PLATAFORMA CSURFACE · 01 · ARQUITECTURA

Operación continua · sin agente, sin instalación

Plataforma de Continuous Exposure Management entregada como SaaS, con aislamiento por tenant e integraciones opcionales para mayor profundidad. Modelo operativo, especificaciones técnicas y postura de seguridad en una sola página.

Ficha técnica 2026
CSURFACE

MODELO OPERATIVO
Sin agente
descubrimiento y monitoreo íntegramente externos · sin instalación en el entorno del cliente

AISLAMIENTO
Tenant aislado
bases de datos y bóvedas de credenciales aisladas por organización

RETENCIÓN DE DATOS
15 días
ventana operativa de telemetría · evidencias exportables bajo demanda

Flujo de datos · de la superficie externa a la alerta

01 · RECOLECCIÓN
Señales externas
CT logs, DNS, WHOIS, ASN, headers, scripts en runtime, threat feeds

→

02 · CORRELACIÓN
Machine Learning
múltiples señales por activo en dimensiones distintas para la atribución de propiedad y contexto

→

03 · ENRIQUECIMIENTO
Threat Sensor
índice de probabilidad de explotación, catálogo de explotación activa, exploit activo, indicadores de campaña

→

04 · SALIDA
Alerta priorizada
SIEM, ticketing, ChatOps, API, dashboard

No hay agente, instrumentación ni tráfico originado en el entorno del cliente hacia la plataforma. La recolección es íntegramente externa, conforme a las prácticas de External Attack Surface Management (EASM).

Especificaciones técnicas

MODELO DE ENTREGA	SaaS · multi-tenant con bases de datos y bóvedas de credenciales aisladas por tenant
ALOJAMIENTO	AWS · controles de infraestructura y certificaciones heredadas de la capa del proveedor
RESIDENCIA DE DATOS	Global · selección de región por contratación
RETENCIÓN OPERATIVA	15 días · ventana estándar de telemetría; evidencias exportables bajo demanda para la retención del cliente
CIFRADO	En reposo y en tránsito · TLS 1.2+; claves gestionadas por el proveedor
AUTENTICACIÓN	MFA obligatorio para todos los usuarios · bóveda interna para credenciales y tokens de integración
CONTROL DE ACCESO	RBAC nativo · SSO vía SAML/OIDC bajo solicitud
AUDITORÍA	Registro de auditoría íntegro · las acciones de usuario, los cambios de configuración y los accesos a evidencia quedan registrados

Postura de seguridad · resumen. Plataforma alojada en AWS con bases de datos y bóvedas de credenciales aisladas por tenant. MFA obligatorio, registro de auditoría íntegro, sin datos sensibles del cliente persistidos más allá de la ventana de 15 días. Los controles de infraestructura heredan las certificaciones del proveedor de nube; los controles de aplicación son de CSURFACE.

Lo que la plataforma *no* hace

No opera dentro del perímetro del cliente. No instala un agente en un servidor, endpoint o nube del cliente. No exige la apertura de una regla de firewall para entrada. No exfiltra payload de aplicación. No actúa como WAF, EDR o SIEM.

Las integraciones opcionales con nube, CIEM o WAF, cuando se contratan, amplían la visibilidad interna sin alterar el modelo central de operación externa.

PLATAFORMA CSURFACE · 02 · CAPACIDADES

Cuatro capacidades en una plataforma única · Machine Learning y capa agéntica

Descubrimiento contextual mediante Machine Learning, telemetría continua de amenazas, monitoreo de credenciales con validación activa y validación de explotabilidad — operando sobre el mismo inventario y el mismo modelo de datos.

Ficha técnica 2026
CSURFACE

Machine Learning & Capa Agéntica

Descubrimiento continuo de la superficie externa con Machine Learning que analiza múltiples señales por activo y una capa agéntica de propiedad. Cobertura amplia y contextual, con el falso positivo prácticamente eliminado y ruido técnicamente mínimo.

Threat Sensor

Telemetría propia de emerging threats que correlaciona bases públicas de vulnerabilidades, índices de probabilidad de explotación, catálogos de explotación activa, exploit activo e indicadores de campaña. Actualización continua de la cola de priorización — recálculo en hasta 24h tras un cambio de señal.

Credential Leak Monitor

Monitoreo de breach databases, dark web y repositorios públicos con validación activa no destructiva. Confirmación de la validez de la credencial antes de la alerta — reduciendo el falso positivo y la movilización innecesaria.

Exposure Validation

Validación activa de explotabilidad donde hay cobertura de pruebas, con monitoreo pasivo en el resto de la superficie. Diferencia "vulnerable" de "explotable en el contexto observado" — eliminando el ruido de los CVEs presentes pero no accesibles por el vector publicado.

Contextualización de activos · Machine Learning en tres dimensiones

Cada activo descubierto se clasifica automáticamente en tres dimensiones — **sector de la industria**, **área de negocio propietaria** y **categoría del activo** — para que la plataforma decida su importancia para la organización sin dependencia de la clasificación manual. La inferencia de propiedad interna acelera la triaje: la alerta llega al equipo correcto preasignada.

Pipeline de discovery · Machine Learning y capa agéntica

Para cada activo observado, la plataforma analiza **múltiples señales** en dimensiones distintas — cada dimensión aportando pistas sobre la propiedad del activo y su relación con la organización. La salida de una capa alimenta a la siguiente, con refinamiento progresivo: lo que asciende a la capa siguiente es más confiable que lo que entró.

El resultado es un **score de confianza por activo** que sintetiza todas las capas — sin dependencia de la clasificación manual, con una decisión auditable en cada etapa.

Capa agéntica de decisión. Sobre los modelos opera un agente autónomo que evalúa los resultados, resuelve conflictos entre señales convergentes y divergentes y decide la atribución final de propiedad. El agente reduce al máximo el esfuerzo humano necesario — eliminando el falso positivo en el origen, con **alta precisión** en las organizaciones analizadas. La retroalimentación humana, cuando ocurre, alimenta la siguiente ronda del modelo, reduciendo aún más la necesidad de interacción futura.

Integraciones nativas

- **SIEM** · Splunk, Sentinel, QRadar, Elastic
- **Ticketing** · Jira, ServiceNow
- **ChatOps** · Slack, Microsoft Teams
- **SOAR** · Splunk SOAR, Tines, Cortex XSOAR
- **API** · REST + webhook genérico para integración personalizada

Modelo de retroalimentación humana

Cuando el analista revisa una alerta y ajusta la atribución, la severidad o el estado, esa señal entra en **loop** con la capa de ML — el modelo aprende con cada interacción. La consecuencia operativa es que la necesidad de intervención humana **disminuye progresivamente** a lo largo del tiempo de uso, a medida que el agente incorpora las preferencias y el contexto específicos de ese tenant.

Conozca la plataforma en acción — Solicitar un análisis