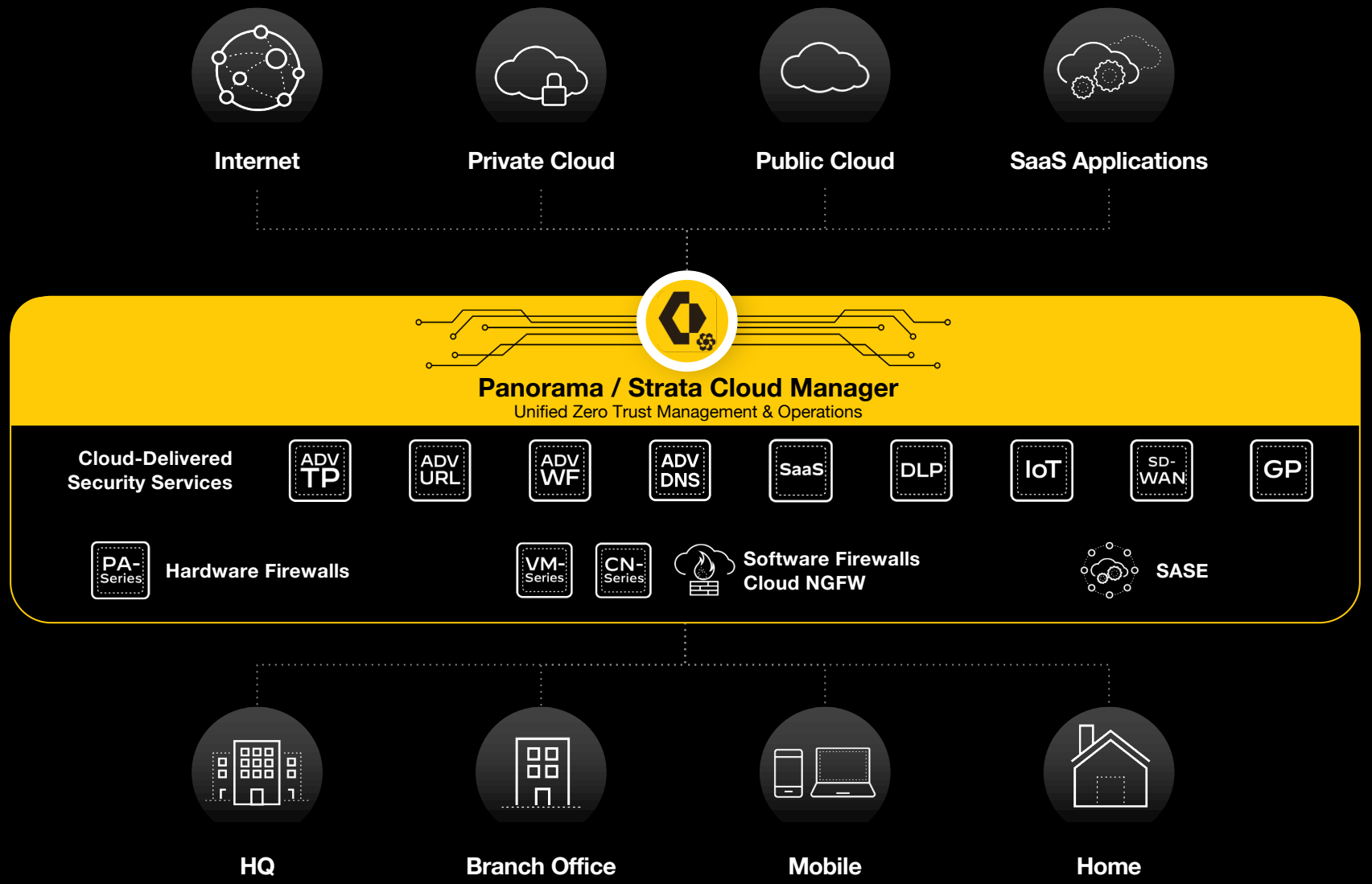
SUB-CATEGORY	MODERN SOC PLATFORM
Security Information & Event Management	Cortex
Endpoint + EDR	
NTA / UEBA	
SOAR	
Attack Surface Management	

Threat Intelligence and Advisory Services

World-renowned threat intelligence, cyber risk management and advisory services

paloalto NETWORKS

LA MEJOR PLATAFORMA DE SEGURIDAD DE RED



Unified Zero Trust Management and Operations

Industry's first AI-powered zero trust management and operations solution for your entire network security estate, preventing operational disruptions **up to 7 days in advance**

Best-in-Class Protection Delivered Everywhere

Inline AI-powered security services secure your entire network, **stopping 8.6B threats inline per day**

Industry-Leading Form Factors

11x leader for hardware and software firewalls in Gartner magic quadrant for NGFW and the **only leader** in SASE for Gartner magic quadrant for single-vendor SASE

paloalto NETWORKS

LA MEJOR PLATAFORMA PARA EL CIBERSOC

Endpoint Security, EDR, NDR, XDR, UEBA, SIEM, SOAR, ASM → **SOC AUTÓNOMO**

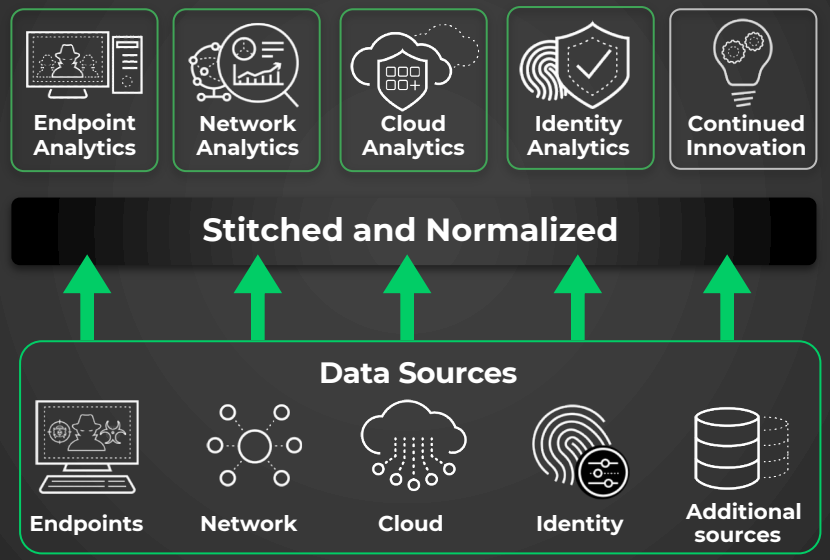
Cortex XPANSE

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



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**

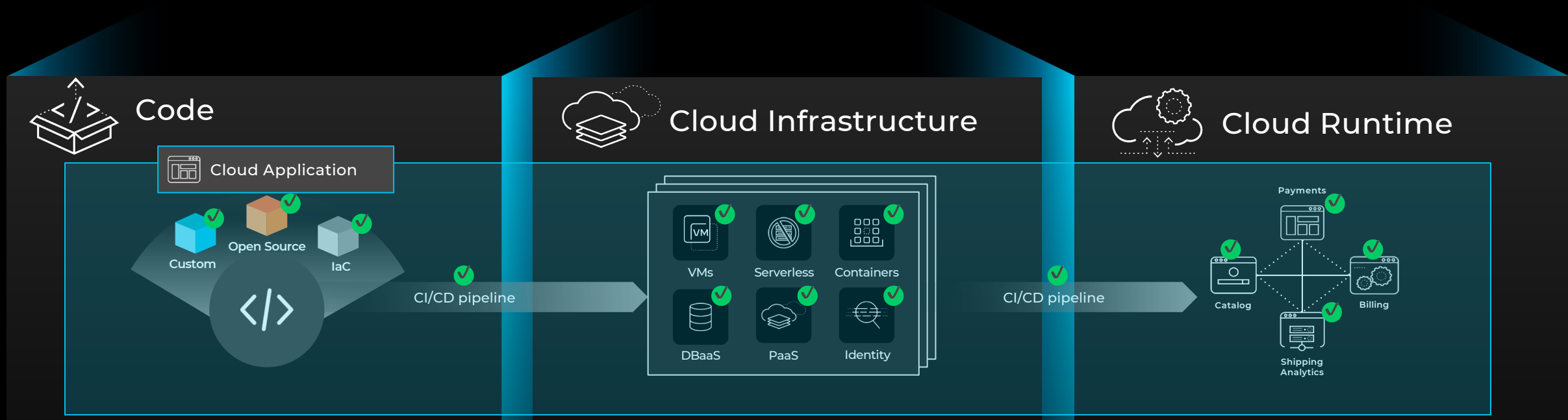
Cortex XSIAM

Unify SOC Operations with an integrated AI-driven platform

End-to-end workflow automation for security operations

paloalto NETWORKS | CORTEX

LA MEJOR PLATAFORMA PARA ASEGURAR LA NUBE



Risk Prevention

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

Visibility & Control

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

Runtime Protection

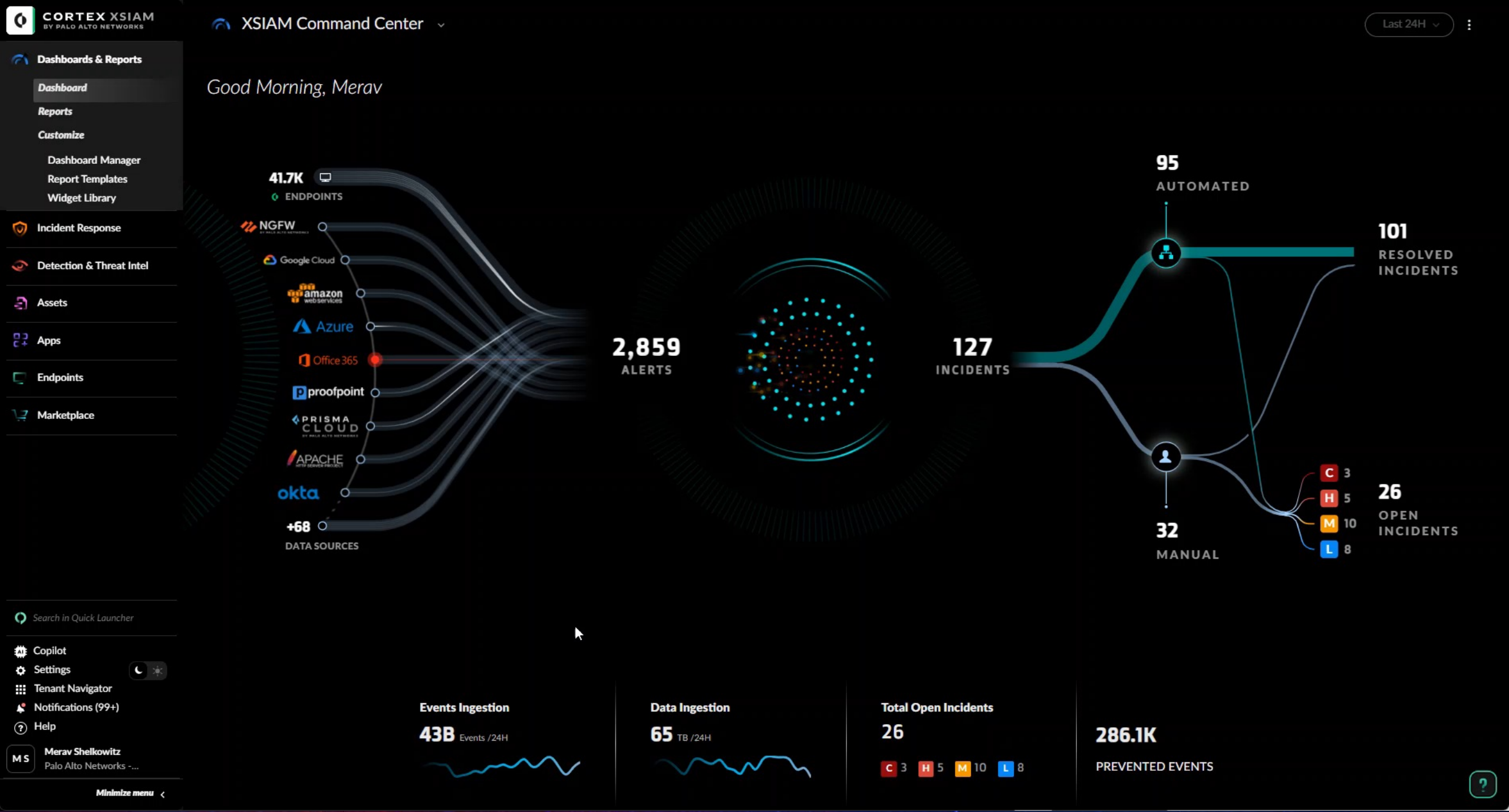
Proactive Runtime Detection and Prevention:
CWP, WAAS/WAF, CNS, CDR

Secure The Source

Secure The Infrastructure

Secure The Runtime

paloalto NETWORKS | PRISMA



The Golden Formula with Data and AI for Better Cybersecurity Outcomes

Integrated, Real-Time Telemetry Data

Networks Cloud Endpoints

+

ML / AI Driven Automation

Strata NGFW Cortex XSIAM Cortex XSOAR

=

Better Cyber Outcome

Risk **10** Efficiency

SECONDS

Mean Time to Detect

TCO **1** Simplicity

MINUTE

Mean Time to Respond
(High priority alerts)

paloaltonetworks.com