illumio

inception
Un evento de TrustDimension 2026

De vulnerable a invencible

Reforzando su red con Microsegmentación

Armando Galván

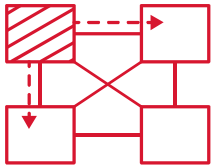
Partner Account Director – LATAM

13 Noviembre, 2025

¿Por qué tienen éxito los ataques?

Fallos de prevención y detección

- Intrusión no detectada + no autorizada
- Los atacantes acechan durante meses: tiempo de permanencia



Propagación de ataques

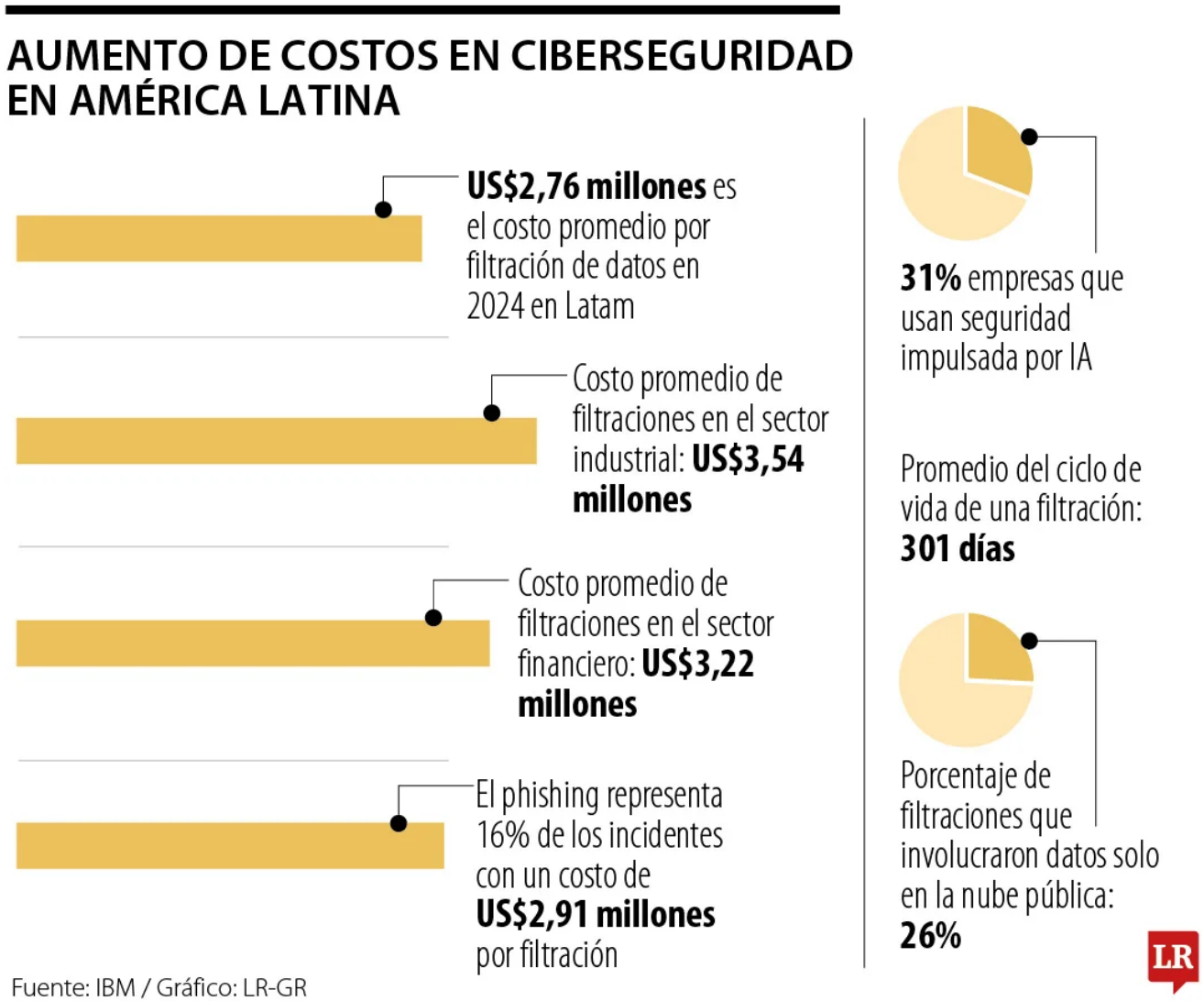
- El movimiento lateral permite a los atacantes un acceso completo a la red
- Las redes planas sin segmentación están indefensas

En un mundo hiperconectado, híbrido y multinube, el movimiento lateral es EL mayor riesgo

Activos críticos comprometidos

- El malware bloquea los sistemas y exige un rescate
- Riesgo de exfiltración de datos y violaciones normativas

América Latina es la región más vulnerable a los ciberataques, en el mundo

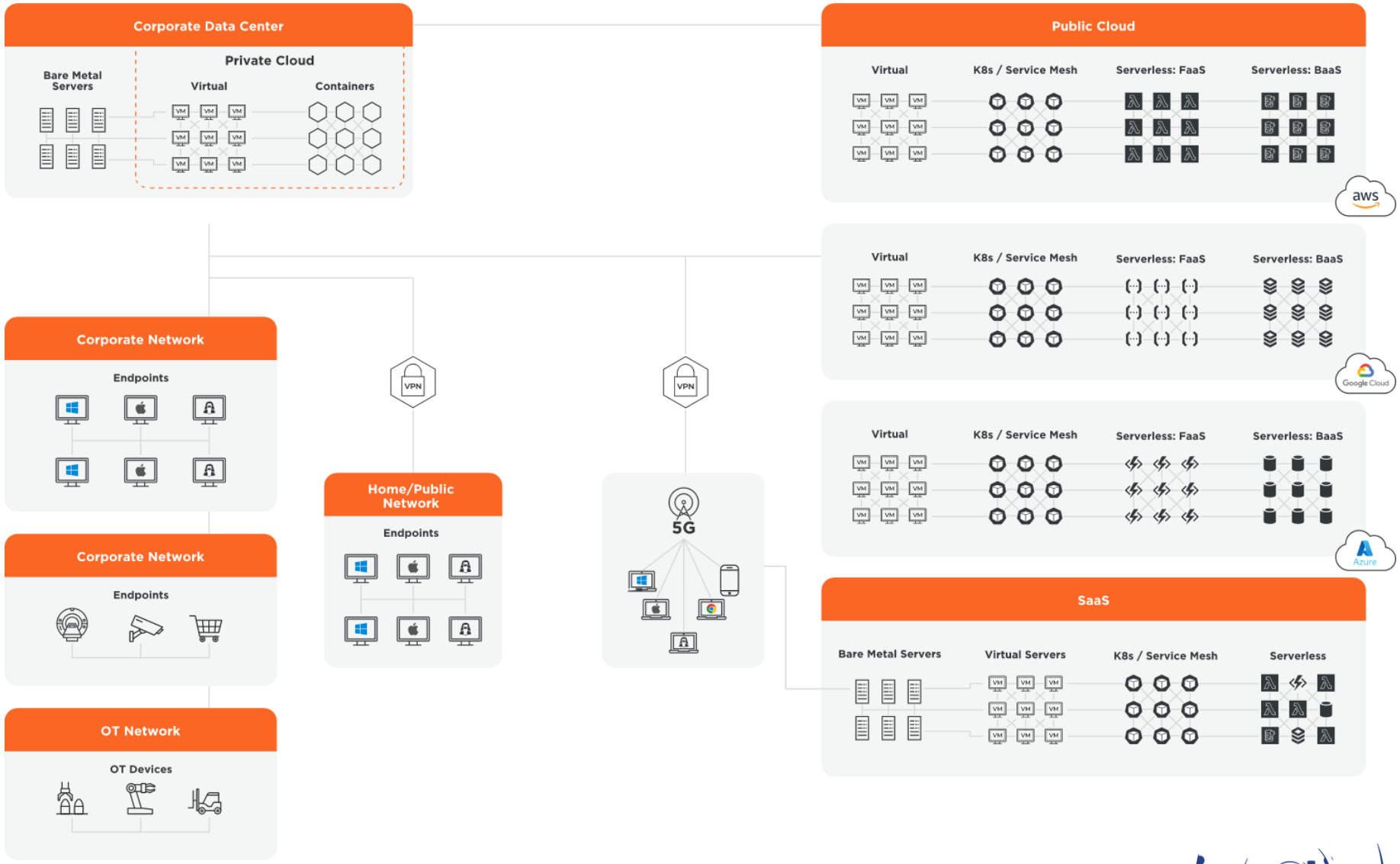


Países y Amenazas Más Detectadas
Los países con el mayor volumen de ciberamenazas detectadas **en el primer semestre de 2024, según ESET,** fueron:

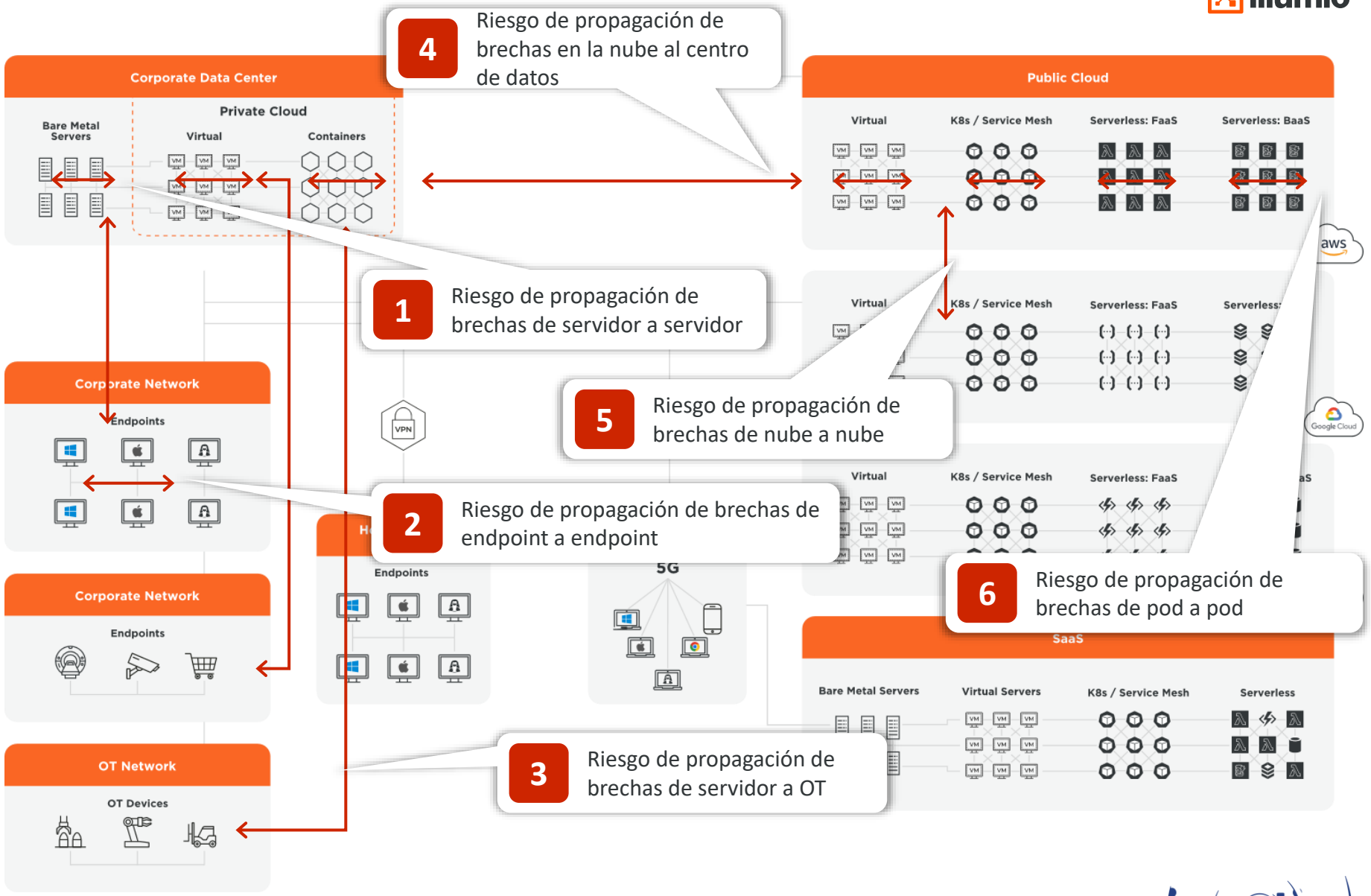
Perú (909.830)
México (351.039)
Ecuador (204.023)
Brasil (201.879)
Argentina (172.162)

Las amenazas más comunes **incluyeron un promedio de 2.6 millones de muestras únicas de malware** (inyectores, troyanos, downloaders, gusanos, exploits, backdoors, spyware, etc.). **El phishing y el ransomware siguen siendo amenazas predominantes.**

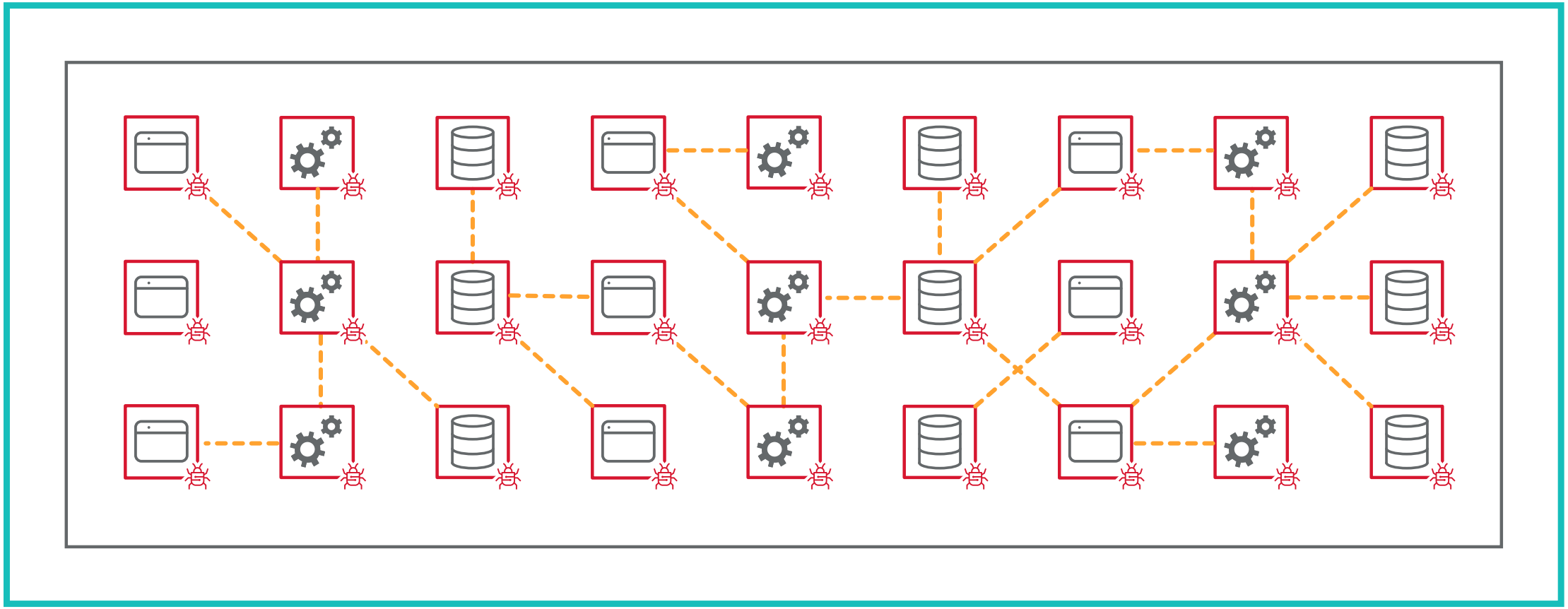
La superficie de ataque se está expandiendo



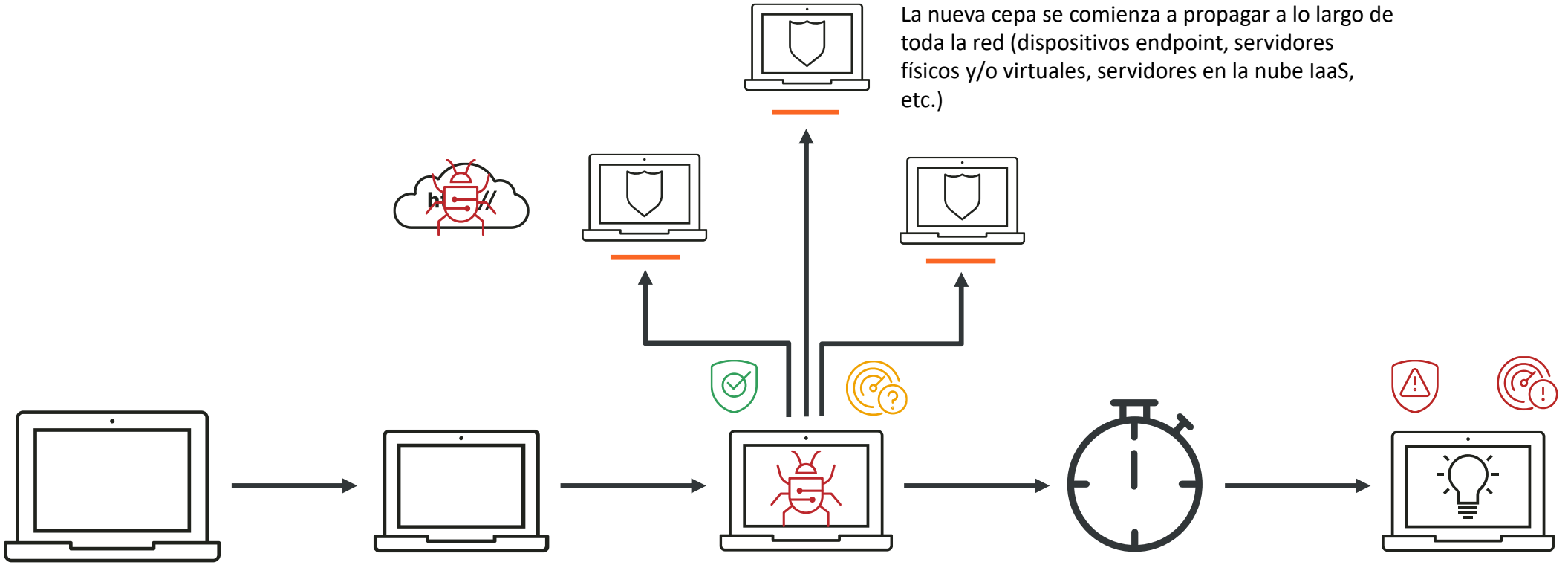
Es fácil que las brechas se propaguen



Las redes planas son peligrosas



¿Cómo se realiza el movimiento lateral?



La nueva cepa se comienza a propagar a lo largo de toda la red (dispositivos endpoint, servidores físicos y/o virtuales, servidores en la nube IaaS, etc.)

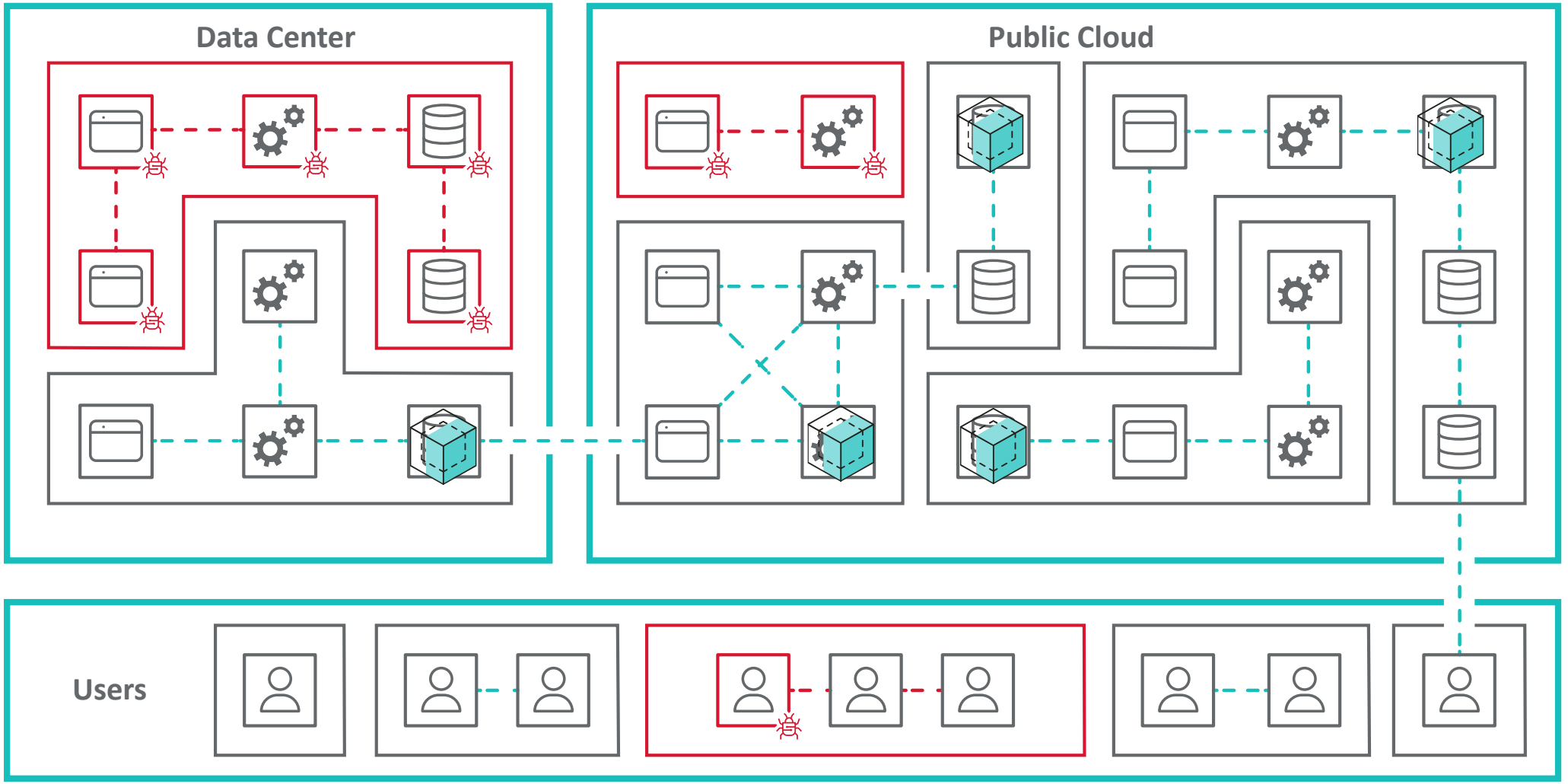
Clics en enlaces sospechosos

Una nueva cepa pasa los controles iniciales, pero aún es monitoreada por el EDR, ya que se desconoce

2 horas después

La nueva cepa se detecta y bloquea después del hecho para proteger al usuario y cualquier intento futuro de descarga

La microsegmentación de Zero Trust crea superficies protegidas



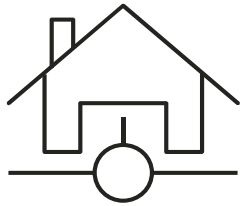
Zero Trust

Una estrategia diseñada para detener las filtraciones de datos y evitar que otros ciberataques tengan éxito al eliminar la confianza de los sistemas digitales.

Taxonimia Zero Trust

La segmentación es fundamental para su estrategia Zero

Zero Trust Network Access



Perímetro de última generación para identificar y verificar de forma segura la conectividad basada en la identidad

Muestra de empresas

netskope
appgate
iboss
Microsoft
CATO NETWORKS
zscaler
paloalto NETWORKS

Zero Trust Segmentation

Mapeo de interdependencias y separación de aplicaciones, sistemas de TI y TO

illumio
The Zero Trust Segmentation Company

Zero Trust Data Security

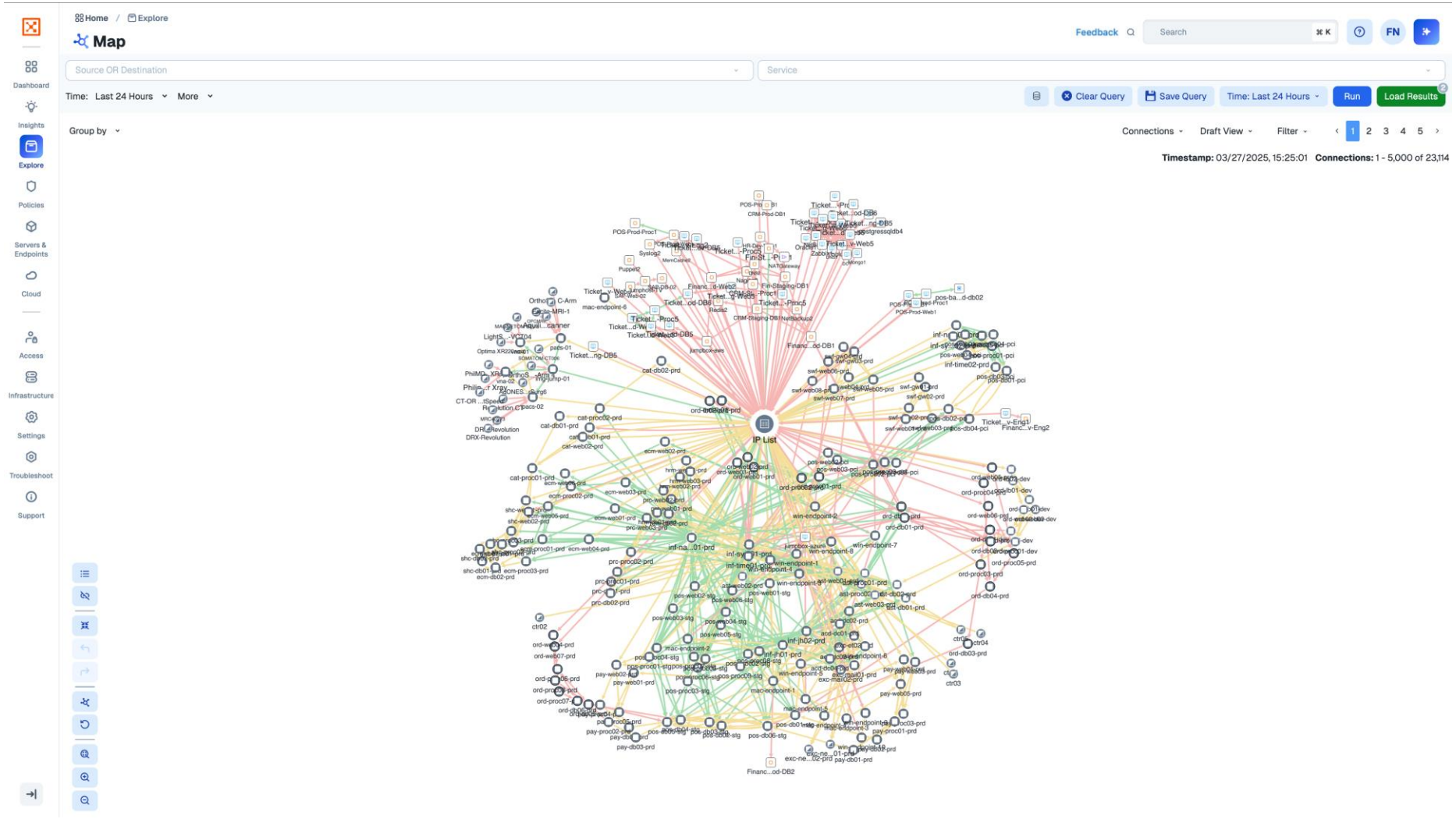
Copia de seguridad y restauración de datos fiables y fiables

Muestra de empresas

rubrik
COMMVAULT
VEEAM
COHESITY

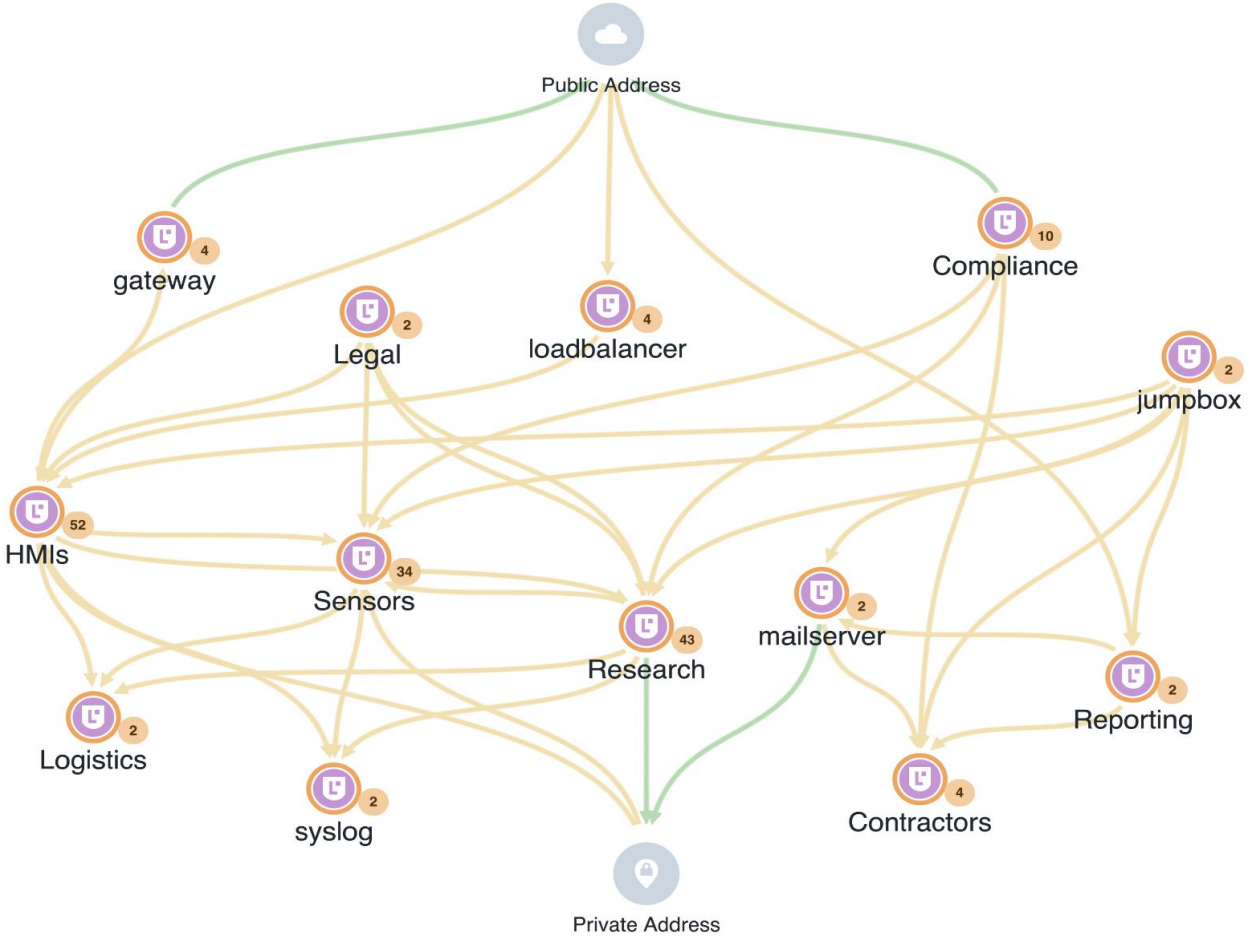
Zero Trust Segmentation 123

Orden a partir del Caos

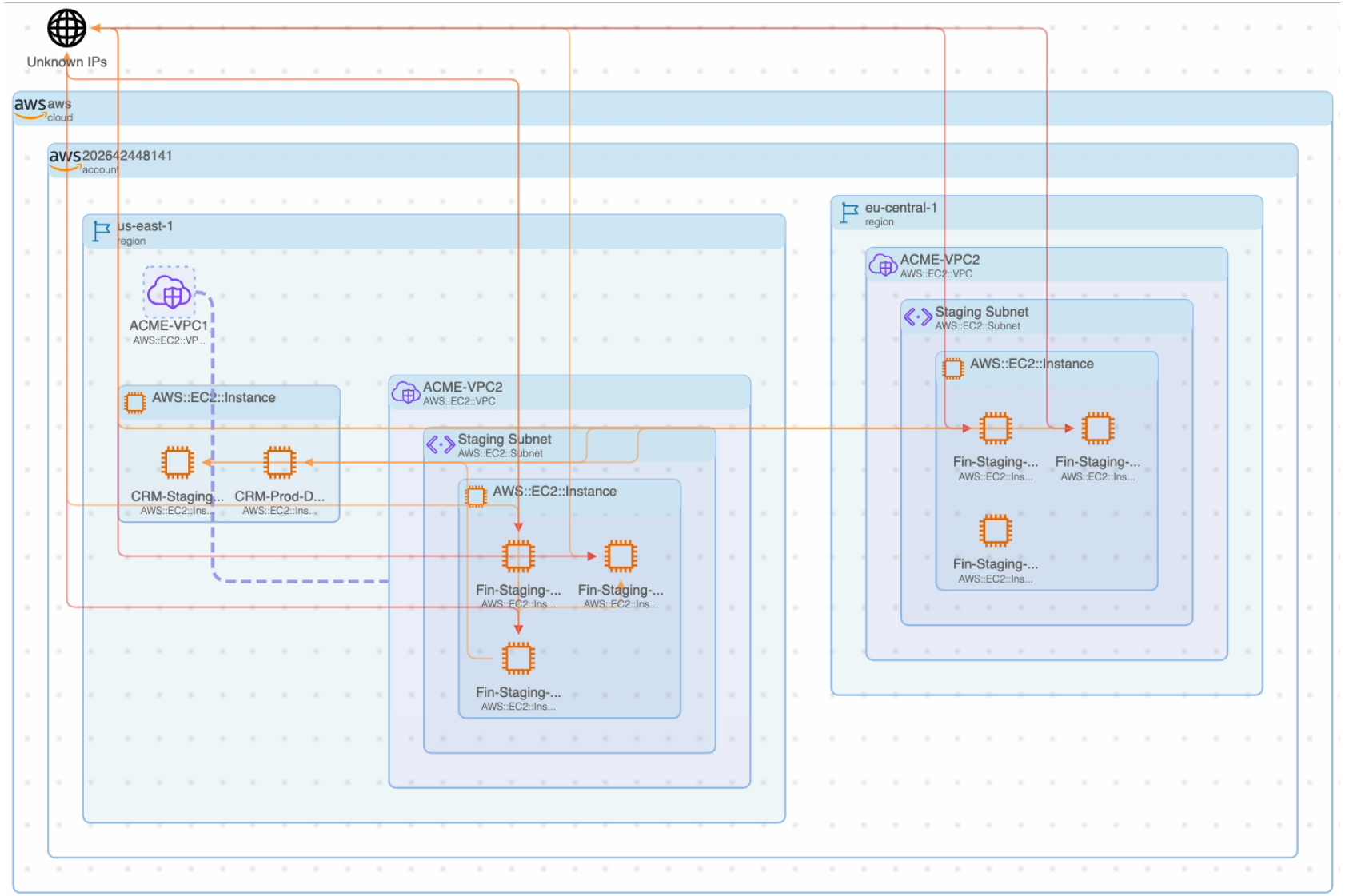


Step 2: Label workloads, along business-defined boundaries

Define Policy using Labels, not using network addressing.

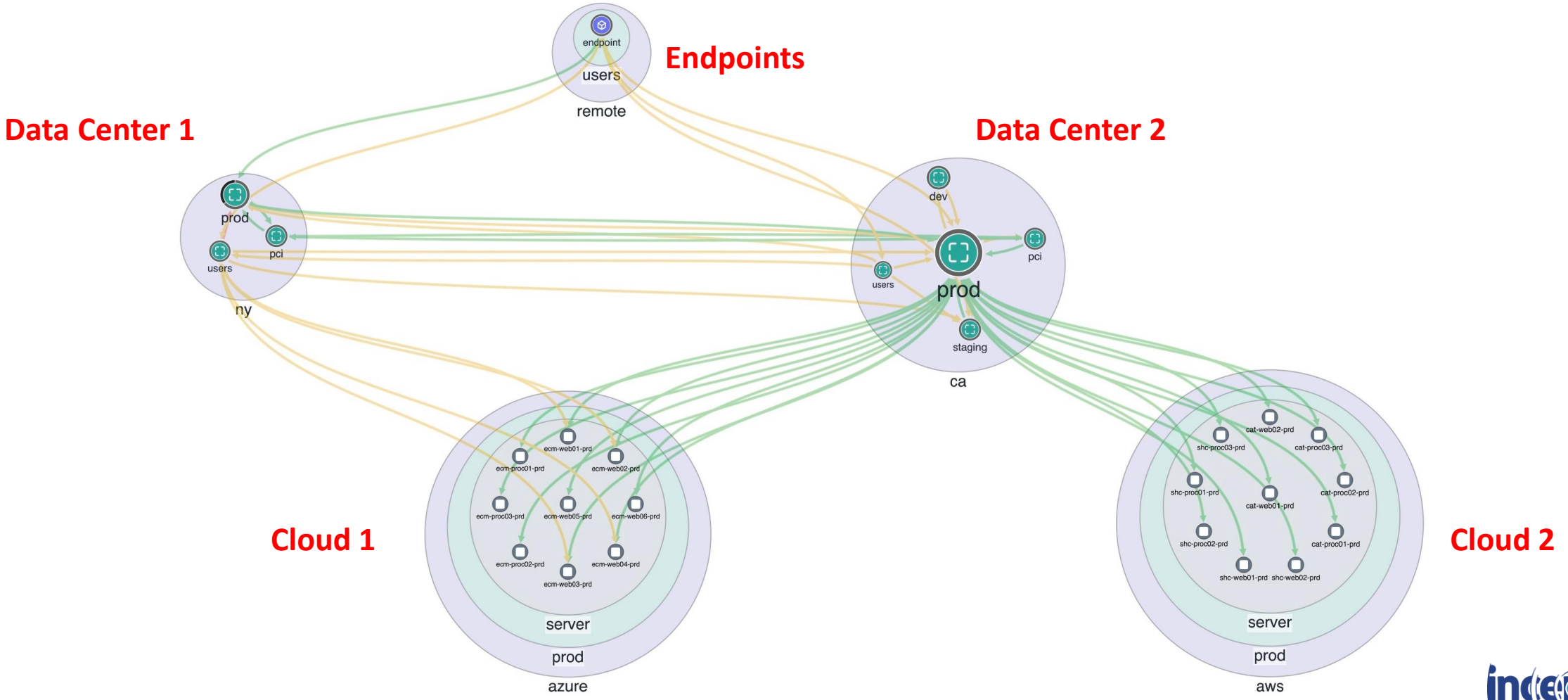


Visibilidad y aplicación sin agentes: en la nube



Result: Visibility Across All Environments, Everywhere

Zero Blind Spots, all Segments Visible & Enforced



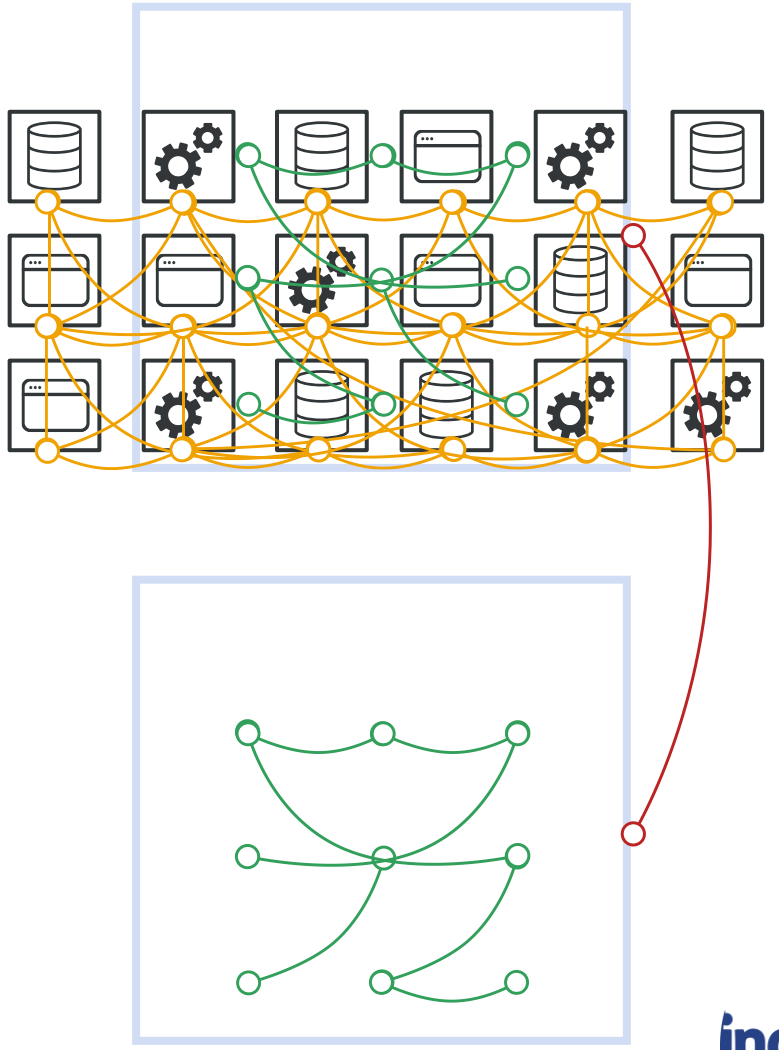
¿Qué hace Illumio?

1

Crear un mapa de sus endpoint, aplicaciones y conectividad

2

Segmentación basada en la política para garantizar que **solo los dispositivos que deberían hablar entre sí lo hacen**



illumio

Home / Insights

Insights Hub

Search ⌘ K

AG

Last 24 hours compared to Previous 24 hours

Traffic is Allowed or Denied

- Dashboard
  - Servers & Endpoints
  - Cloud
  - Ransomware Protection
- Insights
  - Insights Agent BETA
  - Agent Summaries
  - Insights Hub
  - Resource Traffic
  - Country Insights
  - Firewall Insights
  - Risky Traffic
  - Malicious IP Threats
  - Shadow LLMs
  - External Data Transfer
  - DORA Compliance
  - Label Based Insights
- Quarantine
- Explore
  - Map
  - Traffic
  - Mesh
- Segmentation
  - All Policies
  - Deny Rules
  - Drafts & Versions
- Policy Objects
  - Services
  - IP Lists

Top 10 Malicious IPs

Flows | Bytes

Outbound			Inbound		
103.75.183.233	HTTP	2.6K ↑2.6K	101.99.76.21	RustDesk	2.3K ↑2.3K
103.110.221.50	HTTP	2.3K ↑2.3K	114.43.131.125	RustDesk	2.3K ↑2.3K
114.66.58.82	HTTP	2.3K ↑2.3K	105.102.137.34	RustDesk	2K ↑2K
107.174.82.199	FTPControl	2.2K ↑2.2K	141.224.251.187	SSH	1.6K ↑1.6K
103.42.30.157	TeamViewer	2K ↑2K	120.157.80.44	SSH	672 ↑672
107.174.232.95	FTPControl	1.8K ↑1.8K	194.102.104.110	SSH	462 ↑462
117.72.242.9	SSH	1.8K ↑1.8K	14.103.145.185	SSH	321 ↑321

Top Sources With Data Transfer

Flows | Bytes

- rsa-jumphost
- kubernetes
- aks-node...4-vmss_0
- Ticketin...rod-Web5
- aks-node...6-vmss_0
- kubernetes
- kubernetes
- kubernetes
- aks-node...0-vmss_0
- VDI-illumio-001

Risky Services Traffic

Search

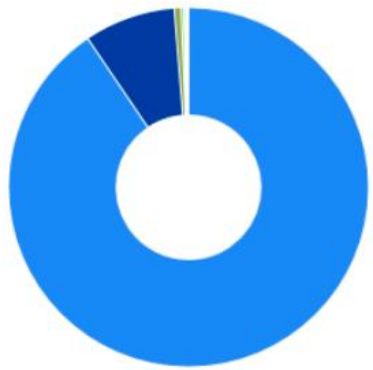
Show All Data

Service	Port	Protocol	Flows Now	Bytes Now	Flows Prev	Bytes Prev
SMB			42.9K	530.6GB	35.2K	452.6GB
MSRPC	135	TCP	16.2K	214GB	11K	141.5GB
WinRMHTTP	5985	TCP	4.2K	55.3GB	2.5K	30.4GB
RDP			35.3K	25.8GB	27.1K	18.6GB
WinRMHTTPS	5986	TCP	940	8.9GB	678	6.1GB
TeamViewer			19.9K	32GB	4.9K	11.9GB
RustDesk			1.8K	23.5GB	1.3K	16.8GB

Top Destination Roles

HTTPS 443 TCP

Flows | Bytes



- 1.4M Unknown
- 122.1K web
- 8.9K EC2NATGate...
- 3.7K db
- 2.4K EC2VPCEndp...
- 1.7K AzureFirewalls
- 626 secrets
- 552 serverless
- 542 Instance
- 537 func
- 0 dns

Importancia de Insights para nuestra cartera de productos

CONTENER LA BRECHA

MicroSegmentación

IDENTIFIQUE LA BRECHA

Insights agrega velocidad

El robo del Louvre 2025: Lecciones en ciberseguridad

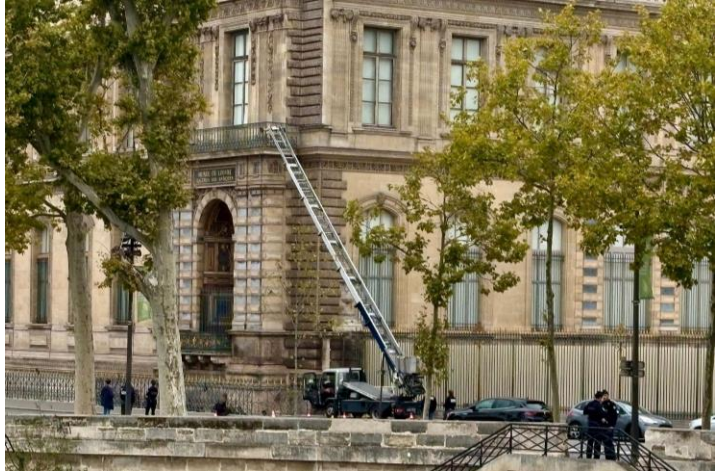
Un audaz robo en el Museo del Louvre reveló vulnerabilidades críticas. A partir de este caso, analizamos cómo la segmentación y visibilidad continua de Illumio habrían prevenido una intrusión tan rápida.

El robo

- El 19 de octubre de 2025, cuatro ladrones disfrazados de obreros ingresaron por una ventana del primer piso usando una plataforma elevadora. En menos de ocho minutos, robaron ocho joyas históricas de la corona francesa.

Vulnerabilidades detectadas

- Ventanas sin blindaje adecuado y cámaras desalineadas.
- Falta de respuesta rápida y reducción de personal.
- Protocolos de seguridad incompletos o desactualizados.



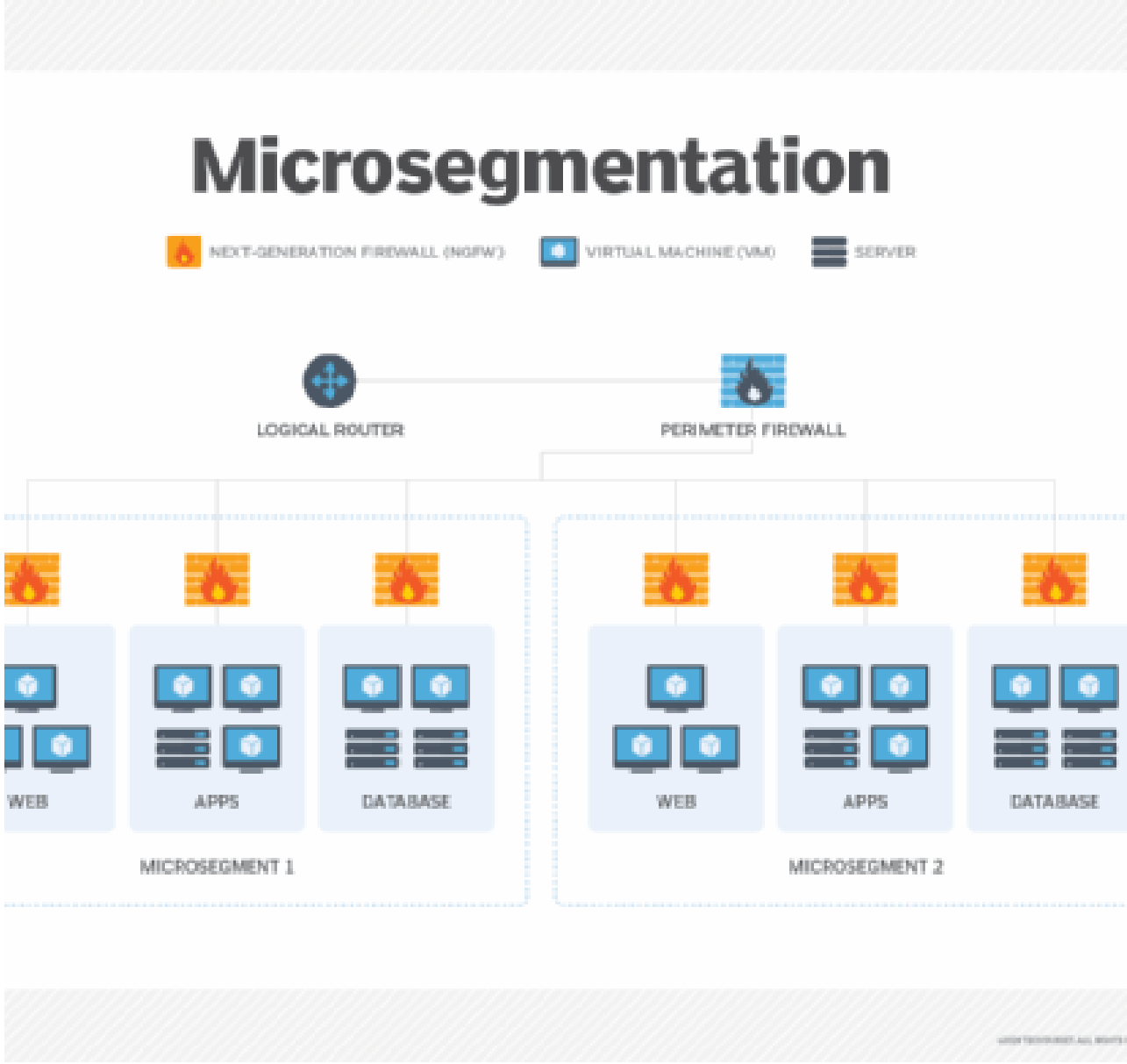
Analogía con ciberseguridad

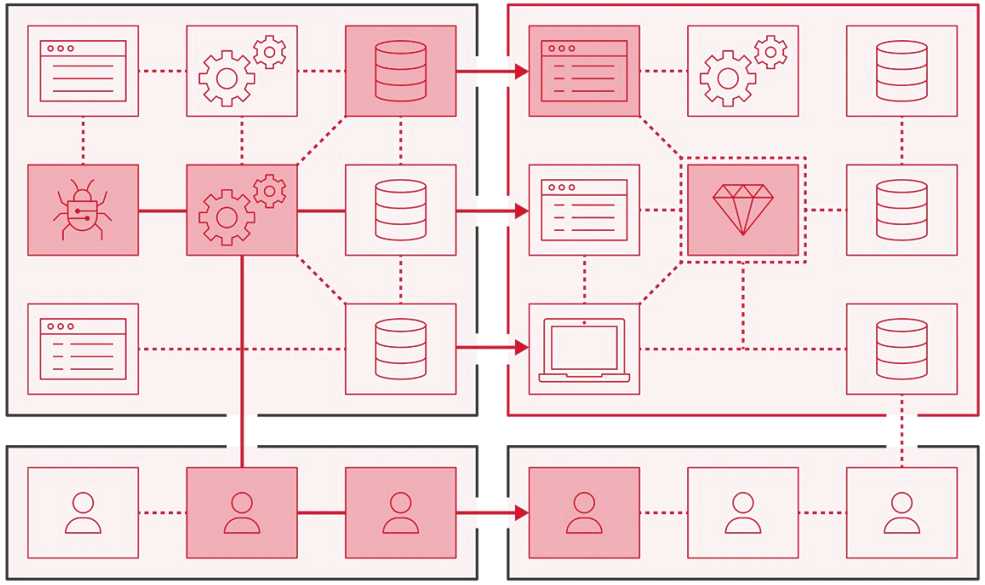
Museo → infraestructura de red / datacenter / sistemas críticos.

Joyas → activos valiosos (datos, propiedad intelectual).

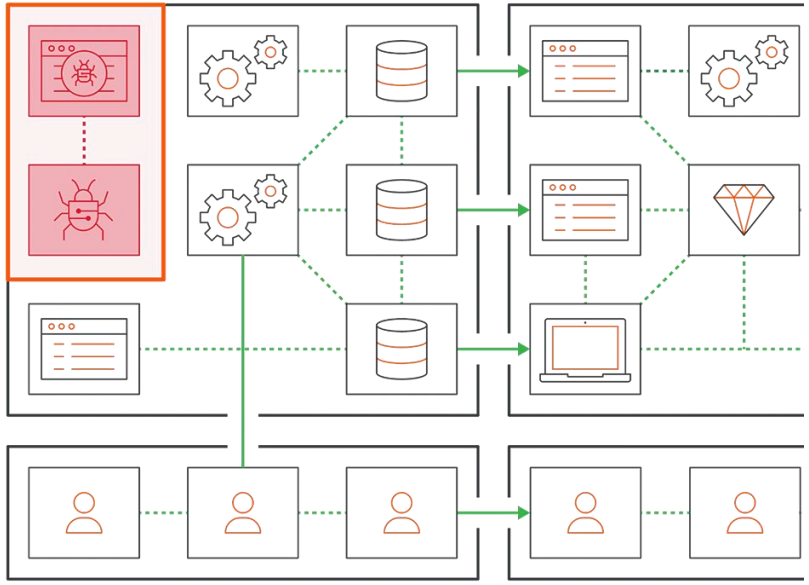
Ladrones → cyber atacantes.

Cámaras /guardias → herramientas de monitoreo y control de acceso.





WITHOUT SEGMENTATION



WITH SEGMENTATION

Cómo Illumio habría prevenido el incidente

- Mapeo de comunicaciones: visibilidad completa del entorno.
- Microsegmentación: aislamiento de activos críticos.
- Contención rápida ante incidentes.
- Modelo Zero Trust: asumir brechas y minimizar privilegios.

Aspecto de seguridad	Sistema del Louvre (pre-robo)	Microsegmentación con Illumio (hipotético)
Arquitectura de seguridad	**Seguridad de perímetro obsoleto:** Basada en la idea de que una vez dentro, no hay seguridad estricta. Los atacantes burlaron el perímetro exterior usando andamios y una plataforma elevadora.	**Seguridad Zero Trust:** El modelo de "confianza cero" de Illumio no asume que el perímetro protege los activos internos. Cada activo se considera un "segmento" que debe ser protegido individualmente.
Protección de activos	**Protección inconsistente:** Las vitrinas de cristal no eran de la calidad más alta, y la seguridad en la exhibición era insuficiente para un ataque coordinado.	**Segmentación granular:** Se podría haber asignado una "política de seguridad" única a cada vitrina (el "activo"). Esta política solo permitiría el acceso de personal autorizado.
Detección de intrusos	**Falta de visibilidad:** Las auditorías previas revelaron que muchas salas carecían de cámaras de vigilancia adecuadas, y la infraestructura de CCTV estaba desactualizada.	**Visibilidad completa:** Illumio ofrece una visibilidad total y en tiempo real del "tráfico" (movimiento y actividad) entre todos los segmentos. Un acceso no autorizado a una vitrina habría generado una alerta inmediata.
Contención de amenazas	**Respuesta reactiva:** El personal de seguridad tardó en responder, lo que permitió que los ladrones escaparan rápidamente.	**Contención ante una brecha de seguridad:** La plataforma de Illumio puede aislar un segmento comprometido (una vitrina o un pasillo) para detener la propagación del ataque. Esto podría haber activado bloqueos de puertas o alarmas de alta prioridad.
Análisis de riesgos	**Fallas ignoradas:** A pesar de los informes que señalaban la falta de modernización, la administración del museo no invirtió lo suficiente en seguridad.	**Análisis proactivo:** El "gráfico de seguridad de IA" de Illumio identifica posibles vías de ataque y recomienda políticas para fortalecer la seguridad de forma preventiva.
Velocidad de respuesta	**Tiempo de respuesta lento:** La dependencia de personal humano y sistemas obsoletos hizo que la respuesta fuera tardía, dejando a los ladrones actuar sin impedimentos.	**Respuesta en segundos:** Las políticas de Illumio permiten contener un ataque en minutos, no horas, lo que reduce drásticamente el impacto de un robo.

Lección final

El robo del Louvre subraya que una estrategia de seguridad moderna no debe limitarse a la protección perimetral. Los museos, como cualquier otra institución con activos de alto valor, necesitan una seguridad por capas que proteja cada objeto individualmente.

Seguridad más allá del perímetro

Segmentación y aislamiento de dispositivos criticos

Visibilidad para la prevención

Inversión en seguridad

El caso del Louvre es un claro recordatorio de que priorizar el presupuesto por encima de la seguridad de activos valiosos puede llevar a pérdidas irreparables. La modernización de los sistemas de seguridad es una inversión necesaria, no un gasto opcional.

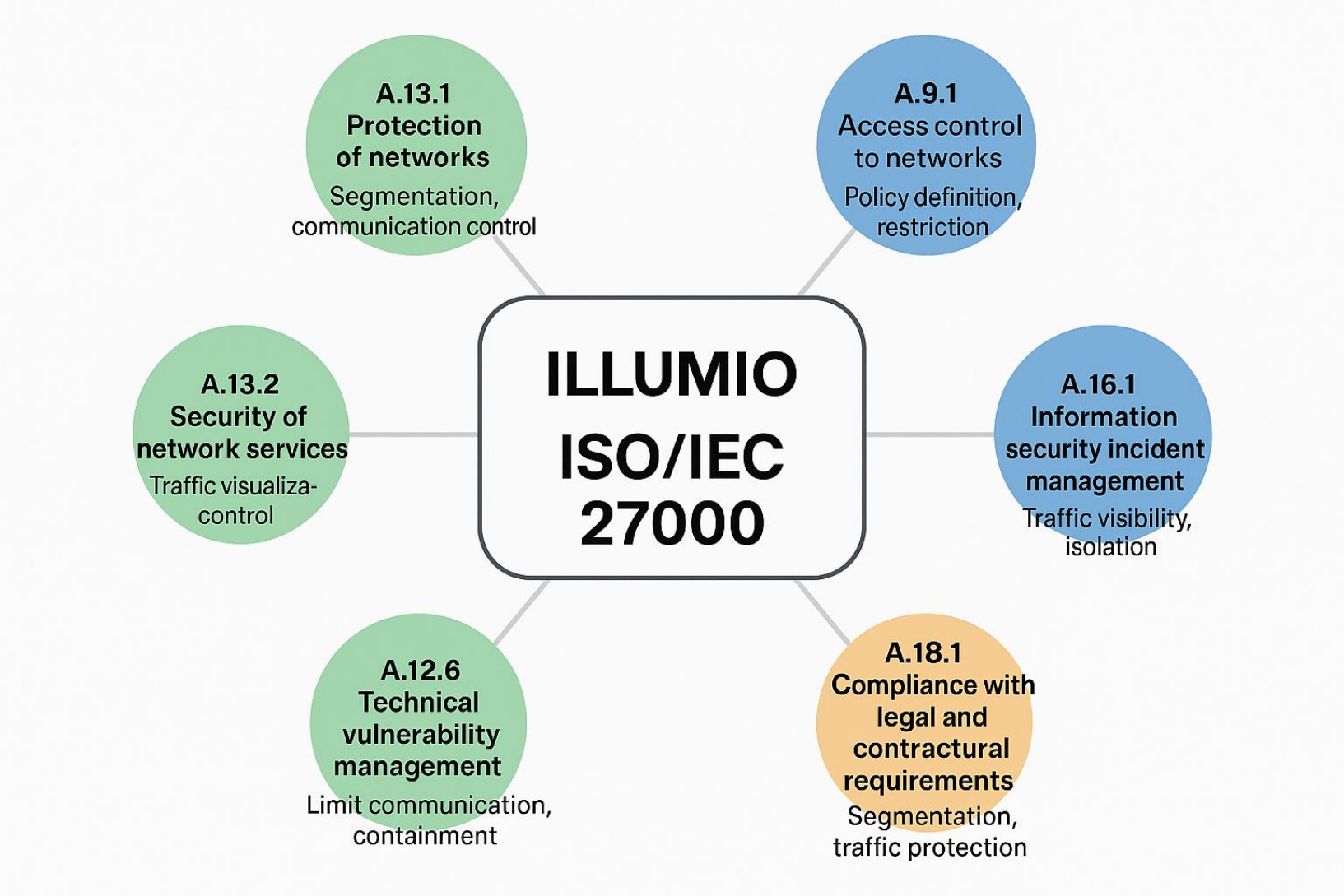
Regulaciones PCI version 4.0

Requisito PCI v4.0	¿Cómo ayuda Illumio?
1.4.2	Segmentación efectiva del CDE
4.2.1	Control de tráfico seguro
6.4.2	Simulación de políticas antes de aplicar
7.2.x	Control granular de acceso entre servicios
10.x	Monitoreo y visibilidad del tráfico
11.4.7	Validación continua de segmentación
12.x	Soporte a políticas de seguridad

NIST – cumplimiento con illumio

Función/Control NIST	Entorno en Nube	Entorno Híbrido (Nube + On-Prem)	Entorno OT / ICS
ID.AM (Asset Management)	Visibilidad de activos y flujos en cargas cloud (AWS, Azure, GCP).	Mapeo dinámico de dependencias entre nube y data center.	Identificación de dispositivos OT conectados y sus comunicaciones.
ID.RA (Risk Assessment)	Evaluación de rutas de ataque internas en entornos cloud.	Análisis de riesgos cruzados entre entornos on-prem y cloud.	Evaluación de exposición y riesgos en redes OT conectadas.
PR.AC (Access Control)	Políticas de segmentación entre servicios cloud.	Control uniforme de acceso entre workloads híbridos.	Segmentación entre dispositivos OT, estaciones de trabajo e interfaces IT.
PR.PT (Protective Technology)	Control lógico de zonas de red y límites entre entornos en la nube.	Aplicación de controles técnicos a nivel de red y host en todos los entornos.	Protección de perímetros OT sin tocar la infraestructura física.
SC-7 (Boundary Protection)	Definición de perímetros lógicos dentro de entornos cloud.	Separación de entornos internos y externos con reglas coherentes.	Aislamiento de redes críticas OT de redes IT corporativas.
SI-4 (System Monitoring)	Visibilidad del tráfico y eventos entre workloads cloud.	Monitorización del tráfico híbrido para detectar comportamientos anómalos.	Seguimiento de comunicaciones industriales en tiempo real.
CM-7 (Least Functionality)	Solo se permiten las conexiones mínimas requeridas entre cargas cloud.	Se limita la conectividad entre aplicaciones a lo esencial, minimizando la superficie.	Se aplica el principio de mínimo privilegio entre PLCs, HMI y estaciones de control.

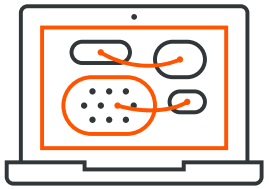
ISO 27000 - illumio



Beneficios de Microsegmentación illumio

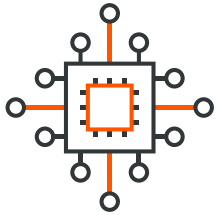
Plataforma avanzada para Zero Trust y Microsegmentación

Visibilidad en tiempo real



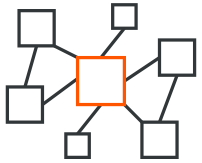
•Proporciona información sobre el movimiento de datos en la red.

Control granular



•Establece políticas específicas para regular la comunicación entre dispositivos.

Implementación sin complicaciones

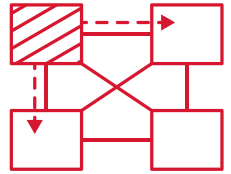


•Facilita la adopción sin cambios en la infraestructura de red.

Adaptabilidad de la plataforma

•Se adapta a entornos locales, en la nube o híbridos.

Prevención de movimientos laterales



•Minimiza el riesgo de desplazamiento de atacantes en la red.

Illumio genera resiliencia al proteger sus activos críticos

La segmentación Zero Trust de Illumio contiene un ataque para detener su propagación

PROTEGIENDO A MÁS DE

20 of the **Fortune 100**

3.5M+ workloads para organizaciones de todos los tamaños, desde Fortune 100 hasta pequeñas empresas

FUNDING

Fundada en2013

Respaldado por inversores como Andreesen Horrowitz y Thoma Bravo

LÍDER DEL MERCADO

Un proveedor representante en el Gartner Market Guide for Microsegmentation

LOS CLIENTES INCLUYEN

BNP PARIBAS

BlueCross BlueShield

BT

CATHAY PACIFIC

DocuSign

Morgan Stanley

ORACLE

QBE

salesforce

servicenow

Illumio nombrado Forrester Wave Leader 2024 en microsegmentación

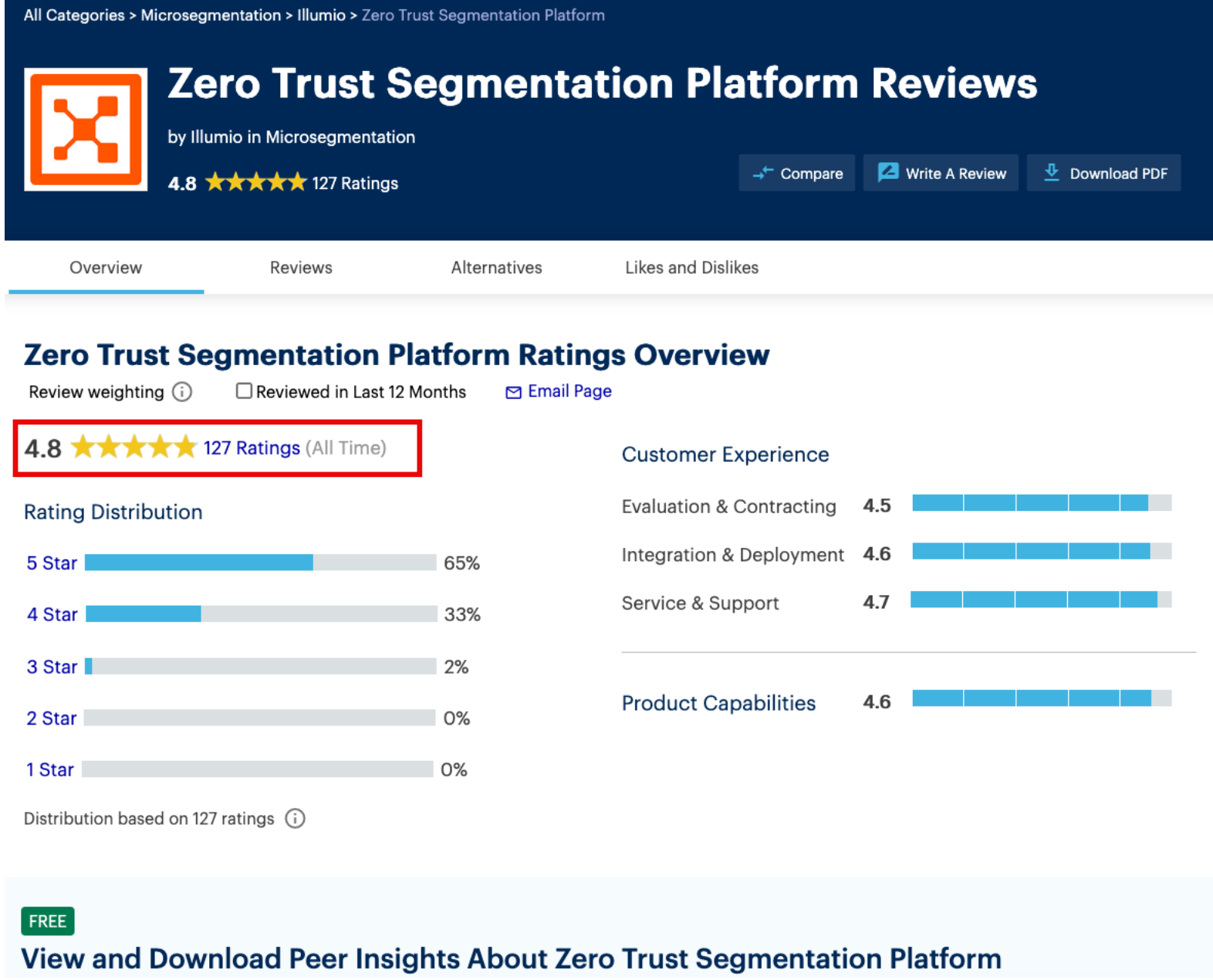
Forrester llama a Illumio "El especialista en microsegmentación original." La firma de investigación agrega que "Grandes organizaciones con programas de ciberseguridad maduros que se encuentren En un zero trust journey o están reforzando las defensas contra el ransomware **debería poner a Illumio en la parte superior de su lista de prioridades."**

Descarga el reporte aqui
Versión en español

Gartner

Peer Insights™

Review link



Thank you