



FORTINET

COLOMBIA
& ECUADOR

XPERTS26



FORTINET | COLOMBIA
& ECUADOR
XPERTS26

Cloud & AppSec Track

David Zambonino Fabara
Cloud Subject Matter Expert - LATAM





Equipo del Track

Para compartir con ustedes esta experiencia de aprendizaje



Ana María Fuentes



Valeria Velastegui



David Zambonino



Juan Peña



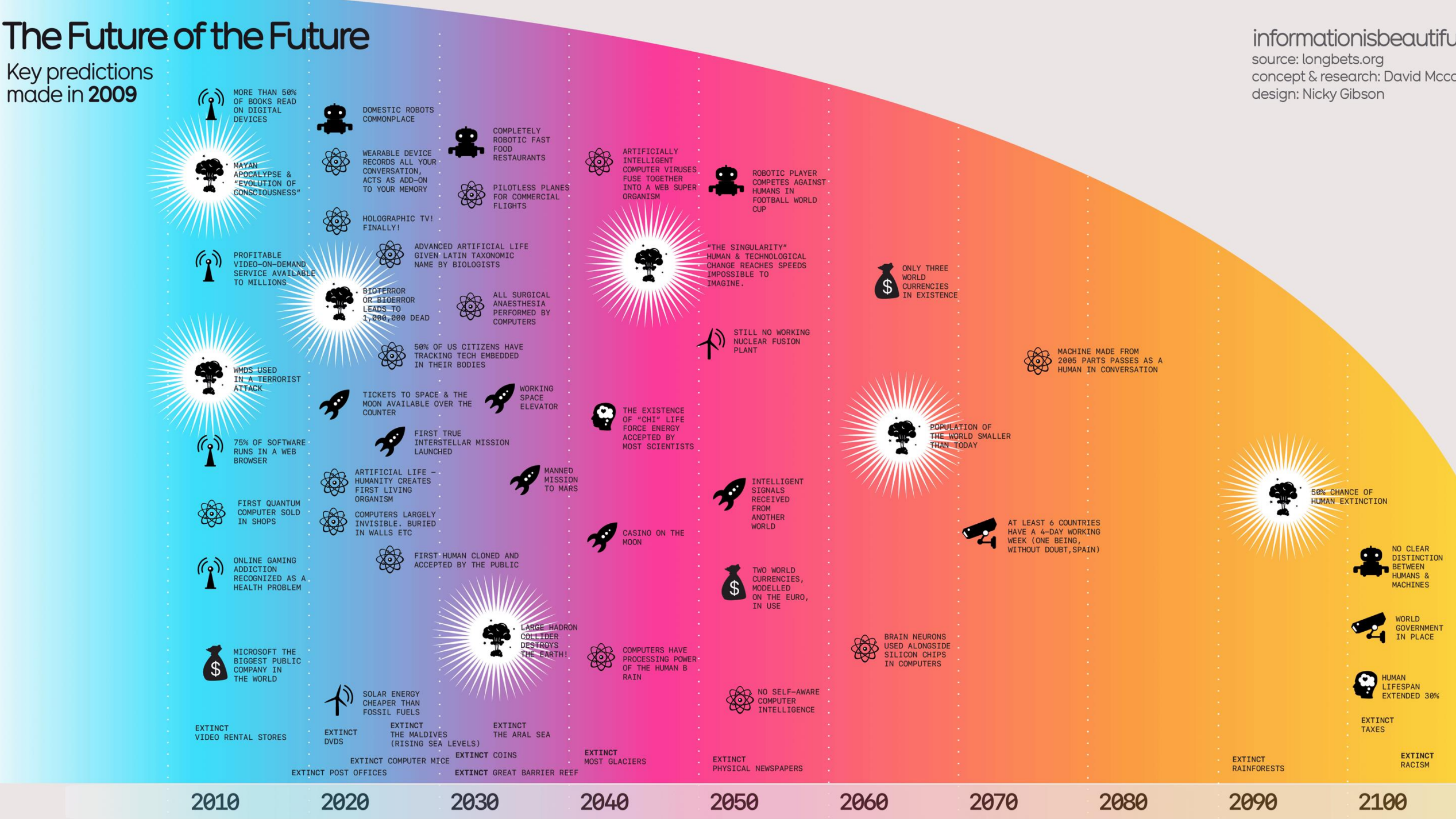
Carlos Montes



The Future of the Future

Key predictions
made in 2009

informationisbeautiful
source: longbets.org
concept & research: David McCann
design: Nicky Gibson



2009 · EL FUTURO QUE IMAGINAMOS



WMDs USED
IN A TERRORIST
ATTACK



75% OF SOFTWARE
RUNS IN A WEB
BROWSER



TICKETS TO SPACE & THE
MOON AVAILABLE OVER THE
COUNTER



FIRST TRUE
INTERSTELLAR MISSION
LAUNCHED



ARTIFICIAL LIFE —
HUMANITY CREATES
FIRST LIVING



ALL SURGICAL
ANAESTHESIA
PERFORMED BY
COMPUTERS



BIOTERROR
OR BIOERROR
LEADS TO
1,000,000 DEAD



50% OF US CITIZENS HAVE
TRACKING TECH EMBEDDED
IN THEIR BODIES



WORKING
SPACE
ELEVATOR



MANNED
MISSION
TO MARS



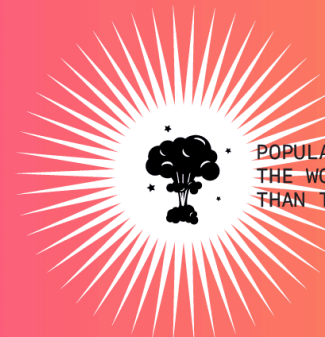
THE EXISTENCE
OF "CHI" LIFE
FORCE ENERGY
ACCEPTED BY
MOST SCIENTISTS



STILL NO WORKING
NUCLEAR FUSION
PLANT



INTELLIGENT
SIGNALS
D



POPULA-
THE WOR
THAN TO

LO QUE IMAGINAMOS · 2009

Autos voladores, colonias en Marte y robots mayordomo.

LO QUE LLEGÓ · 2022

Una IA que escribe, programa y conversa... usada por **800 millones** de personas.

El futuro llegó más rápido — y más raro.

2010

2020

2030

2040

2050

2060

message

Cyber business

information 748.720 followers online

news · analysis · reports

How does the artificial intelligence algorithm
technology and robotics in the near future
impact on employment internet work
revolution future of business and deep learning

748.720 followers online

Does the artificial intelligence algorithm
technology and robotics in the near future
impact on employment internet work
revolution future of business and deep learning

Message

AI REPORT

complex engineering, medicine, technique
 advanced artificial intelligence production
 creating images illustrations and videos
 dialogue in the natural language

technology and robotics in the near f
mpact on employment internet work
volution future of business and deep

technology : technology and robo
mpact on em impact on employmen
evolution future of bu

artificial intelligence

ChatBot

industry 4.0

machine learning

business technology digital

ation

brith

Message

TECHNOLOGY REVIEW

forum business economy

Message

TECHNOLOGY REVIEW

forum business economy online information service

● business ● industry ● trade

work with artificial intelligence decisions
 maging in the absence of all data of all d
 ndustry, trade, factory future of productio
 chatbot and automation process neural n

DIGITAL REPORT

Artificial neural networks and large server farms are driving the growth of speech recognition and natural language processing. The rapid growth of levels of artificial intelligence and high performance computing, machine learning and big data growth potential for artificial general intelligence benefits the corporation business and science.

AI REPORT

techniq
roduction

W

online information service

business • industry • trade

intelligence decisions

data of all

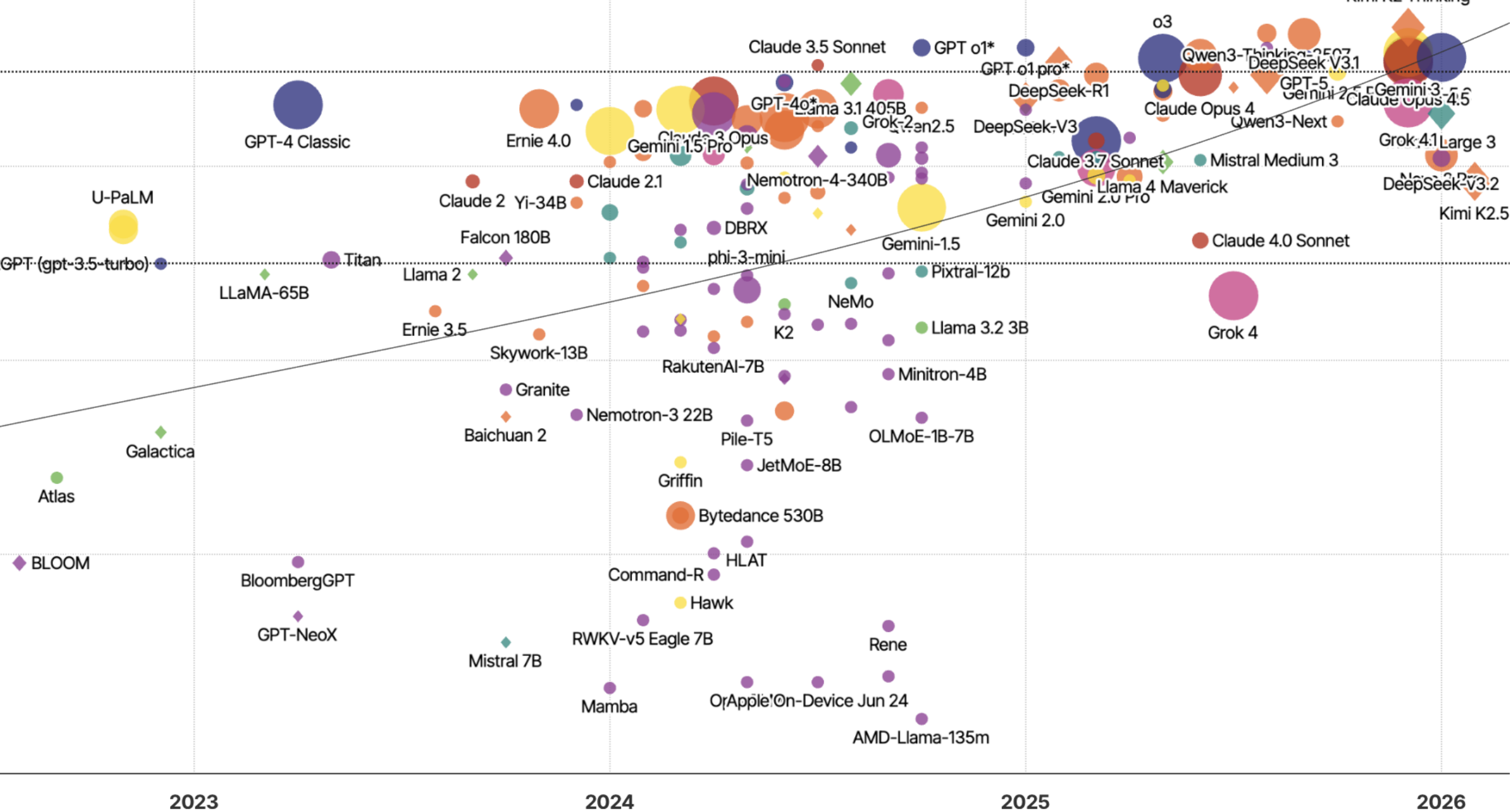
production

neural n

online information service

W

* = parameters undisclosed // source: LifeArchitect // data



La explosión de la IA generativa

88%

de las organizaciones ya usa IA



Panorama de amenazas AppSec 2026

No es una lista. Es una red. Una amenaza no llega sola — arrastra otras 5.

TRAZANDO LAS CASCADAS · 2026

14 amenazas · 17 cascadas conocidas

● ACTIVOS ● NUEVO ● SUPPLY ● CLOUD ● ORG



TOP VECTORES HOY



THREAT INTEL

Fuente: Fortinet Web AppSec Report 2026 · OWASP MCP Top 10 · Threat Intel FortiGuard

La adopción corre; la seguridad camina

Y en esa brecha entre gobernanza y velocidad vive el riesgo.

US\$ 4.4M

coste medio de una brecha de datos

97%

de los incidentes de IA ocurrieron sin controles de acceso adecuados

63%

de las organizaciones no tiene políticas de gobernanza de IA (shadow AI)

Phishing y Social Engineering:

- 1 265% aumento de ataques gracias a IA generativa
- 202% incremento en 2024; +80% de correos usan IA

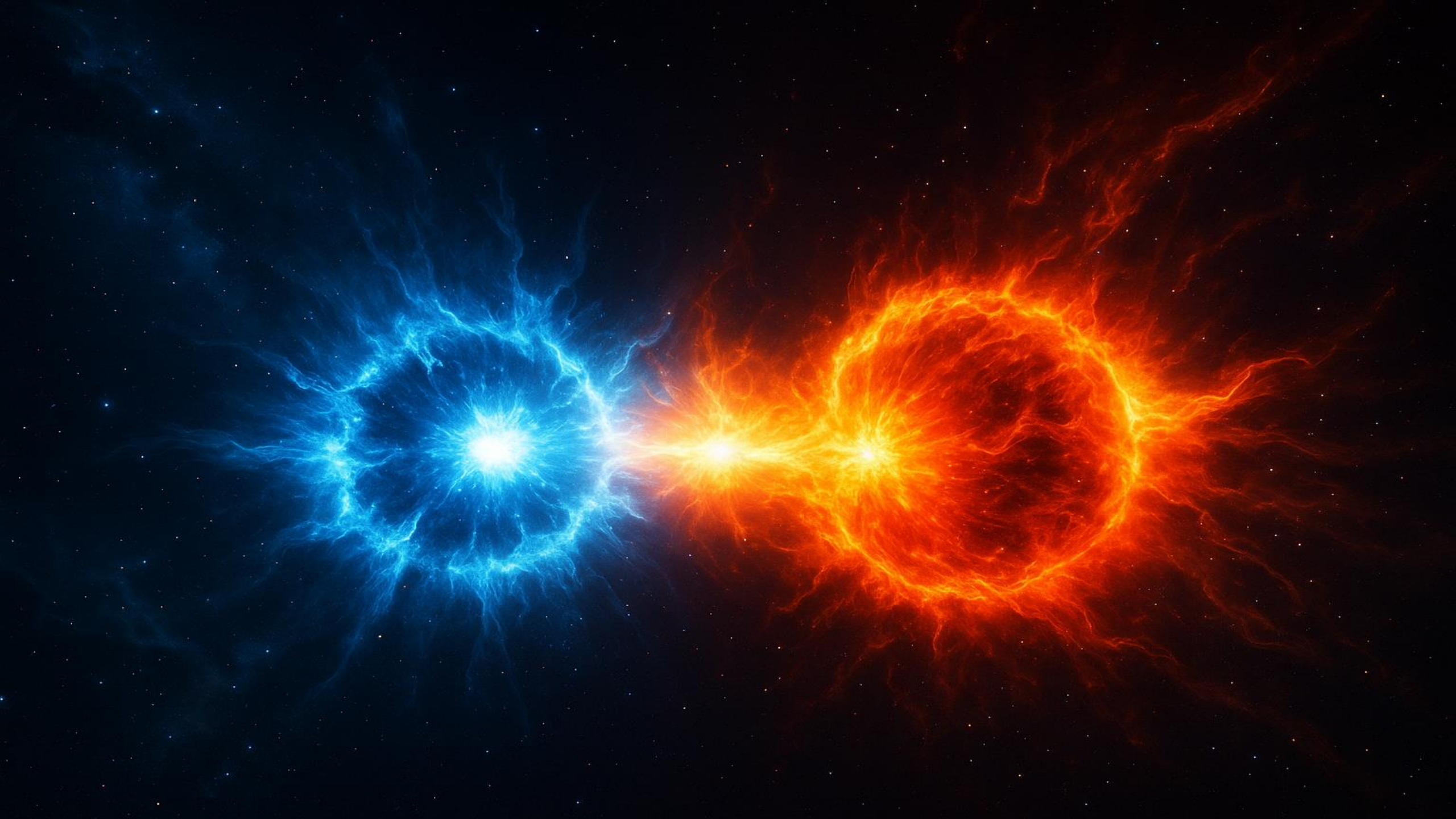
Deepfakes:

- 3 000% incremento en fraudes con audio/vídeo

Cadena de Suministro & API:

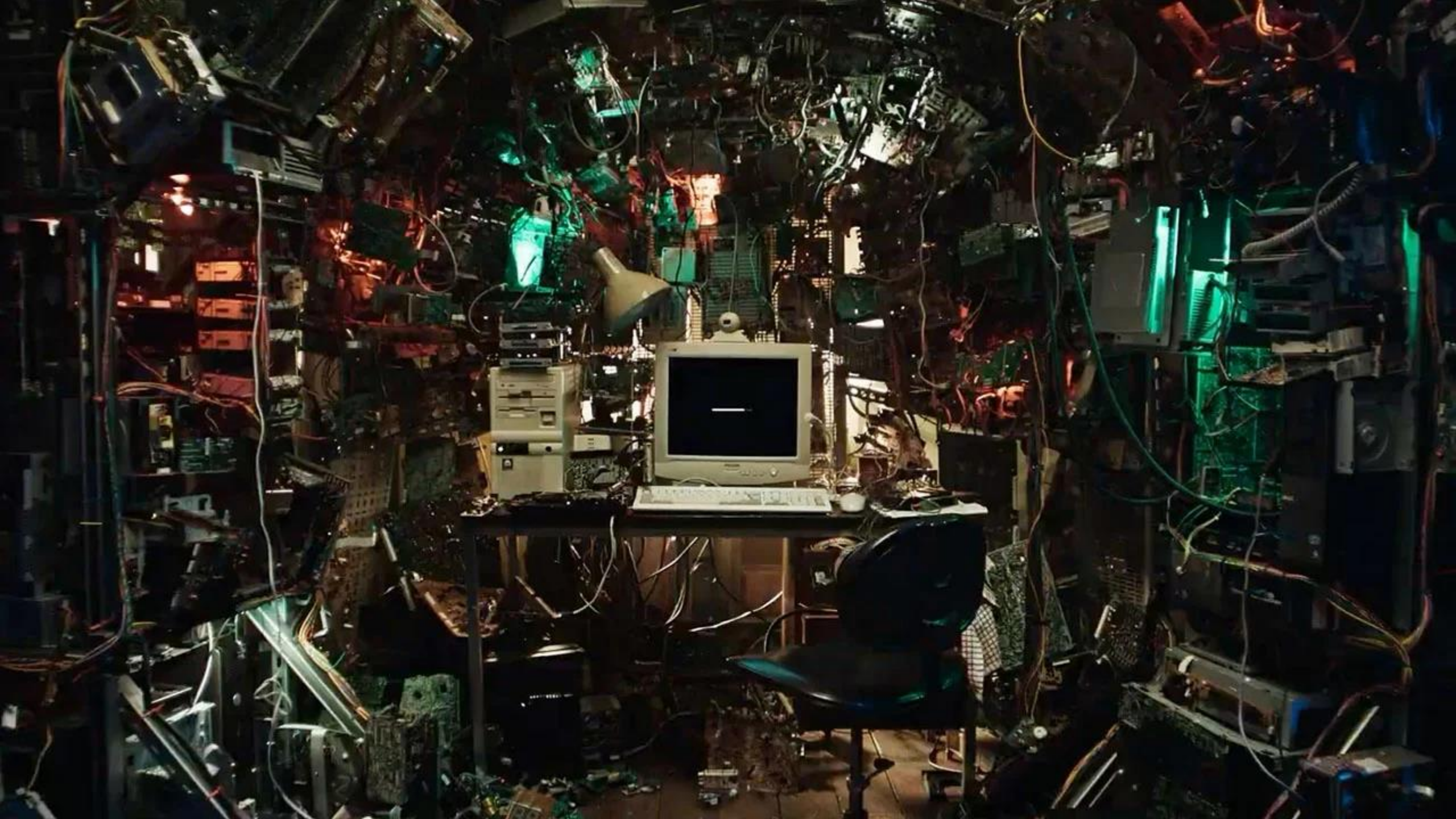
- 40% de brechas provienen de terceros
- 57% de organizaciones sufrieron brechas API
- 99% reportó problemas de seguridad en APIs





A mayor uso de IA, la Seguridad
tiene que ser más estricta





¿Por qué la nube AÚN?

88%

de las organizaciones ya usa IA, un buen porcentaje de ellas en la nube

La adopción ya no es opcional. La pregunta dejó de ser “¿sí?” y pasó a ser “¿qué tan rápido — y qué tan seguro?”.



Productividad

Copilotos y agentes automatizan lo repetitivo. Los equipos producen más, más rápido.



Eficiencia y costo

Hacer más con menos. Hasta US\$ 1.9M de ahorro con IA y automatización (IBM 2025).



Experiencia y velocidad

Atención 24/7, respuestas al instante y menor time-to-market.



Ventaja competitiva

Los competidores ya adoptan. Quedarse fuera es quedarse atrás.

El driver no es la moda: es productividad, costo y competir. La adopción es inevitable — hacerla segura es la decisión de negocio.

Los costos ocultos



Lo que ves y presupuestas

Tokens y llamadas API · GPU y cómputo · Licencias y suscripciones

El costo oculto: la seguridad

- Fuga de datos y PII
- Prompt injection y manipulación
- Incumplimiento: GDPR · PCI · ISO
- Shadow AI: datos fuera de control
- Robo de modelo / propiedad intelectual
- Daño reputacional y remediación

US\$ 4.4M — coste medio de una brecha de datos (IBM 2025)

Ignorar la seguridad no la elimina: la aplaza y la multiplica. Lo que no proteges hoy se paga después — con intereses.

Los modelos de servicio evolucionan

SaaS

App lista para el usuario

ChatGPT · Copilot · Gemini

MaaS

Modelo por API (pagas por token)

Bedrock · Azure OpenAI · OpenAI

PaaS

Construyes y despliegas tu modelo

Azure AI Foundry · SageMaker

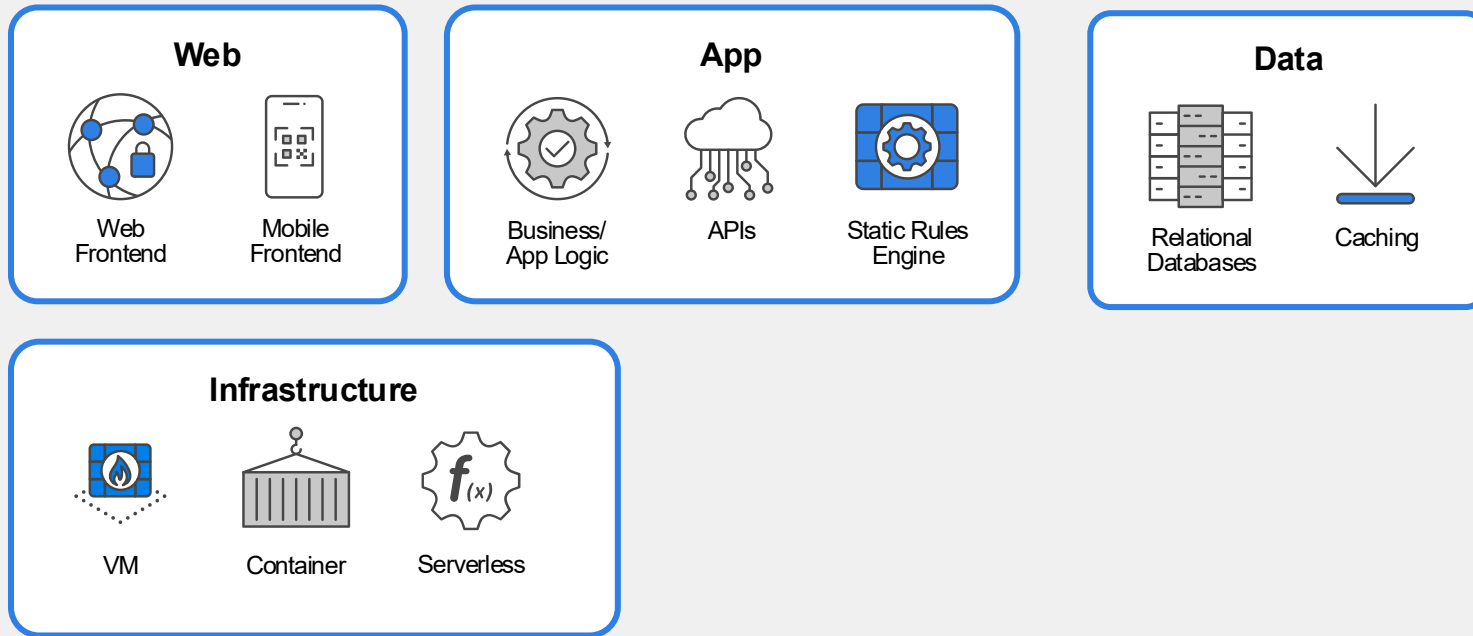
IaaS

Modelos open en tu GPU

Ollama · vLLM · Triton

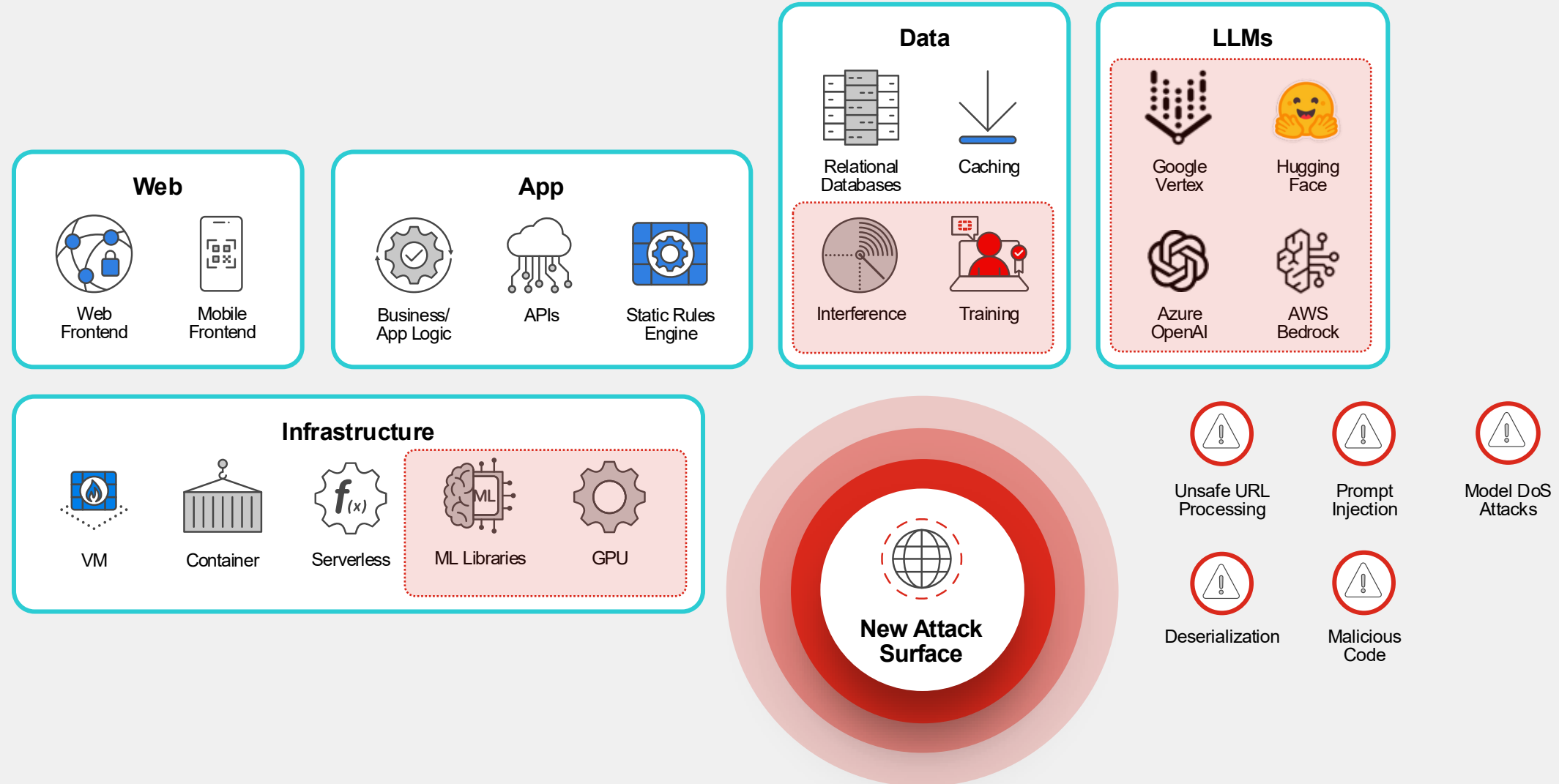
Marco de seguridad de aplicaciones tradicional

Se basa en la monitorización del tráfico en las capas de red y de aplicación, evitando que las amenazas lleguen a recursos sensibles.



Nueva arquitectura de aplicaciones de IA

Introduce nuevas amenazas, ampliando la superficie de ataque de la aplicación.





IA para la seguridad

Aprovechar la GenAI para **mejorar los productos y servicios de Fortinet**



Seguridad para la IA

Usar los productos y servicios de Fortinet para **asegurar el uso de GenAI del cliente**



Asistir

Agentes integrados en los productos para optimizar y automatizar las operaciones diarias

Aprovechar la IA para mejorar o acelerar la detección de amenazas y otras funciones del producto



Proteger

Visibilidad y control sobre todo el uso de IA (Shadow AI)

Asegurar el uso de componentes de IA, incluyendo seguridad de MCP, A2A y LLM



Asegurar la IA

Soluciones



Marco de IA Agéntica



Detección Autónoma de Amenazas



Bloqueo de Shadow AI



IA Fábrica



LLM Seguridad

Tres retos principales



Asegurar el SaaS



**Asegurar la
infraestructura –
"el DC"**



**Asegurar Aplicaciones
AI & LLM**

Agenda



Arquitectura de Ciberseguridad en la Nube



Shadow AI para entornos SaaS



Cacería de Amenazas en la Nube



Seguridad para Código



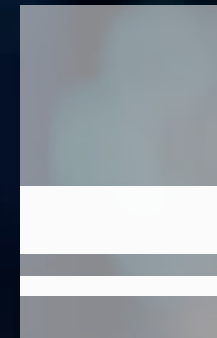
Seguridad para aplicaciones



Agenda

Hora	Martes 08/25	Miércoles 08/26	Jueves 08/27
	Día 1	Día 2	Día 3
07:00	 Breakfast - Rest. Las Chivas	 Breakfast - Rest. Las Chivas	 Breakfast - Rest. Las Chivas
08:00	 INTRODUCCIÓN GENERAL	Cloud Landing Zones · 30 min	 Application Security ★ LAB
08:30	Arquitectura de Ciberseguridad en la Nube 		Shadow AI - Presentación
09:00			
09:30		 Coffee Break	 Coffee Break
10:00	Architecture Battle - Dinámica 	Shadow AI - LAB	 Application Security ★ LAB
10:30			
11:00			
11:30			
12:00	Cierre 		
12:30			
13:00	 Lunch - Terraza Las Chivas	 Lunch - Terraza Las Chivas	 Lunch - Terraza Las Chivas
13:30	Cloud Threat Hunting - LAB	 Code Security ★ LAB	Cloud & App Sec Challenge ★
14:00		 Code Security ★ Presentación	
14:30			
15:00	Cloud Threat Hunting - Presentación		
15:30	Cloud Threat Hunting - LAB parte 2	 Coffee Break	 Cierre!
16:00		 Code Security ★ LAB Part 2	UFC ★
16:30			
17:00			
17:30			
18:00			
18:30			





"Si buscara riqueza, sería **banquero**.
Si ansiara poder, sería **político**.
Si anhelara fama, sería **artista**.

Pero solo quiero **cambiar el mundo**.
Soy un **Ingeniero de Ciberseguridad**."

Es un mundo complejo :
¡Sé un FortiHéroe!



¡Gracias!



¿Preguntas?



FORTINET

COLOMBIA
& ECUADOR

XPERTS26