CSURFACE

WHITEPAPER · ATTACK SURFACE MANAGEMENT

La superficie de ataque real y lo que el inventario oficial no registra

Discovery: cómo identificar lo que las plataformas de enumeración de subdominios no revelan — Shadow IT, infraestructura heredada, APIs no documentadas y la cadena digital de proveedores.

CAPACIDAD	PÚBLICO	EDICIÓN
Attack Surface Management	CISO · Security Engineering	2026

LECTURA	CLASIFICACIÓN	FUENTE
11 páginas	Público	Plataforma CSURFACE

RESUMEN EJECUTIVO

El descubrimiento de activos es un problema de inteligencia

La tesis de este whitepaper, en una página — lo esencial antes del detalle técnico.

INCIDENTES POR ACTIVO NO GESTIONADO

74%

de las organizaciones reportaron incidentes causados por activos desconocidos o no gestionados[1]

ATAQUES VÍA ACTIVO EXPUESTO

69%

sufrieron un ataque originado en un activo expuesto en internet, desconocido o no gestionado[2]

DESCUBRIMIENTO CON MACHINE LEARNING

2–3×

más activos que la enumeración de subdominios — y, en superficies dispersas, mucho más

La mayoría de las herramientas de Attack Surface Management (ASM) parte de una premisa frágil: la de que enumerar subdominios a partir de listas públicas es suficiente para cubrir la superficie de ataque. La práctica demuestra lo contrario. La mayor parte de la superficie real se encuentra fuera de esas listas — **Shadow IT contratado sin el conocimiento del área de TI, infraestructura heredada de fusiones y adquisiciones, APIs no documentadas y entornos de homologación expuestos**.

Las investigaciones de mercado independientes convergen en este diagnóstico. Un estudio global de Trend Micro con más de dos mil líderes de seguridad señala que **el 74% de las organizaciones sufrieron incidentes causados por activos no gestionados**[1]; un estudio de Enterprise Strategy Group registra que **el 69% fueron blanco de un ataque originado en un activo expuesto y desconocido**[2]. Lo que permanece fuera del inventario constituye la porción de la superficie sobre la cual no hay observación — el punto ciego operativo sobre el cual ningún control puede actuar.

Este whitepaper presenta el enfoque de CSURFACE: el **Discovery**, que combina recolección pasiva de señales públicas, correlación mediante una stack de motores de Machine Learning, detección de Shadow IT y mapeo de la cadena digital de proveedores — sin agente, sin instalación y sin trabajo manual por activo.

La tesis. El descubrimiento de activos es un problema de inteligencia. La correlación de señales mediante Machine Learning revela lo que las fuentes aisladas — como el DNS público — no alcanzan. Y lo que permanece fuera del inventario permanece sin protección.

Lo que este documento cubre

- Por qué la superficie de ataque creció — y por qué las herramientas no acompañaron.
- Las cuatro brechas estructurales de la enumeración por wordlist.
- Las cuatro técnicas que componen el Discovery, con énfasis en el motor de correlación.
- Un caso de uso representativo y los indicadores de resultado esperados.

EL ESCENARIO · PARTE 01

La superficie se expandió — las herramientas no acompañaron

De qué se compone la superficie de ataque en 2026 y por qué el inventario tradicional ya nace incompleto.

SUPERFICIE DE ATAQUE · ~2014

Pequeña y estable

DNS público | Servidores de correo | VPN

→

SUPERFICIE DE ATAQUE · 2026

Dispersa por toda la operación

DNS público | Correo | VPN | SaaS & Shadow IT | APIs no documentadas | Múltiples nubes | Herencias de M&A | Cadena de proveedores | Entornos efímeros & low-code

74%
de las organizaciones sufrieron incidentes causados por activos desconocidos o no gestionados[1]

69%
fueron blanco de un ataque originado en un activo expuesto y desconocido[2]

~40%
de la infraestructura corporativa permanece invisible para el equipo de TI[4]

Por qué la superficie crece sin gobierno

La superficie de ataque externa no es un inventario organizado — se acumula. Cada equipo de producto publica una aplicación, cada área de negocio contrata un SaaS, cada adquisición incorpora la infraestructura heredada de otra empresa. La ausencia de procesos formales de desactivación hace que esa acumulación rara vez se revierta.

Según Unit 42 (Palo Alto Networks), la superficie de una organización incorpora, en promedio, **más de 300 nuevos servicios por mes**[5]. Un inventario mantenido manualmente no acompaña ese ritmo: se vuelve incompleto a medida que se concluye.

El resultado es una brecha estructural entre la superficie que la organización *cree* tener y la que de hecho expone. Los activos ausentes del inventario permanecen sin observación, sin priorización y sin respuesta — y constituyen el vector preferente de entrada para el atacante.

Por qué esto importa. El inventario es la base de todo programa de seguridad. Sin el conocimiento de lo que existe, la priorización, las pruebas y la respuesta a incidentes operan sobre una base incompleta — y lo que quedó fuera permanece expuesto.

El costo de no ver. El costo medio de una violación de datos en Brasil alcanzó los **€3,90M** en 2025, según el IBM Cost of a Data Breach 2025[3]. La sanción administrativa de la RGPD puede llegar al 2% de la facturación, limitada a €20M. El descubrimiento continuo reduce la probabilidad de incidente al eliminar puntos ciegos — y a cada reducción de probabilidad corresponde una reducción directa y proporcional de la exposición financiera esperada.

LIMITACIONES ACTUALES · PARTE 02

Por qué la enumeración de subdominios no basta

Las plataformas de ASM del mercado se basan en la enumeración de subdominios — un método que resuelve el caso obvio y falla donde el riesgo se concentra.

Whitepaper 2026
CSURFACE

Lo que hacen las plataformas de enumeración de subdominios

Las plataformas de ASM disponibles en el mercado se basan, en esencia, en la enumeración de subdominios: listas de prefijos comunes (**mail.**, **dev.**, **staging.**, **api.**), permutaciones del nombre de la empresa y consultas a fuentes públicas.

Este método localiza **mail.empresa.com** y **staging.empresa.com**. No localiza:

- **api-gtw-prd-v3-fc8a.empresa.com** — identificador generado automáticamente.
- **tenant-b3b9e0.empresa.com** — subdominio multi-tenant.
- Un dominio adquirido en una fusión, con una convención de nombres distinta.
- SaaS alojado en terceros — **empresa.atlassian.net**, **empresa.salesforce.com**.

El punto ciego es estructural. La enumeración de subdominios localiza únicamente lo que alguien imaginó previamente que existiría. El riesgo relevante se encuentra justamente en aquello que no fue previsto — y que, por eso, no fue buscado.

Las cuatro brechas de la enumeración de subdominios

1. **Shadow IT en SaaS de terceros.** Las áreas de marketing, RR. HH. y ventas contratan herramientas que crean URLs públicas vinculadas a la empresa. Ninguna lista genérica las identifica.
2. **Convenciones de nomenclatura propias en la nube.** Cada equipo provisiona recursos con su propio patrón de nombres, al cual una lista genérica no tiene acceso.
3. **Herencias de fusiones y adquisiciones.** Los dominios de empresas adquiridas permanecen activos durante años, sin gobernanza — y la enumeración de subdominios no conoce a la organización incorporada.
4. **Entornos efímeros.** Los pull requests generan entornos de previsualización con URLs únicas, y los pipelines de CI/CD crean hostnames en cada ejecución.

Cada una de estas brechas representa, en la práctica, un punto de entrada ausente de cualquier inventario — no catalogado, no monitoreado y, por lo tanto, no corregido.

EL ENFOQUE CSURFACE · PARTE 03

El motor de correlación — cuando el WHOIS no basta

Recolección pasiva de señales públicas y correlación mediante Machine Learning — las dos primeras capas del Discovery.

Whitepaper 2026
CSURFACE

DISCOVERY · EL PROCESO DE DESCUBRIMIENTO

1. **Recolección pasiva** — Señales públicas, sin tocar la infraestructura.
2. **Recolección activa** — Verificación activa y no intrusiva de los candidatos.
3. **Correlación por ML** — Estima la probabilidad de propiedad de cada activo.
4. **Decisión agéntica** — La capa de correlación resuelve los casos ambiguos y entrega inventario listo para usar.
5. **Stack de tecnologías** — Identificación activa de las tecnologías de cada activo.
6. **Vulnerabilidades y exposición** — Mapeo de las fallas y exposiciones de cada activo.

El WHOIS dejó de ser prueba de propiedad. Actualmente, la mayoría de los dominios opera bajo protección de privacidad o redacción de los datos de registro, lo que mantiene oculto al titular real. La consulta al WHOIS, de forma aislada, ya no establece a quién pertenece un activo — la determinación de propiedad pasó a exigir inferencia, no simple consulta.

01. Recolección pasiva de señales

El descubrimiento se inicia de forma enteramente pasiva. CSURFACE reúne y cruza un amplio conjunto de información pública disponible en internet — un universo de señales considerablemente más amplio que el DNS público sobre el cual se apoyan las plataformas tradicionales.

Ningún paquete se envía a la infraestructura de la organización en esta etapa: la recolección es no intrusiva y no genera ruido en los activos analizados. Esta amplia base de evidencias es la materia prima sobre la cual actúa el motor de correlación.

Cuanto más amplia y diversa sea la base de señales, mayor es la capacidad del motor de correlación de distinguir lo que pertenece a la organización de lo que no pertenece — con la consecuente reducción de atribuciones incorrectas y ampliación de la cobertura real de la superficie.

02. El motor de correlación — una stack de Machine Learning

Si el WHOIS ya no responde a la pregunta sobre la propiedad, CSURFACE la responde por correlación. La información pública recolectada alimenta una **stack de motores de Machine Learning** — cada uno con características propias, entrenado para una lectura distinta de los datos — que operan de forma combinada.

El objetivo es común a todos: identificar patrones y estimar la **probabilidad de que un activo pertenezca a la organización** analizada. La decisión final resulta del consenso de la stack — es ese arreglo colectivo, y no un modelo aislado, el que sostiene la precisión.

Cada atribución viene acompañada de la **probabilidad** y de las evidencias que la sustentan — se trata de un resultado auditable, que el equipo de seguridad puede verificar y cuestionar.

Precisión medida. En operación combinada, la stack de correlación opera **con confianza elevada**. Con ese nivel de confianza, la plataforma identifica la propiedad de dominios, organizaciones, aplicaciones web, FQDNs, direcciones IP y demás clases de activo.

LO QUE CSURFACE OBSERVA · DATOS PROPIOS DE LA PLATAFORMA

122 mil
activos externos descubiertos en 68 organizaciones analizadas por la plataforma

1.068
organizaciones relacionadas — subsidiarias y coligadas — reveladas por el descubrimiento

hasta 173
organizaciones relacionadas mapeadas a partir de un único dominio raíz

EL ENFOQUE CSURFACE · PARTE 03

Shadow IT, cadena de proveedores y el resultado medible

Las dos técnicas restantes — y lo que el enfoque cambia, lado a lado con la enumeración tradicional.

03. Detección de Shadow IT

La plataforma identifica el SaaS de terceros conectado a la organización — herramientas contratadas por las áreas de negocio que crean presencia pública vinculada a la empresa. Este Shadow IT, invisible para el inventario oficial, es reconocido por la correlación de múltiples indicios públicos que lo asocian al cliente.

04. Mapeo de la cadena de proveedores

Para cada activo descubierto, la plataforma mapea las APIs externas invocadas, los CDNs y el JavaScript de terceros, los proveedores de nube compartidos y las bibliotecas embebidas — la cadena digital de proveedores que expande la superficie sin constar en ningún inventario.

Un especialista dedicado. Para las grandes plataformas de seguridad, el producto central es el scanner y la gestión de vulnerabilidades; el módulo de ASM fue añadido posteriormente, como un componente accesorio que solo alimenta el motor ya existente — y en el cual la velocidad y la precisión del descubrimiento no constituyen una prioridad. CSURFACE adopta la posición opuesta: el descubrimiento es el producto. La plataforma fue concebida como un instrumento dedicado a mantener al cliente al tanto de su exposición en el menor tiempo y con la mayor precisión posibles.

Diferenciadores medibles

CRITERIO	ENUMERACIÓN DE SUBDOMINIOS	CSURFACE · ML DISCOVERY
Cobertura típica de la superficie	Parcial	**Amplia y contextual**
Detección de Shadow IT	Limitada o inexistente	**Activa**
Esfuerzo manual por activo	3–10 horas	**Cero**
Frecuencia	Puntual / programada	**Continua, 24/7**
Profundidad de la cadena de proveedores	Un nivel, cuando lo hay	**Hasta tres niveles**
Entrada necesaria	Lista de activos conocida	**Solo el dominio raíz**

Rangos observados en descubrimientos conducidos por la plataforma CSURFACE; ver la nota metodológica en la página 10. El resultado varía según el tamaño y la dispersión de la superficie de cada organización.

APLICACIÓN Y RESULTADOS · CASO 01

Una startup de ERP: de 84 a 570 activos

Lo que un inventario de gestión de vulnerabilidades dejaba fuera — y que el descubrimiento continuo hizo visible y priorizable.

INVENTARIO POR LA GESTIÓN DE VULNERABILIDADES

84

activos — lo que la empresa creía que era toda su exposición externa.

→

MAPEADO POR CSURFACE

570

activos en la superficie real — **casi 7×** el inventario conocido.

El caso

Una startup de software ERP seguía su exposición externa mediante una plataforma tradicional de gestión de vulnerabilidades. El inventario registraba **84 activos**, y el equipo creía que ese número representaba la totalidad de su superficie de ataque.

En pocos minutos de descubrimiento con CSURFACE, la superficie real se reveló compuesta por **570 activos**. Entre lo que estaba expuesto y fuera del radar:

ATENCIÓN **Certificados digitales expirados**
En servicios aún accesibles por internet.

ATENCIÓN **Software en fin de vida (EoL)**
Activos heredados sin soporte del proveedor ni parches de seguridad.

CRÍTICO **Vulnerabilidades invisibles**
En activos que el inventario ni siquiera conocía — por lo tanto, jamás evaluados.

CRÍTICO **Datos sensibles expuestos**
Errores de configuración que exponían datos de sistemas internos.

CRÍTICO **Paneles administrativos expuestos**
De alto riesgo; deberían estar restringidos a la red interna.

En conjunto, estos hallazgos configuraban un perfil de riesgo significativamente superior al nivel aceptable por la organización — sin que ninguno de ellos hubiera sido catalogado o evaluado.

Por qué pasó desapercibido

Una plataforma tradicional de gestión de vulnerabilidades examina únicamente lo que se le informa: enumera una lista suministrada, mientras el descubrimiento contextual mapea la superficie real. Todo lo que no constaba en la lista de 84 activos permanecía, por definición, invisible.

Un patrón recurrente. Según Unit 42 (Palo Alto Networks), la superficie de ataque de una organización incorpora, en promedio, **más de 300 nuevos servicios por mes**[5]; y más del **25% de las exposiciones** involucran infraestructura crítica de TI — incluyendo páginas de login administrativas accesibles por internet[5]. Un inventario estático se vuelve progresivamente incompleto a medida que la superficie evoluciona.

El resultado

La ganancia inmediata fue la **visibilidad**: de 84 activos presumidos a 570 euros, el riesgo dejó de ser invisible y pasó a ser priorizable. La gestión efectiva de la exposición presupone, como condición previa, el conocimiento completo de la superficie a gestionar.

APLICACIÓN Y RESULTADOS · CASO 02

Un gran banco: empresas enteras fuera del inventario

Crecimiento por adquisiciones, superficie en cambio constante y confianza excesiva en las herramientas tradicionales.

El punto de partida

El banco llegó a CSURFACE con tres cuestiones abiertas:

Sin visibilidad de la superficie externa
Falta de control sobre lo que estaba, de hecho, expuesto.

Confianza excesiva en lo tradicional
Las herramientas existentes solo veían el inventario ya conocido.

Riesgo en la cadena y en las adquisiciones
Cada empresa adquirida ampliaba la superficie sin gobernanza.

Lo que el descubrimiento reveló

Un gran banco — reconocido por su actuación en asset management y por un historial de grandes adquisiciones en los últimos años, de operaciones de logística a cadenas de hoteles — convivía con una superficie en cambio permanente. El entorno corporativo, las múltiples nubes y cada nueva adquisición pasaban a ser responsabilidad del equipo de seguridad cibernética.

Tras algunas semanas con la plataforma CSURFACE, el banco identificó **estructuras de empresas enteras — dentro y fuera del país — que no estaban bajo su radar**. Parte de ellas presentaba vulnerabilidades y exposiciones que exigieron intervención urgente.

El volumen y la dispersión superaron las estimaciones internas: activos distribuidos por múltiples nubes y estructuras corporativas enteras que ningún equipo había mapeado, sin responsable designado, sin monitoreo y sin ningún proceso de respuesta establecido.

Corrección dentro de la ventana crítica. En uno de los activos, la plataforma detectó una vulnerabilidad de impacto **9.8 (CVSS)** el mismo día de su divulgación pública. El equipo de seguridad fue alertado y la corrigió aún dentro del período crítico — cuando la falla ya era explotada en internet. Un incidente potencialmente severo fue evitado.

Adopción por la gobernanza. Los equipos de gobernanza de la seguridad de la información (GSI) pasaron a usar la plataforma para documentar y comprender organizaciones y activos sobre los cuales, hasta entonces, no había ninguna visibilidad.

La lectura

En una organización que crece por adquisición, la superficie de ataque cambia más rápido que cualquier proceso manual de inventario. El descubrimiento continuo deja de ser una conveniencia y se convierte en condición para gobernar el riesgo.

APLICACIÓN Y RESULTADOS · CASO COMPLEMENTARIO

Anatomía de un phishing perfecto — evitado

Cómo un subdominio no gestionado y un registro SPF desactualizado crearon las condiciones para un phishing con infraestructura legítima del banco.

El secuestro de un dominio autorizado en el SPF

El riesgo nace de una distinción sutil entre **dos dominios diferentes**: el **subdominio del propio banco**, que contiene el registro SPF, y el **dominio de un tercero**, que ese registro autoriza a enviar correos. Cuando el segundo es abandonado, el primero continúa confiando en él.

El vector compuesto — SPF secuestrado sumado al subdomain takeover

La plataforma identificó, en el mismo banco, **subdominios susceptibles de takeover** — apuntando a servicios de nube desactivados y, por eso, reclamables por terceros. Combinadas, las dos fallas permitirían un phishing casi indetectable: un correo enviado desde un dominio legítimo del banco — vía SPF secuestrado — conteniendo un enlace a otro dominio legítimo del banco — vía subdominio secuestrado. Para el cuentahabiente, todas las señales apuntarían al banco verdadero.

El desenlace. Ninguna de las dos fallas era visible para las herramientas tradicionales del banco — ambas vivían en activos fuera del inventario. CSURFACE las señaló, y el banco corrigió los registros y los subdominios antes de que fueran encontrados. La campaña real SubdoMailing — que llegó a enviar millones de correos por día a partir de dominios legítimos secuestrados[6] — confirma que la amenaza es real.

METODOLOGÍA Y FUENTES

El origen de cada número

Cómo este documento distingue la investigación de mercado pública de las métricas observadas por la plataforma.

Nota metodológica

Este whitepaper combina dos naturalezas de dato, mantenidas distintas a lo largo del texto:

Estadísticas de mercado. Atribuidas, en el punto de uso, a investigaciones públicas de terceros e identificadas por un marcador numérico. Las referencias completas constan al lado.

Métricas de la plataforma. Indicadores como la cobertura amplia de la superficie y la ganancia material en activos descubiertos resultan de descubrimientos conducidos por la propia plataforma CSURFACE. Varían según el tamaño y la dispersión de la superficie de cada organización.

Ninguna estadística se presenta sin fuente. Los casos descritos se basan en engagements reales y son anonimizados — ninguna organización es identificada.

Material educativo. Este documento está destinado a fines informativos. Las metodologías descritas reflejan el estado de la plataforma CSURFACE en la fecha de publicación.

Referencias

1. **Trend Micro.** Investigación global sobre incidentes de seguridad causados por activos no gestionados, conducida con más de 2.000 líderes de seguridad. 2025.
2. **Enterprise Strategy Group.** Investigación sobre la explotación de activos expuestos en internet, desconocidos o no gestionados. Reportada por SC Media.
3. **IBM.** Cost of a Data Breach Report 2025 — costo medio de violación de datos en Brasil: €3,90M.
4. **Gartner.** Análisis sobre visibilidad de infraestructura corporativa y External Attack Surface Management (EASM).
5. **Unit 42 (Palo Alto Networks).** 2024 Attack Surface Threat Research — exposiciones de infraestructura conectada a internet y ritmo de crecimiento de la superficie de ataque.
6. **Guardio Labs.** SubdoMailing — investigación sobre el secuestro de subdominios y registros SPF para campañas de phishing a gran escala. 2024.

Las estadísticas de mercado citadas tienen carácter público. Los porcentajes pueden variar según la metodología y el recorte muestral de cada estudio.

PRÓXIMOS PASOS

El descubrimiento comienza con un único dominio

El Discovery es una de las capacidades de la plataforma CSURFACE — una plataforma de Continuous Exposure Management. En una plataforma integrada, reúne descubrimiento continuo de la superficie externa, análisis de la cadena digital de proveedores, validación de explotabilidad, inteligencia de amenazas con priorización dinámica y monitoreo de credenciales filtradas. Opera de forma enteramente externa — sin agente y sin instalación —, con integraciones opcionales de nube, WAF y CIEM para organizaciones que necesitan mayor profundidad analítica.

Reciba el análisis preliminar
Indique el dominio de su empresa y reciba, sin costo, un retrato de los activos expuestos descubiertos por la plataforma.

Use la calculadora de riesgo
Estime la pérdida anual esperada (ALE) y el VaR de su sector, con metodología FAIR calibrada por benchmark de mercado.

Lea el próximo whitepaper
Cadena Digital de Proveedores — el caso Polyfill.io y cómo mapear dependencias en tres niveles.

Vea su superficie real — descubierta con el dominio raíz como única entrada

Recibir análisis preliminar gratuito