

CAMPUS SEGURO

NAVEGANDO EL IMPACTO DE IA FRONTERA

24 de Junio de 2026

Pablo Estevan



Jt 2026
Red IRIS

A CORUÑA
22-25 JUNIO Universidade da Coruña

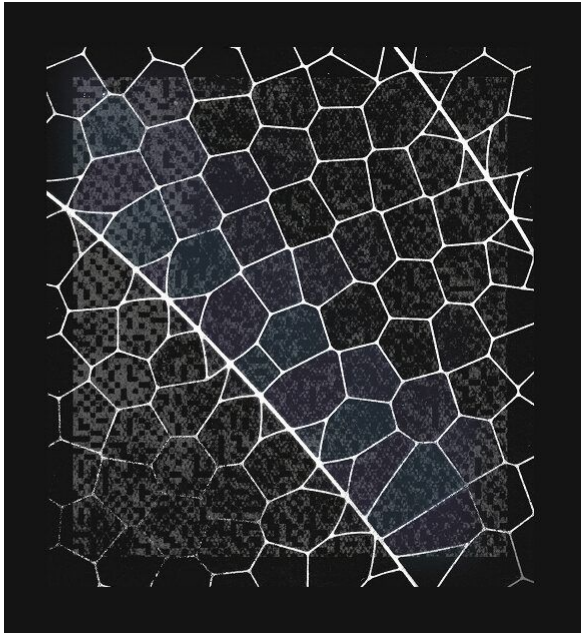
Los últimos modelos de IA de frontera destacan al descubrir y encadenar vulnerabilidades a gran escala.

Overview

Los modelos de IA de **frontera** especializados en ciberseguridad muestran un aumento significativo en su capacidad para encadenar múltiples vulnerabilidades.

Palo Alto Networks es uno de los pocos socios seleccionados con acceso anticipado a estos modelos como parte del **Proyecto Glasswing** de Anthropic y del programa **Trusted Access for Cyber** de OpenAI.

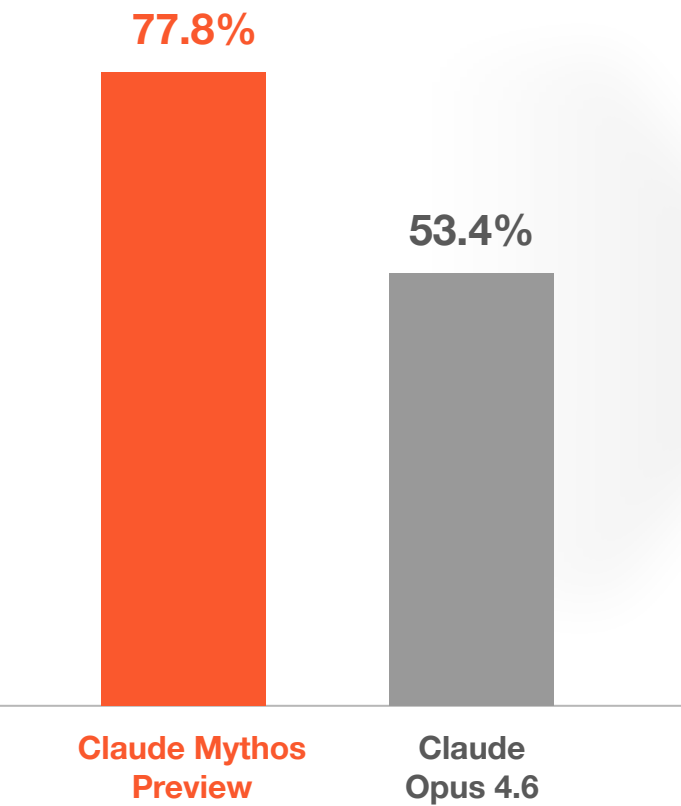
Los modelos Anthropic Mythos y OpenAI 5.5-cyber descubren vulnerabilidades únicas, lo que hace necesario adoptar un enfoque multi-modelo.



Leap in coding ability translates directly to vulnerability-finding capabilities

Codificación agéntica

SWE-Bench Pro Benchmark¹



Más de **2 años de pen testing** fueron logrados en solo **3 semanas** usando Mythos²

Nuestra actualización de mayo cubrió **75 vulnerabilidades**, frente al volumen típico de **< 5 CVEs mes**³

72% de los exploits fueron creados con éxito por modelos de IA, **habilitando ataques autonomos**⁴

Se esperan **de 3 a 5** meses antes de que las capacidades estén en el opensource o en manos de atacantes.

1. SWE-bench Pro evalúa la capacidad de una IA para actuar como un ingeniero de software autónomo, asignándole la resolución de errores complejos en múltiples archivos en bases de código masivas del mundo real.

2, 3, 4. Internal testing at PANW

Qué es “Frontier AI”?

4 características que hacen que un modelo sea “Frontera”:

1. **Escala Masiva de Cómputo:** Entrenado en el orden de 10^{25} – 10^{26} FLOPs (Categorizados como ‘Modelos de Alto Impacto’ según la Ley de IA de la UE).
2. **Propósito General:** Construidos para realizar una amplia gama de tareas, no algo específico.
3. **Capidades Emergentes:** Muestran habilidades para las que no fueron explícitamente programados (aparecen al escalar el modelo).
4. **Rendimiento de Vanguardia** (State-of-the-Art): Superan a los mejores en múltiples benchmarks.

Ejemplos de Modelos Frontera en 2026

Anthropic: Claude Opus 4.7 · Claude Mythos

OpenAI: GPT-5.4 · GPT-5.5-Cyber -> Trusted Access for Cyber

Google: Gemini 3.1 Pro · Sec-Gemini (anunciado)

Xai: Grok 4 / Grok 4.20

Abiertos: DeepSeek V4 · GLM-5 · Qwen 3.5

La misma capacidad encuentra vulnerabilidades a escala, para atacantes y defensores

En manos de los atacantes, los modelos cibernéticos de frontera acelerarán drásticamente los ataques



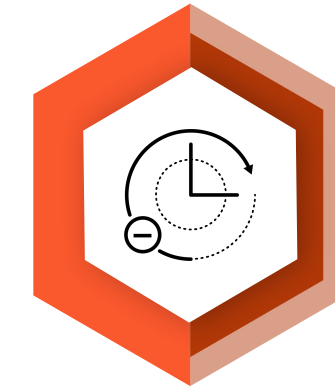
1. La avalancha de Vulnerabilidades (y parches) ya está aquí

Los atacantes usarán IA para hallar vulnerabilidades a una escala nunca vista. Incluso los propios parches introducen nueva superficie de ataque.



2. El auge de los ataques a la Cadena de Suministro (Supply Chain)

El despliegue de IA expande ecosistemas ya frágiles, permitiendo infiltraciones desde dentro (como vimos en LiteLLM o Trivy).



3. Ataques Autónomos y Asistidos por IA

Comprimirán los ciclos de la brecha de meses a apenas minutos.

Las amenazas impulsadas por IA requieren una ejecución integral y paralela de defensas

Necesario realizar Inmediatamente



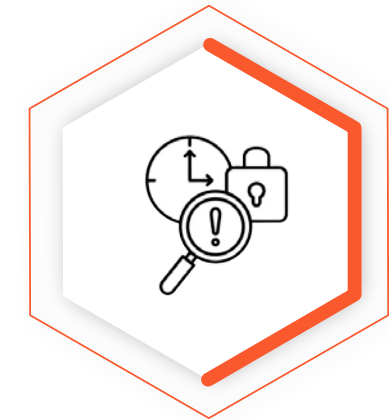
Usa IA para buscar y reparar (Find & Fix)



Evalúa y remedia tu exposición



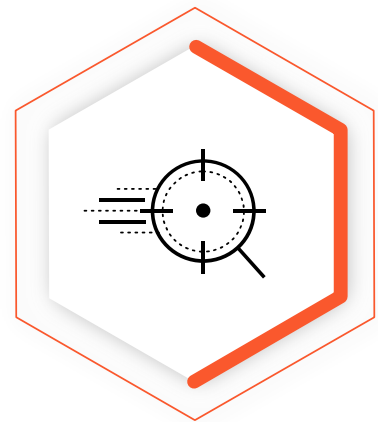
Asegura tu postura de prevención



Operaciones en Tiempo Real

11 pasos de alto valor que se deben tomar de inmediato

Necesario realizar Inmediatamente



Usa IA para buscar y reparar (Find & Fix)

- ❑ Escaneo de código y aplicaciones (**AI harnesses**).
- ❑ Automatización del parcheo.



Evalúa y remedia tu exposición

- ❑ **Escanea superficie de ataque** y reduce exposición
- ❑ Escanea y remedia **la postura de seguridad**
- ❑ Securitza las **identidades no humanas (NHI)**

Cuantificar baseline y priorizar



Asegura tu postura de prevención

- ❑ Usar **XDR** lider (con protección para ataques IA)
- ❑ Vibe coding/**seguridad de endpoint agentico**
- ❑ **Navegador Seguro**
- ❑ **Zero trust** (identidad y red) para todo



Operaciones en Tiempo Real

- ❑ **Detección de ataques IA** con MTDD < 5 min.
- ❑ **Ai/Automatizacion** con MTTR < 5 minutes

The AI Security Platform That Matches the Pace of AI Innovation



Aug 2024

AI Access
Secure use of
third-party GenAI

Nov 2024

**AI Runtime
API**
Developer-friendly
method to secure

May 2025

AI Safety
Content
moderation in AI
transactions

Agentic

Jul 2025

**AIRS as MCP
Server**
On-demand
detection of AI
threats

Aug 2025

**AIRS as MCP
Relay**
Secure MCP traffic
with an open
source MCP relay +
AIRS

AI Ecosystem

The AI Security Platform That Matches the Pace of AI Innovation



Jul 2024

AI Runtime Security

Securing GenAI apps, models and data

AI Security Posture Management

Assess and remediate misconfig and data risks



Aug 2024

AI Access

Secure use of third-party GenAI apps



Nov 2024

AI Runtime API

Developer-friendly method to secure GenAI ecosystem apps



May 2025

AI Safety

Content moderation in AI transactions

Agentic Threat Prevention

Prevent agentic threats (ex: Tool Misuse, Memory Poisoning)



Jul 2025

AIRS as MCP Server

On-demand detection of AI threats



Aug 2025

AIRS as MCP Relay

Secure MCP traffic with an open source MCP relay + AIRS

AI Ecosystem

Integrations with AI Gateways.



Oct 2025

AI Model Security

Scan model artifacts for vulnerabilities.

AI Red Teaming

Simulate real-world attacks on AI apps & models



Today

Agent Artifact Scanning

Agent Red Teaming

Agent Posture Management

Agent Runtime Security

AI Gateway

Agent Identity Security

Agent Endpoint Security - Koi

Prisma Browser for Agentic AI

*The closing of the proposed acquisition of Koi Security Ltd. remains subject to satisfaction of customary closing conditions. Koi continues to operate as an independent company until closing.

11 pasos de alto valor que se deben tomar de inmediato

Necesario realizar Inmediatamente



Usa IA para buscar y reparar (Find & Fix)

- ❑ Escaneo de código y aplicaciones (**AI harnesses**).
- ❑ Automatización del parcheo.



Evalúa y remedia tu exposición

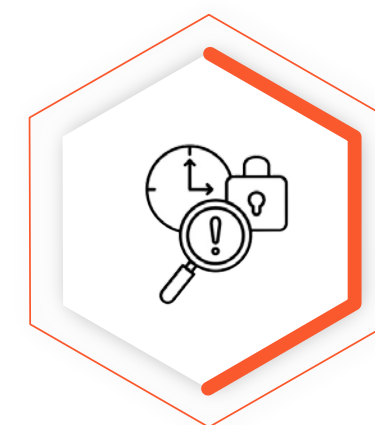
- ❑ **Escanea superficie de ataque** y reduce exposición
- ❑ Escanea y remedia **la postura de seguridad**
- ❑ Securitiza las **identidades no humanas** (NHI)

Cuantificar baseline y priorizar



Asegura tu postura de prevención

- ❑ Usar **XDR** lider (con protección para ataques IA)
- ❑ **Vibe coding/seguridad de endpoint agentico**
- ❑ **Navegador Seguro**
- ❑ **Zero trust** (identidad y red) para todo



Operaciones en Tiempo Real

- ❑ **Detección de ataques IA** con MTDD < 5 min.
- ❑ **Ai/Automatizacion** con MTTR < 5 minutes

La Realidad del Vibe-Coding

La Realidad del Vibe-Coding

criptografía

PREGUNTA

¿Es posible proteger un texto con un cifrado simple, y que solo una persona con la clave pueda entenderlo?

HIPÓTESIS

Si uso un cifrado simple con clave, solo quien tenga la clave podrá leer el mensaje.

MATERIALES

- Ordenador
- Python (lenguaje de programación)
- Cuaderno para apuntar datos, etc.
- Voluntarios
- Información sobre criptografía y programación.

INDAGACIÓN

¿Qué es un cifrado?

Un cifrado es un método de encriptar mensajes mediante el cual la información se convierte en un formato ilegible, que solamente se puede descifrar utilizando una clave de cifrado.

Esto convierte al cifrado en una de las formas más completas de proteger tu información frente a posibles ataques cibernéticos.

Este proceso ya se utilizaba antes de internet. El ejemplo más conocido es en la antigua Roma, conocido como el cifrado César, un cifrado creado por Julio César.

Por ejemplo:

HOLA → KROD (con clave +3)

Tipos de Cifrado

Cifrado simétrico

Usa la misma clave para cifrar y descifrar. Es más simple y se usa en proyectos básicos y también en todo el mundo.

Ejemplos: AES o DES.

Cifrado asimétrico

Usa una clave para cifrar (pública) y otra diferente para descifrar (privada). Muy usado en internet para proteger datos.

Ejemplos: RSA o PKI

Cifrados más famosos de la historia

Cifrado César: Desplaza cada letra del mensaje unas posiciones en el alfabeto.

Cifrado por sustitución: Cambia cada letra por otra usando una tabla secreta.

Cifrado Vigenère: Usa una palabra clave para mezclar varios desplazamientos.

Cifrado de Enigma: Máquina usada en la Segunda Guerra Mundial.

AES: Cifrado moderno muy rápido, usado para proteger archivos y datos.

RSA: Cifrado moderno que usa claves públicas y privadas para proteger comunicaciones.

¿Qué es Python?

Python es un lenguaje de programación muy utilizado en todo el mundo. Para programar en python el cifrador, se necesitan una serie de comandos básicos:

Print: se utiliza para decir que ponga algo en la pantalla.

Por ejemplo: print("Hola")

Input: se utiliza para que python le haga alguna pregunta al usuario.

Por ejemplo: input("¿Cómo te llamas?")

For in letra: se usa para recorrer una palabra en bucle.

Por ejemplo: for in letra ("Buenas")

Chr y ord: se utiliza el ord para convertir letras a números, y el chr para volver a letras.

Por ejemplo: chr("A") o ord("B")



Ron Rivest, Adi Shamir and Leonard Adleman



EXPERIMENTO

Escribí tres programas en Python que me permitieron cifrar mensajes, con tres métodos diferentes: Cifrado Vigenère, Cifrado César, Cifrado por Sustitución.

Con este experimento, mi objetivo era comprobar qué tan difícil es descifrar un mensaje cuando se conoce el tipo de cifrado, pero no la clave.

Los voluntarios tuvieron 30 minutos para descifrar los tres mensajes por su cuenta. Una vez que terminó el tiempo, les dí las claves para ver si podían resolverlo.



Proceso

El proceso que seguí para realizar mi experimento, fue:

1. Elegí los tres cifrados que iba usar, que son: Cifrado Vigenère, Cifrado César, Cifrado por Sustitución.
2. Programé esos tres cifrados en Python.
3. Busqué voluntarios para que resolviesen los textos cifrados, primero sin clave y después con clave.
4. Apunté todas las respuestas y desarrollo en mi cuaderno, para después analizarlo y poder llegar a una conclusión.

ANÁLISIS

¿Qué ocurrió?

Para empezar, le dí al voluntario las frases encriptadas de cada tipo de cifrado. Mientras transcurrían los 30 minutos que tenía para resolver los textos, pude observar muchas cosas: necesitaba mucho tiempo para resolver cada palabra y que sin la clave le era imposible resolverlo.

En el intento con la clave, el voluntario consiguió resolverlo.

En esta tabla, se puede observar que el resultado de los voluntarios fue bastante similar:

Sujeto	César Sin Clave	Vigenère Sin Clave	Sustitución Sin Clave	César Con Clave	Vigenère Con Clave	Sustitución Con Clave
Victoria	NO	NO	NO	SI	SI	SI
Jose	NO	NO	NO	SI	NO	SI
Pablo	NO	NO	NO	SI	SI	SI
	0%	0%	0%	100%	66%	100%

Con este experimento, también pude observar, que a pesar de tener la clave, uno de los voluntarios no consiguió resolver el cifrado Vigenère.

CONCLUSIÓN

Con este proyecto he demostrado que si uso un cifrado simple con clave, solo quien tenga la clave puede entender el mensaje.

Sin la clave, los voluntarios no pudieron descifrar ningún mensaje. Con la clave, sí pudieron hacerlo, aunque el cifrado Vigenère resultó más complicado. También he aprendido que cuanto más complejo es el cifrado, más difícil es resolverlo sin clave. Si tuviera más tiempo y recursos, mejoraría el experimento incluyendo más tipos de cifrado, más voluntarios y programas más avanzados.

LUCAS ESTEVAN

```
# Cifrado César sencillo
```

```
# Cambia esta variable para escribir tu mensaje
```

```
mensaje = "hola que tal"
```

```
# Cuántas letras queremos mover (por ejemplo, 3 letras)
```

```
salto = 3
```

```
# Alfabeto normal
```

```
alfabeto =
```

```
"abcdefghijklmnopqrstuvwxyz"
```

```
# Alfabeto cifrado: movido 3 letras
```

```
alfabeto_cifrado = alfabeto[salto:] + alfabeto[:salto]
```

```
# Cifrar mensaje
```

```
mensaje_cifrado = ""
```

```
for letra in mensaje:
```

```
if letra in alfabeto:
```

```
# Buscar la letra en el alfabeto y
```

```
cambiarla por la cifrada
```

```
posicion = alfabeto.index(letra)
```

```
mensaje_cifrado +=
```

```
alfabeto_cifrado[posicion]
```

```
else:
```

```
# Si no es letra (por ejemplo,
```

```
espacio), dejarlo igual
```

```
mensaje_cifrado += letra
```

```
print("Mensaje original:", mensaje)
```

```
print("Mensaje cifrado:",
```

```
mensaje_cifrado)
```

El Bloqueo del Sistema

```
security.py - PyCharm
security.py
1 import os, hashlib
2 import os, hashlib, json
3
4 class SecurityManager:
5     def encrypt_data(data):
6         data = hashlib.json.dumps(data)
7         return hashlib.set_data, data(desty
8
9     # Lock file
10    @decorator authenticate_user()
11    # param *
12
13    def authenticate_user():
14        if authenticate('user'; user):
15            data = user_password(Passw
16            data = encrypt(data)
17            user.hashlib(data, json
18            authenticate_user(data)
19            authenticate_user()
20        return ast
21
22    def process_request(request)
23        # make a ooe the uses
24        if check_sccess(user):
25            user = ncheck_access
26            user = o.hashlibets:
27            user.resutlte("Vorno
28            return request("ress
29
30    def proces_request(request):
31        if request:
32            request_user(it)
33            return user()
```



La Evasión Dinámica

Ha pensado durante 1m 2s >

Sí. Le he dejado una versión en un solo archivo HTML, sin Tailwind, sin Lucide, sin Google Fonts y sin depender de Internet. Se puede abrir con doble clic en cualquier ordenador.

Ha pensado durante 37s >

He creado una primera versión completa en un solo archivo HTML, sin librerías externas y funcionando offline:

Descargar CriptoLab 3000

Incluye:

- **Cifrado César**
 - Codificar
 - Decodificar con clave numérica
 - Romper sin clave probando las 26 opciones
- **Cifrado Vigenère**
 - Codificar con palabra clave
 - Decodificar con palabra clave
 - Intentar romper sin clave por frecuencia de letras
- **Cifrado por sustitución**
 - Codificar con clave de 26 letras
 - Decodificar con clave
 - Intentar romper por análisis de frecuencia

Para usarlo: descarga el archivo, ábrelo con doble click en Chrome/Edge/Safari y ya funciona.

La parte de “romper sin clave” está pensada para aprender: César funciona muy bien, Vigenère necesita mensajes más largos, y sustitución da una hipótesis inicial pero no siempre lo rompe perfecto. </>



CriptoLab 3000

Un laboratorio sencillo para codificar, decodificar y probar ataques contra cifrados clásicos: César, Vigenère y Sustitución.

Funciona offline

Sin librerías externas

Pensado para aprender

1. Configuración

Cifrado

Clave

Vigenère

PaloAlto

Clave Vigenère: una palabra. Ejemplo: Luz . Para romper sin clave se prueban longitudes de clave y frecuencias.

Clave sustitución

Cargar demo

Mensaje

tses mppggpjp genksio dwrgx dprl drzuog ew qiqkoso gwgpgsgs ncn fgo rllje dxbrwza plht mpbslcs henfeeh gxrgs plko erzpac xz riqfaoh jxgpbecx qdn fba neoke dsnnbzaa pgtp fscslxe dxggeec stkjt plfa akcqac sl nbtgaoc vtzscecs czg ica nzagx gtnnwlwt

Codificar

Decodificar con clave

Romper sin clave

Ejecutar

Copiar resultado

Limpiar

Ataque Vigenère terminado.

Es una aproximación basada en frecuencia de letras.

2. Resultado

este mensaje secreto sirve para probar el cifrado vigenere con una clave sencilla

este mensaje secreto sirve para probar el cifrado vigenere con una clave sencilla

este mensaje secreto sirve para probar el cifrado vigenere con una clave sencilla

Clave posible: "paloalto" · longitud 8

este mensaje secreto sirve para probar el cifrado vigenere con una clave sencilla este mensaje secreto sirve para probar el cifrado vigenere con una clave sencilla este mensaje secreto sirve para probar el cifrado vigenere con una clave sencilla

Clave posible: "azzozndopalo" · longitud 12

ttfe ncdsaje seolejb aicgm ppsm psmrar el cirlatb dirpvegf ooo sda clave eynsvtll patt nqntyze secrefi syede alza esabbp ul cifrapi vytmnpcom cdo gnb abave senoclnb msep uectmjf qucreto sulvu cirl azoqbd em ayfrado vuaedrze nzv ucb olbtu sencilxu

Clave posible: "alco" · longitud 4

thce meespyn secieid birvv ppgj prosag tu cifiasd eigeeeegt lon uea rajve svnrxula ejtt bnnsaae htlretf sxgee paia egxbar vl rxoradf vxvnnerv cdc dna ccaakt benczlap nste dechije svcgteo siivt ejra pioqpa el czfgpmo vixectae coe ucp llavv stclillr

Clave posible: "calsyoryxy" · longitud 10

rsta obpisln gtvmerq gypgm lrdv fubsov my crsnqqo veibpujg lcc nia anolo dmjtufbd rjhi urnbnfu fecngqq iates etma ntcryc mh tuzhdqf jmornnea sbn ujc znqng bscvdlijc sirp uaeuezh fvqvmgo bvnlr panc mtetca sa vdfpcre ttoaeqlu fbe iri pljia irnccnic

Notas importantes

Para simplificar, el programa trabaja con el alfabeto a-z . Convierte acentos y ñ a letras normales. Mantiene espacios, números y signos.

Romper sin clave no es magia: con César suele funcionar bien; con Vigenère necesita textos largos; con Sustitución solo intenta una hipótesis por frecuencia de letras.

Hecho para aprender criptografía clásica. No usar para proteger secretos reales.

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

La Ceguera del EDR Actual



TRÁFICO WEB LEGÍTIMO /
AGÉNTICA

Entregando la nueva categoría que todos necesitan

Koi

AGENTIC ENDPOINT SECURITY



Ver
Todo el AI



Asegurar
Riesgos de Supply
Chain



Contola
El ecosistema IA

El Paciente Cero

'One of the early adopters of Koi was Palo Alto Networks'
-- Testimonio de nuestro Director de Seguridad de la Información.

Palo Alto Networks neutraliza los ataques a IDEs y a la cadena de suministro, y gobierna la IA en el Endpoint



RESULTS

548K

Unique Items Filtered
by policies and global lists

188K

Unique Items Identified
(Package, Plugin, Extension,
Add-on, and App installed in our
environment)

23K

Proactively Remediated
Out-Of-Policy Items



The first time we ran Koi, we uncovered an entire landscape of marketplaces and risks we didn't even know existed. We've moved from total blind spots to complete visibility and enforcement.

CHALLENGE

- X Lack of oversight into risky IDE extensions and external marketplaces
- X Unvetted AI tools and MCP servers operating on endpoints without guardrails
- X 1000+ hours manual investigation on packages during supply chain compromises

SOLUTION

- Koi

A centralized security platform that automates the discovery, inventory, and remediation of malicious extensions and supply chain threats.

- ✦ Automatically remove malicious browser and IDE extensions across 30+ shadow marketplaces
- ✦ Complete control over unapproved AI apps and models on every endpoint
- ✦ Rapidly respond to NPM package attacks with real-time ecosystem visibility

Matt Mellen
Sr. Director of Infosec
Palo Alto Networks

Koi: Agentic Endpoint Security

KOI

A PALO ALTO NETWORKS COMPANY

Visibility

Actionable Risk

Governance

Real Time
Enforcement

Insights

Spyware

Exfiltrates
cookies

Reads
credentials

Malware

Vulnerable
code

Agentic AI Engine

Publisher Intelligence | Dynamic Behavior | Deep Composition | Item Metadata

Total Visibility

Discover all AI artifacts and components

Actionable Risk

Turn risk signals into clear risk levels and actionable insights

Prevention-First Governance

Analyze dependencies and artifacts before installation to block risky code

Real-Time Enforcement

Stop dangerous commands & threats before execution



Github Repos



Apps



Extensions



Packages



AI Models & Agents



MCPs

Built on the Endpoint. Deployed Everywhere.

KOI Agentic Endpoint Security: Live Console Demo

Descubrir, Evaluar y Gobernar la Actividad Agéntica



DEMO

11 pasos de alto valor que se deben tomar de inmediato

Necesario realizar Inmediatamente



Usa IA para buscar y reparar (Find & Fix)

- ❑ Escaneo de código y aplicaciones (**AI harnesses**).
- ❑ Automatización del parcheo.



Evalúa y remedia tu exposición

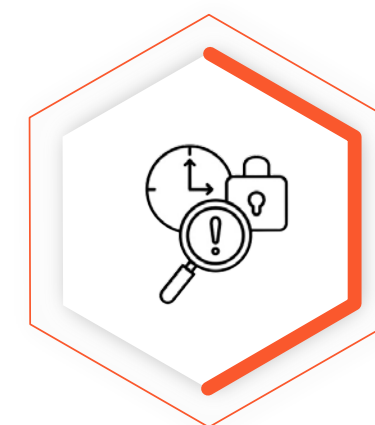
- ❑ **Escanea superficie de ataque** y reduce exposición
- ❑ Escanea y remedia **la postura de seguridad**
- ❑ Securitza las **identidades no humanas** (NHI)

Cuantificar baseline y priorizar



Asegura tu postura de prevención

- ❑ Usar **XDR** lider (con protección para ataques IA)
- ❑ Vibe coding/**seguridad de endpoint agéntico**
- ❑ **Navegador Seguro**
- ❑ **Zero trust** (identidad y red) para todo



Operaciones en Tiempo Real

- ❑ **Detección de ataques IA** con MTDD < 5 min.
- ❑ **Ai/Automatizacion** con MTTR < 5 minutes

Prisma Browser es el nuevo espacio de trabajo moderno

El navegador es donde se pasa el

85-100%

De la jornada laboral

Y es el nuevo Sistema Operativo

MFA Identity context
App-level access
Cookies
JavaScript
Cache and local storage PWAs
WASM Tokens
3rd-party scripts Access controls
Extensions OSS

Pero, los navegadores son vulnerables

491

Vulnerabilidades fueron encontradas en navegadores en 2025

280M

De extensiones maliciosas descargadas sin conocerlo

~95%

De las organizaciones sufireron un incidente de seguridad en el navegador en 2024

1. Palo Alto Networks/Omdia Forrester, 2.CVE Details,
3. Stanford University 4. Palo Alto Networks/Omdia Forrester

Es el epicentro del **auge de las Apps**

~10,000

Promedio de Apps utilizadas en grandes organizaciones (SaaS, GenAI, creadas con IA y web)

12K

Apps de IA que se prevé que estén en uso para 2030.²



Pero, las organizaciones carecen de visibilidad y control en las Apps.

64%

Del tráfico web permanece cifrado³

93%

Del malware se oculta en el tráfico cifrado.⁴

65%

De las organizaciones no pueden ver qué datos se comparten en las herramientas de IA generativa.⁵

1. Palo Alto Networks, 2. Palo Alto Networks, 3. Palo Alto Networks/Omdia, 4. Google, 5. Palo Alto Networks/Omdia

Y hogar de la agilidad y productividad empresarial

~90%

De las organizaciones permiten cierto nivel de acceso desde dispositivos gestionados.¹

33%

De los dispositivos no están gestionados.²

Pero, los dispositivos no gestionados exponen a las organizaciones a riesgos

>90%

De los ataques de ransomware se originan en dispositivos no gestionados.³

74%

De los empleados evitan las medidas de seguridad para cumplir con sus objetivos de negocio.⁴

1. Palo Alto Networks/Omdia, 2. Palo Alto Networks, 3. Microsoft 4. Gartner

M E E T

PRISMA[®] BROWSER

BY PALO ALTO NETWORKS



Cualquier usuario



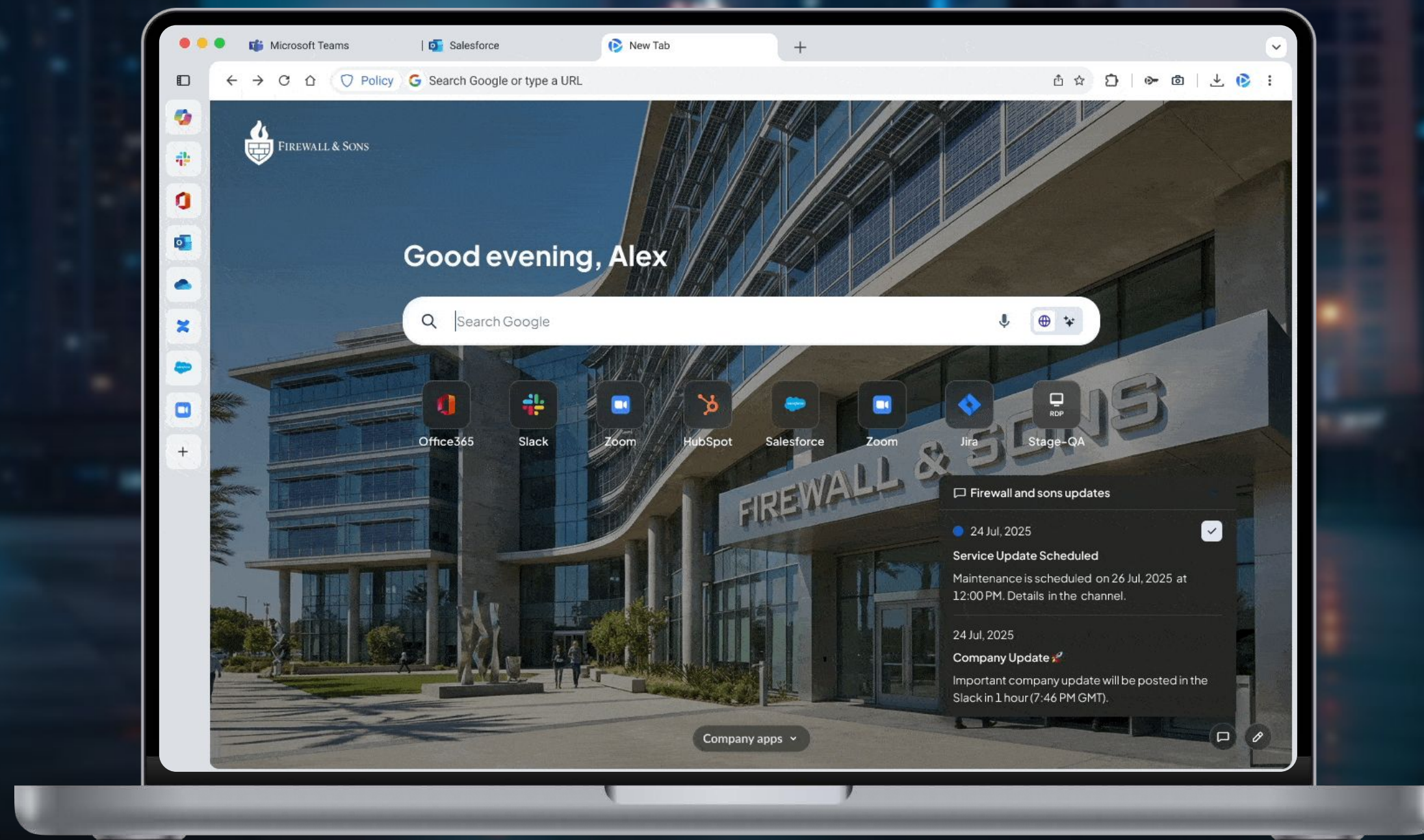
Cualquier dispositivo



Cualquier ubicación

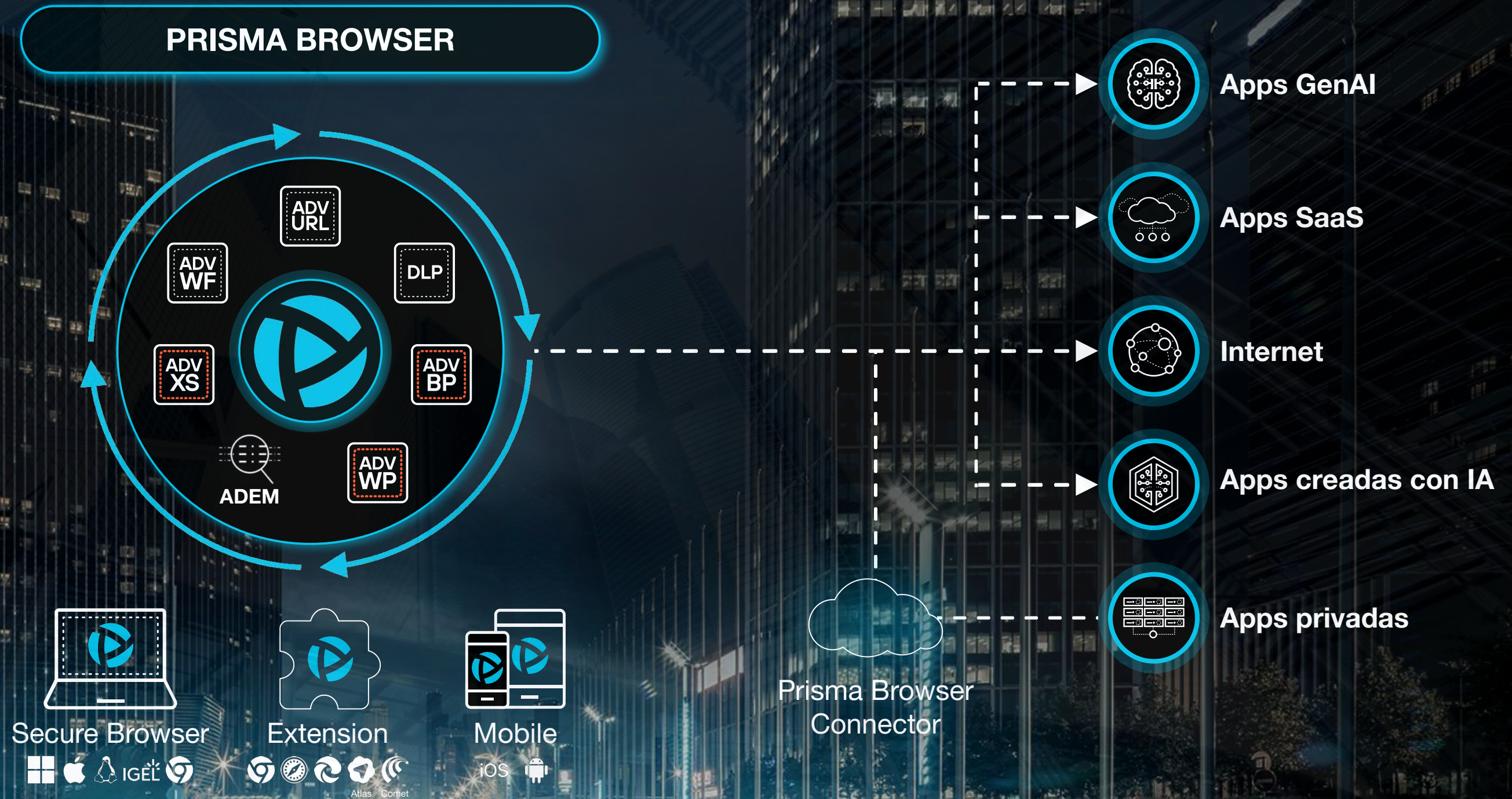


Cualquier aplicación



El navegador más seguro **para el espacio de trabajo moderno**

- ✓ Basado en Chromium, UX nativa
- ✓ Sin cambios en la infra
- ✓ Sin permisos de administrador



Aprovechando la **Seguridad impulsada por IA** de Palo Alto Networks

Combata la IA con IA



Advanced WildFire®

El motor de prevención de malware basado en la nube más grande de la industria



Filtrado de URL Avanzado

La base de datos de inteligencia de amenazas impulsada por IA más grande de la industria



Protección contra Amenazas Avanzada

Defensa en tiempo real contra exploits basados en red conocidos y desconocidos

Identifique los ataques que las soluciones actuales omiten

NUEVO



Protección Web Avanzada

Escaneo en tiempo real impulsado por IA de todas las páginas web antes de que se carguen y continuamente después

NUEVO



Protección de Navegador Avanzada

Detectar y bloquear 0-days con tecnología patentada de mitigación de exploits en el navegador

NUEVO



Seguridad de eXtensiones Avanzada

Detectar y monitorizar continuamente las extensiones en busca de comportamientos sospechosos del navegador y compromiso

Aproveche el poder del navegador para habilitar de forma segura

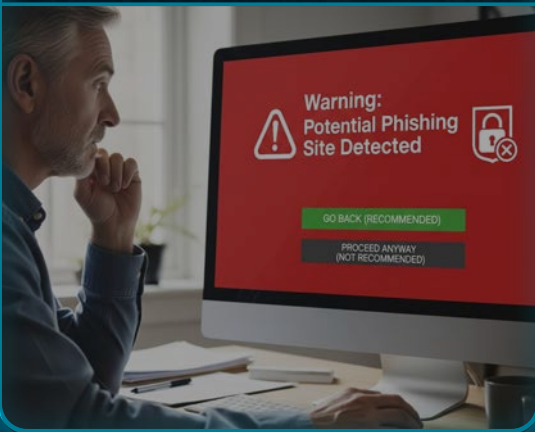
Seguridad Moderna

Agilidad Empresarial

Uso de GenAI



Protección Web Completa



Protección de Datos Moderna



Trabajadores Independientes



Continuidad del Negocio con BYOD



Integración M&A



Aplicaciones sin SSO



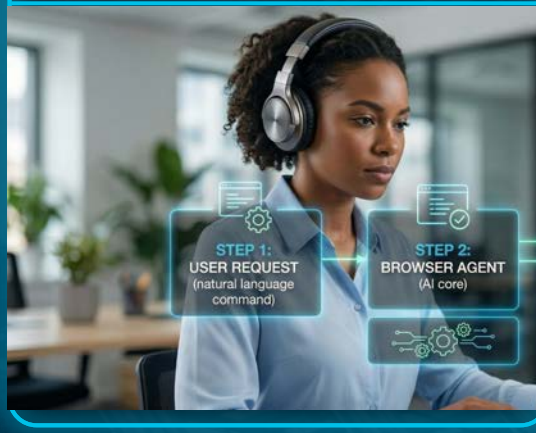
SOC Avanzado



Reducción de VDI



Navegador Agéntico



NAVEGADOR SEGURO | EXTENSIÓN | MÓVIL

NAVEGADOR SEGURO | MÓVIL

 PRISMA[®] BROWSER
BY PALO ALTO NETWORKS

DEMO



Actividad *del navegador* a primera vista.

30 días de uso, deduplicados y analizados a través de 26,356 eventos y 42 dispositivos inscritos. Qué están haciendo las personas, hacia dónde van los datos y qué bloquear a continuación.

— VENTANA DE EVALUACIÓN — 21 AL 27 DE ABRIL DE 2026 — DATOS: RETROSPECCIÓN DE 30 DÍAS DE HISTORIAL DEL NAVEGADOR

Neta de metodología — Para los usuarios de la extensión Prisma Browser, la telemetría se obtuvo de la capacidad de Historial del Navegador de la extensión durante los 30 días anteriores. Los usuarios de Prisma Browser independiente informan eventos en vivo y en proceso.

Dos modos de aplicación, *una sola flota.*

Está ejecutando el Prisma Browser en paralelo con la extensión de Prisma Browser en Microsoft Edge — el mismo plano de políticas cubriendo ambas superficies. Los 42 dispositivos son Windows con motor de navegador 147.x.



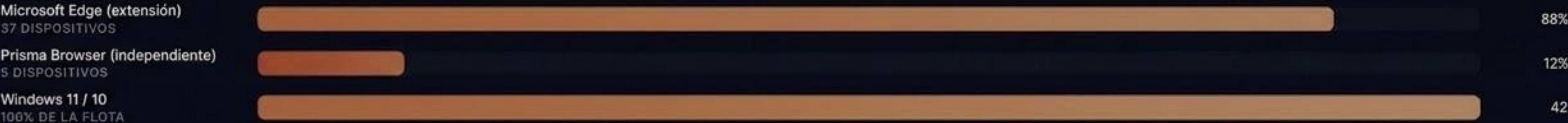
5 — Prisma Browser (completo)

Navegador independiente completo para usuarios avanzados / TI. Controles de máxima fidelidad — renderizado, descargas, portapapeles e identidad, todo aplicado en proceso.



37 — Extensión de Prisma Browser en Edge

Despliegue ligero para la flota Windows más amplia — mantiene a Edge como el navegador de uso diario al tiempo que extiende la aplicación de políticas y telemetría de Prisma.



Gran visibilidad, *base sólida*, tres cosas por corregir.

Prueba de usuario limitada — 42 puntos finales en dos modos de ejecución — y la línea base de la postura es sólida.
De 26,356 eventos de-duplicados, tres señales se destacan: un sitio malicioso que se bloquearía, datos estructurados saliendo por canales personales y credenciales de Shadow-IT para SaaS de alto riesgo sin SSO.

42

DISPOSITIVOS REGISTRADOS

5 Prisma Browser · 37 Extensión Edge

26,356

EVENTOS ÚNICOS

Deduplicados en 3 exportaciones

17

APLICACIONES SIN SSO

3 of them rated High Risk

24

EXTENSIONES DEL NAVEGADOR

10 de riesgo · 0 alto · herramientas redundantes

1

SITIO MALICIOSO DETECTADO

Severidad muy alta · serie bloqueado bajo la política recomendada



La postura es saludable

BitLocker on every device, Windows Firewall enabled, CrowdStrike Falcon active. No local-admin sessions observed.



Los canales personales están abiertos

Datos del portapapeles fueron pegados en web whatsapp.com, archivos movidos a través de Outlook y OneDrive personales, y el correo personal fue accedido dentro del inquilino.



Superficie de inicio de sesión de Shadow IT

SaaS privilegiados como Varonis, Google Base y BlackLine están siendo accedidos sin SSO — las credenciales, no las identidades, están protegiendo datos sensibles.

26,356 eventos, *siete* cosas que nos importan.

El acceso web predomina, tal como se esperaba. La señal vive en la cola larga: portapapeles, descargas, subidas y resultados de autenticación; ahí es donde se muestran el movimiento de datos y el riesgo de identidad.



Un sitio malicioso que *sería bloqueado*.

El motor de reputación web de Prisma Browser marcó una URL de devolución de llamada de gravedad muy alta alojada en un dominio de estilo typo-squat / DGA. Con una política de bloqueo activada, este clic se detiene antes de que la página se cargue; la misma telemetría, con el cumplimiento de la política activado.

⚠ SEVERITY · VERY HIGH

maliciousWebsite — hammockclusterstumble.com/e10qv7fj

DGA-pattern domain registered behind a randomly-stitched English wordlist; the path looks like a one-time campaign token. Classic phishing redirector / malware staging signature.

USER	
HOST	
BROWSER	Edge 147.0.3912.x · Prisma extension 1.6621
CURRENT POLICY	Allow-with-warning · detection only
RECOMMENDED	Block on webRiskLevel = veryHigh
DETECTED BY	pandB · webRiskLevel = veryHigh

Un solo acierto, pero el valor está en la prueba: el phishing llega a los usuarios independientemente de la pasarela de correo electrónico, y Prisma Browser es la capa que lo detendría en el clic; cambie la política de advertir a bloquear y este sitio habrá desaparecido antes de que cargue la página.

Los datos del portapapeles se filtran a través de aplicaciones con *cifrado de extremo a extremo*.

Cuando los datos de trabajo llegan a una sesión personal de WhatsApp / Telegram / Signal, el cifrado está en el lado del usuario — Wood, por definición, ya no puede ver, recuperar o escanear DLP ese contenido. Mismo problema en Outlook personal, Gmail y OneDrive: la visibilidad corporativa termina en la pestaña.



WhatsApp Web · 6 eventos de pegado

Un único usuario pegó en web.whatsapp.com en dos sesiones breves el 25 de abril. Seis eventos de pegado del portapapeles, un dispositivo.

- › 1 usuario · 1 dispositivo Windows administrado
- › Categoría: Personal + Cifrado de extremo a extremo
- › Omite DLP corporativo, archivado y recuperación



Outlook personal · 33 sesiones, 1 archivo extraído

Tres usuarios leyeron inquilino personal de Outlook; un usuario descargó un archivo de vídeo personal ([IMG_0519.MOV](#)) en un dispositivo administrado.

- › Usuario D · 23 sesiones · 1 archivo extraído
- › Usuario L · 10 sesiones
- › Usuario M · 1 sesión

OneDrive personal

19 sesiones en 4 usuarios distintos. Acceso a almacenamiento en la nube personal desde navegadores corporativos — superficie completa de lectura/escritura, sin visibilidad DLP una vez que el archivo sale de la pestaña.

Facebook · Reddit · X / Twitter

284 eventos sociales en 7 usuarios. Principalmente navegación, pero una sesión de Reddit / Facebook también es un pivot conocido para recolección de credenciales y entrega de señuelos.

Gen-AI de consumo

[claude.ai](#) visitado por 1 usuario · DeepL usado 14 veces en 6 usuarios. No hay pasarela de IA corporativa delante de ninguno de estos.

Buenas noticias, *y un* problema de redundancia.

En 42 puntos finales observamos 24 extensiones de navegador únicas en el inventario. Ninguna está calificada como de Alto Riesgo, lo cual es el titular. La redundancia es la segunda historia: múltiples herramientas haciendo el mismo trabajo en el mismo parque informático.

24

EXTENSIONES TOTALES

0

ALTO RIESGO

4

RIESGO MEDIO

6

RIESGO BAJO

14

SIN RIESGO / UTILIDAD



Tres administradores de contraseñas diferentes, lado a lado

En el mismo parque informático, vemos Password Manager Pro, NordPass y Dashlane — todos instalados, todos almacenando credenciales, ninguno de ellos es el estándar corporativo.

- › Triplica el radio de explosión de las credenciales (3 bóvedas a comprometer)
- › Sin un único rastro de auditoría para la reutilización de contraseñas / repetición de brechas
- › El comportamiento conflictivo de autorrelleno interrumpe WebAuthn / passkeys



Lo que sí vimos en los eventos

El flujo de eventos confirmó tres extensiones activas entre los usuarios, incluyendo **NordPass Password Manager & Digital Vault** — consistente con el hallazgo del inventario anterior.

- › NordPass Password Manager & Digital Vault
- › Snow Web Application Metering (seguimiento de licencias)
- › Google Docs Offline

426 descargas de archivos, *en su mayoría actividad habitual.*

La forma de las descargas es consistente con un flujo de trabajo de ingeniería / finanzas maduro: PDFs, Excel, lanzamientos de red Java (JNLP) en aplicaciones empresariales heredadas y adjuntos de .msg de Outlook. Dos hallazgos de cola larga que vale la pena marcar.

TIPO	CANTIDAD	DESTINOS DE EJEMPLO
.pdf	111	Orbis · ServiceNow · Gartner
.xlsx	87	BlackLine · OneTrust · SharePoint
.jnlp	75	Aplicaciones Java heredadas · lanzadores empresariales
.msg / .eml	28	Exportación de Outlook
.xls / .xla / .xlsb	27	Modelos financieros / de ingeniería
.docx / .doc	21	SharePoint · OneTrust
.zip	14	Archivos masivos
.pptx	11	Cubiertas internas
.gov	10	Informes · exportaciones



Archivos JNLP — revisar los lanzadores

75 descargas de .jnlp a Java Web Start. Java es cada vez más una vía de ataque; confirme que cada host que sirve JNLP esté en una lista de permitidos empresariales aprobados, y que los JRE administrados estén parcheados.

Descargas desde dominios externos

Principales fuentes no corporativas: [app-de.onetrust.com](#) (25), [pr.crm.dynamics.com](#) (12), [www.gartner.com](#) (12), Snow Software, Apple Identity, DigiCert, Indian Visa Online.

2,015 eventos de inicio de sesión, *una anomalía*.

908 inicios de sesión exitosos, 1,107 intentos y 144 fallos — una proporción saludable para una flota de este tamaño. La anomalía: 122 de los 144 fallos son contra Bing, casi todos de un pequeño número de usuarios. Vale la pena echar un vistazo más de cerca.

908

ÉXITO DE INICIO DE SESIÓN

En 17 aplicaciones SaaS

144

FALLO DE INICIO DE SESIÓN

122 de estos son contra Bing

6

WEBAUTHN / LLAVE DE PASO

Dell · Amazon · Microsoft

Superficies de fallo principales

- › Bing — 122 fallos. Probablemente una galleta atascada / confusión de cuenta de consumidor en sesiones de navegación, pero también un objetivo conocido de relleno de credenciales. Vale la pena confirmar que no es un script de fondo automatizado.
- › Microsoft 365 SharePoint — 7, luego Microsoft 365 — 5 y un puñado de eventos únicos en dominios públicos.
- › Dos fallos contra aplicaciones de Palo Alto Networks — higiene de cuentas internas.

¿Dónde están empezando a aterrizar las llaves de paso?

- › www.dell.com — 4 eventos.
- › amazon.co.uk — 1 evento.
- › login.microsoft.com — 1 evento

Una señal pequeña pero real — la autenticación resistente al phishing está empezando a utilizarse. Prisma Browser tiene visibilidad completa en las ceremonias de WebAuthn.

Política recomendada, *basada en datos de 42 usuarios.*

1 Bloquear el pegado del portapapeles en mensajeros personales / E2E. Añada una regla DLP de Prisma Browser: denegar pegado de portapapeles en web.whatsapp.com · web.telegram.org · signal.org Una regla, valor instantáneo, recupera la cobertura DLP que estamos perdiendo hoy.

GANANCIA RÁPIDA

2 Bloquear subidas / descargas de archivos a la nube personal + correo electrónico personal. outlook.live.com · mail.google.com · onedrive.live.com · drive.google.com · dropbox.com 33 sesiones personales de Outlook y un archivo de video ya llegaron en este período.

GANANCIA RÁPIDA

3 Federar las 17 aplicaciones que no son SSO — comience con Varonis, Google Base, NinjaRMM. Estas tres son de Alto Riesgo y actualmente están autenticadas por contraseña. El Acceso Condicional + DLP del lado del navegador es la combinación correcta.

ALTO

4 Consolidar los administradores de contraseñas a uno solo. Elija un estándar corporativo, impleméntelo mediante política, bloquee los otros dos. Reduce a la mitad el radio de impacto de credenciales y hace que el comportamiento de autocompletado sea predecible en toda la flota.

MEDIO

5 Active la integración Prisma Browser x CrowdStrike ZTA. Wood ya paga por Falcon en cada terminal — haga que la postura del dispositivo sea una señal de política de navegador de primera clase. Cero agentes nuevos.

INTEGRACIÓN

6 Establezca una alerta de sitio web malicioso + cuaderno de investigación. El acierto del 25-abr en hammockclusterstumble.com es el tipo de clic que debería autopaginar a SecOps con contexto completo de sesión.

OPERACIONAL

Navega sin límites con **Prisma Browser**



Defender lo que otros no pueden ver

- Proteger el trabajo de las amenazas web más evasivas
- Asegurar el trabajo en dispositivos no confiables
- Eliminar los puntos ciegos en las operaciones del SOC



Cobertura total Zero-Trust

- Control de **CUALQUIER** app: Shadow IT, GenAI y más
- Asegurar **TODAS** las acciones de usuario
- Motores de clasificación de datos en **TODOS** los controles



Experiencia de usuario óptima

- Acceso rápido con apps en un solo espacio de trabajo
- Máxima disponibilidad con arquitectura distribuida
- Alta de usuarios **en minutos** con **85% menos TCO**



GRACIAS

¿PREGUNTAS?