CSURFACE

WHITEPAPER · VENTANA DE EXPOSICIÓN

La ventana de exposición entre el escaneo programado y la corrección

En tres años, el tiempo medio entre la publicación de una vulnerabilidad y el primer exploit cayó de 32 a 5 días — y el ciclo de la gestión de vulnerabilidades tradicional, puntual y mensual, ya no acompaña el ritmo.

CAPACIDAD **Gestión Continua de Exposición**	PÚBLICO **CISO · Riesgo · GestVuln · SOC**	EDICIÓN **2026**
LECTURA **14 páginas**	CLASIFICACIÓN **Público**	FUENTE **Plataforma CSURFACE**

RESUMEN EJECUTIVO

El exploit es más rápido — y su ventana está abierta

La tesis de este whitepaper en una página, con datos de la telemetría de emerging threats de CSURFACE: la velocidad de la explotación y el ciclo de la gestión de vulnerabilidades ya no se encuentran.

Whitepaper 2026
CSURFACE

EXPLOITS EN ≤ 5 DÍAS · 2024 VS. 2020

+183%

153 CVE explotados en ≤ 5 días en 2024 — frente a 54 en 2020[1]

CICLO TÍPICO DE GESTVULN

30 días

escaneo mensual — el intervalo mínimo entre fotografías

ZERO-DAYS ANTES DEL DISCLOSURE · 2026*

52%

de los zero-days observados en 2026 ya fueron explotados antes de la publicación del CVE — frente al 21% en 2025[1]

La telemetría de emerging threats de CSURFACE registra que **153 CVE fueron explotados en ≤ 5 días tras el disclosure en 2024** — casi tres veces los 54 de 2020. En 2026, solo en los primeros meses, ya son 81. El salto ocurrió en 2024 y la franja anual se estabilizó en un nivel estructuralmente más alto que en cualquier año anterior. La aceleración es lo que la telemetría ha registrado año tras año.

La gestión de vulnerabilidades tradicional, basada en escaneos periódicos, opera a un ritmo heredado de otra era. Un ciclo mensual — ya considerado bueno en muchas organizaciones — entrega una fotografía del parque cada 30 días. El ciclo trimestral o anual entrega una fotografía aún más desfasada. Entre una fotografía y la siguiente, la ventana de exposición permanece abierta — y el atacante dispone de tiempo suficiente para entrar.

Este whitepaper analiza la aceleración de la explotación a lo largo de los últimos tres años, expone la brecha matemática entre la velocidad del atacante y el ciclo del tradicional, y presenta el enfoque de CSURFACE — descubrimiento continuo, threat sensor y priorización dinámica — para cerrar esa ventana en horas, no en semanas.

La tesis. Ventana de exposición es el intervalo entre el momento en que una vulnerabilidad se vuelve explotable y el momento en que la organización aplica el control correspondiente. Solo puede cerrarse mediante un instrumento que opere de forma continua, a la misma cadencia del atacante.

Qué cubre este whitepaper

- La aceleración de la explotación — tendencia de 3 años, con datos públicos.
- Siete casos públicos recientes — explotación en horas y días.
- La anatomía de la ventana de exposición y por qué el ciclo puntual no la cierra.
- El enfoque de CSURFACE — threat sensor, descubrimiento y priorización continuos.

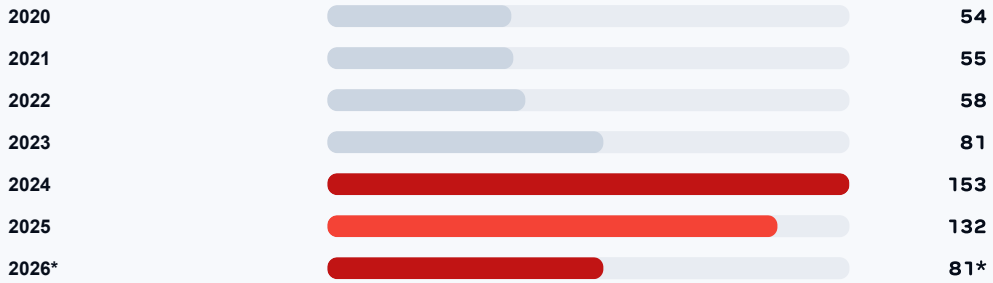
LA ACELERACIÓN · PARTE 01

De 54 a 153 en cuatro años · el salto del exploit rápido

El número de CVE explotados en ≤ 5 días tras la divulgación casi se triplicó entre 2020 y 2024 — lectura del sensor propio de emerging threats de CSURFACE.

Número absoluto de CVE explotados en ≤ 5 días · por año

La telemetría de emerging threats de CSURFACE sigue, año a año, el número absoluto de CVE cuya explotación en producción se observó dentro de los 5 días tras la divulgación pública. La serie de siete años muestra un régimen estructuralmente nuevo a partir de 2024 — casi tres veces la base de 2020:



Fuente: telemetría de emerging threats de CSURFACE. *2026 cubre solo los primeros meses del año. El salto entre 2023 (81) y 2024 (153) marca la entrada en un régimen estructuralmente diferente — corroborado por Mandiant M-Trends 2024, que reporta una caída de la mediana de TTE a 5 días.[2]

Lo que CSURFACE observó en los últimos tres años

1. **Volumen de CVE al alza.** La NVD publicó 18.362 CVE en 2020. En 2025, fueron **48.126** — casi 2,6× el volumen de cinco años antes. La presión sobre las colas de remediación aumentó en proporción.
2. **Los zero-days se duplicaron en 2024.** CSURFACE registró 57 zero-days en 2023, **103 en 2024** y 89 en 2025. En 2026, ya son 64 en los primeros meses — un ritmo que proyecta un nuevo récord anual.
3. **Explotación antes del disclosure.** En 2025, el 21% de los zero-days fueron explotados antes de que el CVE se hiciera público. En 2026, **52%** — más de la mitad. El atacante llega antes de que el registro exista.
4. **El salto de 2024 fue estructural.** El número de exploits en ≤ 5 días pasó de 81 (2023) a 153 (2024) — un crecimiento del 88% en un año. 2025 registró 132; 2026, en pocos meses, ya llega a 81. La franja anual se estabilizó en un nivel estructuralmente nuevo.

La implicación. El paso de 54-81 a 132-153 exploits rápidos por año es estructural. Refleja una reorganización del ecosistema ofensivo — automatización, explotación asistida por IA, especialización y mercado de exploits — que perdurará. El instrumento defensivo debe operar en una escala temporal comparable.

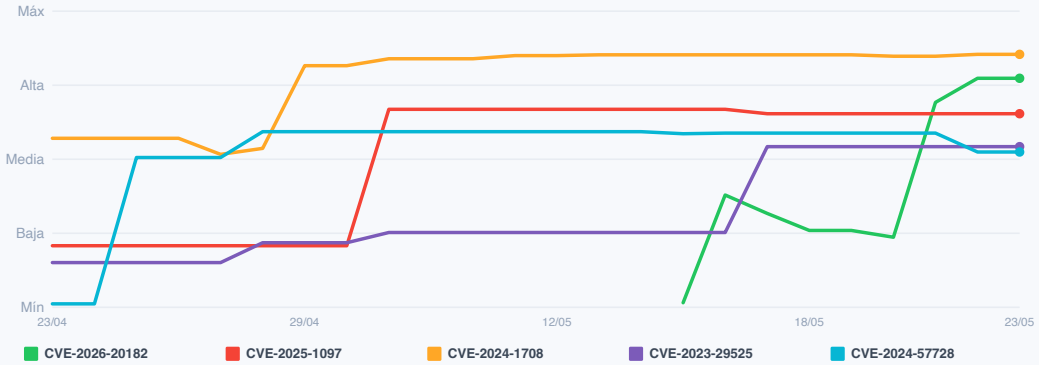
EXPLOTACIÓN DINÁMICA · PARTE 02

CVE dormidos que despertaron · lo que el CVSS por sí solo ignora

Cinco vulnerabilidades reales cuya probabilidad de explotación más que se duplicó en las últimas semanas — observadas por la telemetría de emerging threats de CSURFACE.

Por qué esto importa. El CVSS expresa la gravedad *teórica* de la falla — asignado en la publicación y rara vez actualizado. El **índice de probabilidad de explotación** expresa la probabilidad real de explotación en los próximos 30 días y cambia a diario. Una vulnerabilidad puede dormir durante meses con una probabilidad de explotación baja y, en pocos días, ver su índice multiplicado por 10× o 50× cuando surgen exploits, PoCs o campañas. Quien prioriza solo por CVSS pierde ese movimiento.

PROBABILIDAD DE EXPLOTACIÓN · 30 DÍAS · 5 CVE CON MAYOR CRECIMIENTO



Las cinco vulnerabilidades del gráfico

CVE	PRODUCTO AFECTADO	PROBABILIDAD MÍN → ACTUAL	SEÑALES
CVE-2026-20182	Cisco Catalyst SD-WAN Manager	**Baja → Inminente**	ACTIVA EXPLOIT
CVE-2025-1097	Kubernetes ingress-nginx	**Moderada → Elevada**	rising
CVE-2024-1708	ConnectWise ScreenConnect	**Elevada → Crítica**	ACTIVA EXPLOIT
CVE-2023-29525	XWiki Platform	**Baja → Elevada**	dormido en 2023, reactivado
CVE-2024-57728	SimpleHelp Remote Access	**Baja → Elevada**	ACTIVA

Fuente: telemetría de emerging threats de CSURFACE. Captura diaria del índice de probabilidad de explotación, del catálogo de explotación activa y de la disponibilidad pública de exploit. Snapshot: 23 de mayo de 2026.

Lo que el CVSS por sí solo no ve

La CVE-2026-20182 (Cisco Catalyst SD-WAN Manager) tenía una probabilidad de explotación baja el 15 de mayo. Siete días después, el índice ya la clasificaba entre las de explotación inminente — sin ninguna alteración en el CVSS. Una cola basada solo en CVSS, recalculada una vez al mes, mantendría esa CVE en medio del bloque. Una cola dinámica la empuja a la cima el día en que la señal aparece.

Priorización inteligente y continua. CSURFACE compone la cola combinando el índice de probabilidad de explotación actual, el delta de 30 días, el catálogo de explotación activa, el exploit público y la telemetría de explotación activa — reflejando el presente de la amenaza en lugar de un score asignado meses antes.

CASOS PÚBLICOS · PARTE 02

Siete incidentes recientes · explotación en horas y días

Siete incidentes públicos con explotación masiva dentro de los 15 días tras el disclosure — todos post-CVE, todos dentro del ciclo de escaneo de la mayoría de las organizaciones.

El patrón detrás de los siete casos. Cada incidente a continuación fue explotado en producción dentro de una ventana de hasta **15 días tras el disclosure público** — en varios casos, en **menos de 24 horas**. Todos post-CVE, todos dentro del intervalo de un escaneo mensual. Ninguno de ellos sería capturado a tiempo por la gestión de vulnerabilidades tradicional.

CRÍTICO **Log4Shell · CVE-2021-44228**

Divulgada el 9 de diciembre de 2021. Cloudflare y Cisco Talos registraron intentos de explotación a gran escala en las primeras horas tras el disclosure. RCE remoto no autenticado en millones de aplicaciones Java. Siguió siendo explotada en producción durante meses tras el patch.

Tiempo hasta la explotación masiva · ≤ 24 horas

CRÍTICO **Spring4Shell · CVE-2022-22965**

Divulgada el 30 de marzo de 2022. PoC público en 24 horas, explotación activa en ~48 horas tras el disclosure. Explotación masiva por botnets variantes de Mirai observada por múltiples vendors. RCE en Spring Framework — stack web ampliamente adoptado en corporaciones.

Tiempo hasta la explotación masiva · 24-48 horas

CRÍTICO **VMware vRealize · CVE-2022-22954**

Divulgada el 6 de abril de 2022. Sophos, Rapid7 y Morphisec detectaron explotación activa durante ~3 días tras el disclosure, con cryptominers y shells reversos. RCE vía template injection en Workspace ONE Access — objetivo de operaciones de movimiento lateral en redes corporativas.

Tiempo hasta la explotación masiva · ~3 días

CRÍTICO **F5 BIG-IP · CVE-2022-1388**

Divulgada el 4 de mayo de 2022. PoCs públicos en ~4 días, explotación activa masiva alrededor del 9 de mayo. Un bypass de autenticación en iControl REST permitía RCE con privilegio root. Cientos de instancias expuestas comprometidas en pocos días.

Tiempo hasta la explotación masiva · ~5 días

CRÍTICO **Citrix Bleed · CVE-2023-4966**

Divulgada el 10 de octubre de 2023. Explotación masiva post-disclosure observada en ~10 a 14 días — afectando a Boeing, Comcast y decenas de otras. Captura de sesión sin autenticación adicional, con bypass efectivo de MFA vía cookie robada.

Tiempo hasta la explotación masiva · ~10-14 días

CRÍTICO **ScreenConnect AuthBypass · CVE-2024-1709**

Divulgada el 19-20 de febrero de 2024 por ConnectWise. Bypass de autenticación trivial (creación de usuario admin vía path manipulation). Explotación masiva observada en menos de 24 horas — Huntress, Sophos y CISA emitieron alertas urgentes.

Tiempo hasta la explotación masiva · ≤ 24 horas

CRÍTICO **CrushFTP · CVE-2024-4040**

Divulgada el 19 de abril de 2024. CrowdStrike y Rapid7 detectaron explotación activa en horas. Path traversal permitía la lectura de archivos sensibles sin autenticación, incluyendo configuraciones y secretos. Cientos de instancias expuestas comprometidas el primer día.

Tiempo hasta la explotación masiva · ≤ 24 horas

ATENCIÓN **La conclusión: anticipar deja de ser un refinamiento**

Los siete incidentes comparten un denominador: el intervalo entre el disclosure y la explotación masiva se midió en **horas o días**, nunca en semanas. Cualquier defensa que opere en ciclo mensual — o peor, trimestral — llega después. La capacidad de anticipar el exploit, captando la señal de riesgo antes de la explotación, se convierte en la **arquitectura más alineada con la velocidad actual del atacante** en la gestión de exposición.

VENTANA DE EXPOSICIÓN · PARTE 03

Anatomía de la ventana · del disclosure al patch aplicado

Cuatro hitos definen la ventana de exposición. El intervalo entre el segundo y el cuarto es donde el ataque ocurre.

Definición operativa. Ventana de exposición es el intervalo durante el cual una vulnerabilidad es explotable en la superficie de una organización — comienza cuando el exploit se vuelve viable y termina cuando el control correspondiente se aplica. Cuanto mayor la ventana, mayor la probabilidad de explotación.

Los cuatro hitos de la ventana

0. **Pre-disclosure.** La vulnerabilidad existe en el código y puede estar siendo explotada por actores con conocimiento privilegiado — zero-day. Para la defensa, ese periodo es invisible por definición. En 2023, varios incidentes comenzaron en esta zona.
1. **Disclosure (T0).** El CVE se publica, con o sin patch disponible. La información se hace pública — y el reloj del atacante empieza a correr a la misma velocidad que el reloj de la defensa.
2. **Exploit observado (T1).** El primer exploit se registra en producción. En 2023, la mediana entre T0 y T1 fue de **5 días** — en muchos casos, menos de 24 horas. Aquí se abre la fase más peligrosa de la ventana.
3. **Patch aplicado (T2).** La organización aplica el control en el activo afectado. El Verizon DBIR observa, año tras año, una **mediana cercana a 55 días** entre el disclosure y la corrección en producción.[4]

El cálculo de la ventana abierta. Mediana de exploit en **5 días**, mediana de remediación en **55 días**. La ventana es el intervalo entre los dos — **~50 días por vulnerabilidad crítica**, en promedio, para la organización típica que opera en el ciclo tradicional de gestión de vulnerabilidades.

La pregunta defensiva

Si el exploit llega en 5 días y el patch aplicado tarda 55, la defensa tiene tres palancas técnicas para reducir la ventana:

- **Anticipar la detección** — observar la exposición antes del disclosure, vía inteligencia de amenaza y telemetría de borde.
- **Priorizar lo que está siendo explotado** — no tratar todos los CVE por igual.
- **Acortar el ciclo de descubrimiento y validación** — pasar de la fotografía mensual al flujo continuo.

LA CURVA HISTÓRICA · PARTE 04

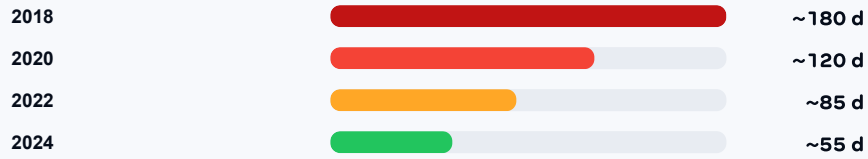
Adopción de ASM × tiempo de remediación · una correlación inversa

A medida que las plataformas de ASM ganaron adopción en mercados maduros, el tiempo medio de remediación cayó. El movimiento ocurrió en EE. UU. y en Europa. Brasil todavía está en la curva.

Whitepaper 2026
CSURFACE

La coincidencia con una causa. Entre 2018 y 2024, el tiempo medio de remediación de CVE críticos en organizaciones de EE. UU. y de Europa cayó de cerca de 180 a 55 días — una reducción de aproximadamente el 70%. En el mismo periodo, el mercado global de Attack Surface Management creció a una tasa compuesta anual estimada en ~27-29% (CAGR), alcanzando un múltiplo de cerca de 4,5× el tamaño de 2018. Los dos movimientos son, en gran medida, el mismo movimiento.

Mediana de tiempo hasta remediación · CVE críticos



Fuentes: Edgescan Vulnerability Stats Report (series 2019-2023), Verizon DBIR 2024. Mediana global; mercados EE. UU. y Europa.

Mercado de ASM · multiplicador acumulado vs. 2018

Fuentes: MarketsandMarkets, Allied Market Research, 360iResearch (series 2022-2030 normalizadas a base 2018). CAGR estimado: ~27-29%.

La correlación observada

La caída del tiempo de remediación no fue lineal ni uniforme. Los mercados que adoptaron pronto ASM dedicado — EE. UU. y Europa Occidental — concentraron la mayor parte de la reducción. Las industrias con regulación fuerte (finanzas, defensa, infraestructura crítica) impulsaron la curva. Cuando dos curvas opuestas se cruzan con esa consistencia a lo largo de seis años, la correlación pasa de hipótesis a lectura razonable: la adopción de plataformas especializadas en descubrimiento continuo y priorización dinámica es el instrumento técnico que hizo posible acortar la ventana.

No es el único factor — la automatización de pipelines, la telemetría de cloud y la maduración de procesos contribuyeron. Pero ASM es el componente que, en esos mismos seis años, pasó de categoría nicho a partida de presupuesto estándar en programas de seguridad corporativos.

Brasil · dónde está el retraso. La adopción de ASM especializado en Brasil se concentra en el sector financiero, impulsada por la regulación BACEN. Fuera de él, la mayoría de las organizaciones aún opera el ciclo tradicional de gestión de vulnerabilidades — mensual o trimestral. El tiempo medio de remediación en el mercado brasileño permanece en una franja observada en EE. UU. y Europa en 2020-2021, con un desfase estimado de 3 a 4 años respecto a la curva más avanzada.

El ASM adyacente × el ASM especializado. Muchas suites amplias de TI corporativa incorporaron módulos de External Attack Surface Management alrededor del producto principal, orientados sobre todo al inventario y, en algunos casos, al descubrimiento. Una plataforma dedicada se organiza en torno a la **velocidad de detección** y la **priorización dinámica** — la diferencia que determina si la ventana de exposición será de días o de meses.

EL PARADIGMA PUNTUAL · PARTE 04

La gestión de vulnerabilidades tradicional · una fotografía que envejece

El ciclo de escaneo anual y mensual fue diseñado para un mundo en el que el exploit llegaba en meses — no en días.

Lo que el ciclo puntual entrega — y lo que pierde

La gestión de vulnerabilidades tradicional opera en ciclos. El scanner se programa para barrer el parque en una cadencia fija — anual en muchas organizaciones, trimestral en las más maduras, mensual en las que más invierten en seguridad. Cada ejecución es una fotografía: registra el estado del parque en el instante en que el escaneo se ejecutó.

Entre una fotografía y la siguiente, la realidad cambia. Nuevos activos suben a la nube. Se alteran configuraciones. Las bibliotecas reciben versiones. Se divulgan nuevas vulnerabilidades. Todo esto queda fuera del registro hasta la siguiente ejecución del scanner — y, al llegar allí, se suma al flujo de hallazgos que entra en la cola de remediación.

Ese modelo funciona cuando la velocidad del atacante es comparable a la cadencia del escaneo. En 2015, con un tiempo medio de exploit superior a 100 días, un escaneo mensual estaba razonablemente alineado con la amenaza. En 2023, con el exploit en 5 días, la fotografía mensual muestra un estado que ya no existe — y la ventana permanece abierta entre fotografías.

La brecha matemática · ventana abierta por ciclo de GestVuln

CADENCIA DEL ESCANEO	VENTANA MÁXIMA ENTRE ESCANEOS	VS. EXPLOIT EN 5 D
Anual	365 días	**73× la ventana del atacante**
Trimestral	90 días	**18× la ventana del atacante**
Mensual	30 días	**6× la ventana del atacante**
Semanal	7 días	1,4× la ventana del atacante
Continuo	< 1 día	**alineado con la amenaza**

El escaneo que se ejecuta una vez al mes deja a la organización en una ventana seis veces mayor que la del atacante mediano. En activos críticos, esta proporción es la diferencia entre detectar una vulnerabilidad antes o después de la explotación.

El retraso adicional del proceso. El escaneo es solo el punto de partida. Triaje, asignación, ventana de mantenimiento, validación y re-escaneo extienden el ciclo total. En organizaciones de porte medio, la mediana entre detección y remediación de un CVE crítico permanece en torno a **55 días**, según el Verizon DBIR — incluso cuando el escaneo opera mensualmente.[4]

EL COSTE DE LA VENTANA · PARTE 05

El precio de una ventana abierta · en días y en euros

La ventana de exposición es, en esencia, una métrica de riesgo financiero — cuanto mayor, más alta la probabilidad y el coste del incidente.

241 días
tiempo medio para identificar y contener una brecha · Informe IBM Cost of a Data Breach 2025[5]

€3,90M
coste medio de una brecha en Brasil — IBM 2025

–US$ 0,5 mi
coste medio menor cuando la detección y la contención ocurren en menos de 200 días (US$ 4,93 mi vs. US$ 5,46 mi)

La correlación entre ventana y coste

El Informe IBM Cost of a Data Breach 2025 documenta, año tras año, una correlación inequívoca: **cuanto mayor el tiempo entre el compromiso y la detección, mayor el coste final del incidente**. Las organizaciones que detectaron y contuvieron en menos de 200 días gastaron, en promedio, US$ 4,93 millones — frente a US$ 5,46 millones en las que tardaron más de 200 días. La diferencia es estructural.

El motivo es matemático. Un atacante con más tiempo dentro del perímetro tiene más activos descubiertos, más privilegios acumulados, más datos accedidos y más tiempo para preparar el movimiento lateral y la exfiltración. Cada día de ventana abierta amplía, simultáneamente, la probabilidad y la magnitud de la pérdida.

La ventana de exposición, en esta lectura, constituye el **parámetro central** que vincula la postura técnica de una organización con su exposición financiera. Reducirla es la palanca más directa de reducción de coste esperado.

El coste de la ventana en el lenguaje del CFO. Cada día de ventana abierta tiene un coste esperado proporcional a la probabilidad de explotación en ese día y al impacto financiero del incidente correspondiente. Para una vulnerabilidad crítica en un activo de producción, ese coste diario puede estimarse en miles de euros por día expuesto — composición que se convierte en la base del cálculo de ROI de la remediación.

El efecto compuesto sobre el portafolio

En una organización con cientos de activos y decenas de vulnerabilidades críticas abiertas en cualquier momento, el coste de la ventana es acumulativo. Evaluar la ventana de un solo activo no basta — es necesario sumar el coste esperado de cada ventana abierta en el portafolio.

La reducción media de 50 días a 10 días de ventana en una vulnerabilidad crítica corresponde, en ALE, a una **reducción material** de la exposición esperada de esa vulnerabilidad. Aplicada al portafolio entero, la reducción de ventana se convierte en la palanca de mayor retorno del programa de seguridad.

MONITOREO CONTINUO · PARTE 06

El nuevo paradigma · cuatro principios del monitoreo continuo

Un modelo operativo diferente, en el que descubrimiento, evaluación y priorización operan en flujo continuo, sustituyendo las fotografías periódicas del escaneo.

Whitepaper 2026
CSURFACE

La naturaleza del monitoreo continuo. Acelerar un escaneo mensual a semanal mantiene el mismo paradigma — fotografía, cola, ciclo. El monitoreo continuo es un **cambio de modelo operativo**: descubrimiento en flujo, postura observada en tiempo real, priorización dirigida por amenaza activa, y acción disparada por evento.

LOS CUATRO PRINCIPIOS DEL MONITOREO CONTINUO

1. **Descubrimiento en flujo**
   Cada nuevo activo, cada cambio de configuración y cada nuevo componente entra automáticamente en el alcance en el momento en que aparece — sin esperar la siguiente ronda del scanner.

2. **Postura observada**
   La evaluación de postura se rehace continuamente, activo por activo, ante cada alteración observada en el estado externo.

3. **Priorización por amenaza activa**
   El orden de la cola lo determina la amenaza real y observada. Lo que está siendo explotado ahora sube al frente; el score estático de un CVE publicado meses antes cede posición.

4. **Acción disparada por evento**
   Los cambios relevantes generan alertas que alimentan directamente el ciclo de remediación — sin esperar el siguiente informe periódico.

Lo que cambia en la operación

En el modelo puntual, el equipo de GestVuln espera el escaneo, recibe un informe con cientos de hallazgos, hace triaje por score estático, asigna responsabilidad y abre tickets. El ciclo se repite en la siguiente ejecución.

En el modelo continuo, el equipo trabaja sobre **un flujo de eventos significativos** — nuevos activos, cambios de postura, nuevas vulnerabilidades en producción, evidencia de explotación activa contra organizaciones pares. Cada evento trae su contexto y su prioridad ya calculados; el triaje pasa de ser un ejercicio de barrido a uno de decisión.

Frameworks que exigen monitoreo continuo. El modelo continuo es lo que múltiples frameworks recomiendan desde hace más de una década. **NIST CSF** (DE.CM-8: continuous vulnerability scans), **CIS Controls v8** (Control 7: Continuous Vulnerability Management), **ISO 27001:2022** (A.8.8: gestión de vulnerabilidades técnicas sobre base continua) y **PCI DSS 4.0** (Req. 6.3.1: identificar vulnerabilidades continuamente) ya establecen el estándar. El desfase está en la implementación, no en la norma.

EL PAPEL DE CSURFACE · PARTE 07

Cómo CSURFACE cierra la ventana

Descubrimiento continuo + threat sensor + priorización dinámica — los tres instrumentos con los que la plataforma opera a la cadencia del atacante.

Descubrimiento continuo de la superficie externa

La plataforma mapea la superficie externa de la organización en flujo — cada nuevo subdominio, cada nuevo certificado, cada nueva exposición entra automáticamente en el alcance en el momento en que se vuelve observable. No hay ventana de escaneo: el intervalo entre la aparición de un activo nuevo y su entrada en el inventario es típicamente de horas.

Es esta base la que hace posible todo lo demás — sin descubrimiento continuo, el threat sensor y la priorización dinámica operarían sobre un inventario que envejece.

Threat sensor · señal de amenaza en tiempo real

El threat sensor de CSURFACE observa, en tiempo real, la **actividad de explotación observada** contra la superficie monitoreada: intentos de explotación, inteligencia de exploits publicados, indicadores de campaña en curso, telemetría de fuentes externas. El resultado es una lectura de amenaza que refleja el presente de la explotación, tal como está — más allá de la estimación estática de un score publicado meses antes.

Es esta lectura la que decide el orden de la cola: las vulnerabilidades bajo explotación activa suben a la cima, incluso cuando su CVSS es menor que otras pendientes.

El contraste con el ciclo puntual

DIMENSIÓN	CICLO PUNTUAL	CSURFACE
Cadencia de descubrimiento	Mensual / trimestral	**Continua**
Postura externa	Snapshot del escaneo	**Observada**
Priorización	CVSS estático	**Threat sensor**
Recalibración	Siguiente ejecución	**En flujo**
Time-to-detect mediano	15-30 días	**< 24 horas donde hay cobertura de pruebas**

El resultado en términos de ventana. La combinación reduce la ventana de exposición típica de una vulnerabilidad crítica en activo monitoreado de **~50 días** (escenario tradicional) a la **cadencia de remediación interna de la organización** — porque la detección deja de ser el cuello de botella. La ventana pasa a depender solo de la velocidad interna de aplicación del control.

APLICACIÓN Y CUMPLIMIENTO · PARTE 08

El mismo trabajo que protege y comprueba

El monitoreo continuo es lo que múltiples regulaciones ya exigen. Aplicarlo satisface, en un solo esfuerzo, la protección y la evidencia regulatoria.

Requisitos regulatorios y normativos

NORMA	REQUISITO	ADHERENCIA
BACEN 4.557	Gestión de riesgo operacional · monitoreo continuo de vulnerabilidades	Cumplido
NIST CSF	DE.CM-8 · escaneos continuos de vulnerabilidades	Cumplido
CIS Controls v8	Control 7 · Continuous Vulnerability Management	Cumplido
ISO 27001:2022	A.8.8 · gestión de vulnerabilidades técnicas sobre base continua	Cumplido
PCI DSS 4.0	Req. 6.3.1 · identificar vulnerabilidades continuamente	Cumplido
RGPD · Art. 46	Medidas técnicas aptas para proteger datos personales	Soporta

La lectura "cumplido" indica que el monitoreo continuo de CSURFACE entrega, en la práctica, el requisito técnico que cada norma establece. La adherencia formal depende del alcance contratado y de la política interna de la organización.

Cumplimiento como subproducto. El trabajo técnico de monitoreo continuo entrega, en el mismo movimiento, la evidencia que cada una de esas normas exige — un inventario verificable, fechado y auditable de cada descubrimiento, cambio y remediación. La organización deja de mantener dos operaciones paralelas (una para el control, otra para la evidencia) y pasa a operar con una única traza.

El argumento para el comité de auditoría

El comité de auditoría pide **evidencia de un control en operación**, más que una herramienta. En un modelo puntual, la evidencia es el informe del escaneo mensual. En un modelo continuo, la evidencia es la traza que muestra, para cada vulnerabilidad crítica, el tiempo entre la aparición de la exposición, la detección y la remediación.

En organizaciones reguladas — BACEN, B3, ANS —, esa traza pasa a ser la base del KRI (Key Risk Indicator) de ventana de exposición, comparable trimestre a trimestre.

APÉNDICE · FUENTES

Metodología y fuentes

Las referencias externas que sustentan los datos de este whitepaper.

Referencias

1. **Telemetría de emerging threats de CSURFACE.** Pipeline propio de monitoreo que correlaciona CVE (NVD), índice de probabilidad de explotación, catálogo de explotación activa, observación de explotación activa y telemetría de campaña. Serie histórica 2020-2026 (parcial) usada en los gráficos de la página 3 y en los KPIs del resumen ejecutivo. Funnel de CVE: publicación NVD → monitoreados → alta probabilidad de explotación → explotación confirmada → TTE ≤ 5 días → zero-day.
2. **Mandiant M-Trends 2024.** Informe anual de Mandiant (Google) sobre tendencias de amenaza. La edición de abril de 2024 (datos de 2023) registra una mediana de Time-to-Exploit de 5 días, corroborando el salto observado por la telemetría de CSURFACE en 2024.
3. **Google Threat Analysis Group + Mandiant.** Informe conjunto sobre zero-days. Documenta un crecimiento sostenido de zero-days explotados en producción y atribución parcial a proveedores comerciales de vigilancia.
4. **Verizon DBIR 2024 y 2025.** Análisis anual de incidentes corporativos. DBIR 2024 reporta un crecimiento del 180% en brechas originadas en explotación de vulnerabilidad; DBIR 2025 proyecta una aceleración específica en dispositivos de borde.
5. **Informe IBM Cost of a Data Breach 2025.** Informe anual basado en incidentes investigados en más de 600 organizaciones en 17 países. Mediana global para identificar y contener una brecha: 241 días.

Nota metodológica

Los conteos de CVE con explotación rápida (TTE ≤ 5 días) citados en este whitepaper son producidos por la telemetría de emerging threats de CSURFACE, computados sobre el universo total de CVE publicados en la NVD cada año. La metodología combina el feed NVD con señal de explotación activa, índice de probabilidad de explotación y catálogo de explotación activa, y produce un funnel anual desde 2020. La mediana de TTE en días, publicada por Mandiant en los informes M-Trends, se usa como referencia corroborativa.

Las medianas de tiempo hasta remediación citadas siguen la metodología del Verizon DBIR, que computa el intervalo entre el disclosure y la corrección efectiva en ambiente de producción, considerando el conjunto de organizaciones con incidentes investigados en el año.

Los datos específicos de cada caso (Log4Shell, Spring4Shell, VMware vRealize, F5 BIG-IP, Citrix Bleed, ScreenConnect, CrushFTP) siguen las comunicaciones de los propios proveedores y los análisis técnicos publicados por equipos de investigación en seguridad (Cloudflare, Cisco Talos, Microsoft Threat Intelligence, Volexity).

Lo que este whitepaper no cubre. Este material es educativo y descriptivo. No constituye proyección actuarial, recomendación jurídica o regulatoria. Los números mencionados son valores medianos de población observada; la aplicación a una organización específica requiere modelar la propia ventana con base en su superficie, postura y telemetría.

PRÓXIMOS PASOS

Cierre la ventana antes del próximo exploit

La gestión continua de exposición es una de las capacidades de la plataforma CSURFACE — una plataforma de Continuous Exposure Management. En arquitectura integrada, reúne descubrimiento continuo de la superficie externa con Machine Learning, análisis de la cadena digital de proveedores, validación de explotabilidad, inteligencia de amenazas con priorización dinámica, monitoreo de credenciales filtradas y cuantificación financiera de riesgo. Opera de forma íntegramente externa — sin agente y sin instalación —, con integraciones opcionales de nube, WAF y CIEM disponibles para organizaciones que buscan mayor profundidad de visibilidad.

Mida la ventana de su parque

En un análisis preliminar gratuito, CSURFACE mapea la superficie externa de la organización y reporta la ventana de exposición observada en los activos críticos.

Use la calculadora de riesgo

Estime el impacto financiero de su ventana de exposición con la calculadora pública de CSURFACE, calibrada por benchmark de mercado.

Lea el whitepaper de Threat Intel

El detalle de la priorización dinámica — cómo el índice de probabilidad de explotación, el catálogo de explotación activa y el threat sensor de CSURFACE componen la cola real de remediación.

¿Quiere ver la ventana de exposición de sus activos — de forma gratuita?

Solicitar análisis gratuito