PLATAFORMA CSURFACE · 01 · ARQUITETURA

Operação contínua · sem agente, sem instalação

Plataforma de Continuous Exposure Management entregue como SaaS, com isolamento por tenant e integrações opcionais para profundidade adicional. Modelo operacional, especificações técnicas e postura de segurança em uma página.

Datasheet 2026
CSURFACE

MODELO OPERACIONAL
Sem agente
descoberta e monitoramento integralmente externos · sem instalação no ambiente do cliente

ISOLAMENTO
Tenant isolado
databases e cofres de credenciais isolados por organização

RETENÇÃO DE DADOS
15 dias
janela operacional de telemetria · evidências exportáveis sob demanda

Fluxo de dados · da superfície externa ao alerta

01 · COLETA
Sinais externos
CT logs, DNS, WHOIS, ASN, headers, scripts em runtime, threat feeds

→

02 · CORRELAÇÃO
Machine Learning
dezenas de sinais por ativo em dimensões distintas para atribuição de propriedade e contexto

→

03 · ENRIQUECIMENTO
Threat Sensor
índice de probabilidade de exploração, catálogo de exploração ativa, exploit ativo, indicadores de campanha

→

04 · SAÍDA
Alerta priorizado
SIEM, ticketing, ChatOps, API, dashboard

Não há agente, instrumentação ou tráfego originado do ambiente do cliente para a plataforma. Coleta é integralmente externa, conforme práticas de External Attack Surface Management (EASM).

Especificações técnicas

MODELO DE ENTREGA	**SaaS** · multi-tenant com databases e cofres de credenciais isolados por tenant
HOSPEDAGEM	AWS · controles de infraestrutura e **certificações herdadas** da camada de provedor
RESIDÊNCIA DE DADOS	Global · seleção de região por contratação
RETENÇÃO OPERACIONAL	**15 dias** · janela padrão de telemetria; evidências exportáveis sob demanda para retenção do cliente
CRIPTOGRAFIA	Em repouso e em trânsito · TLS 1.2+; chaves gerenciadas pelo provedor
AUTENTICAÇÃO	**MFA obrigatório** para todos os usuários · cofre interno para credenciais e tokens de integração
CONTROLE DE ACESSO	RBAC nativo · SSO via SAML/OIDC sob solicitação
AUDITORIA	Log de auditoria integral · ações de usuário, alterações de configuração e acessos a evidência são registrados

Postura de segurança · sumário. Plataforma hospedada em AWS com databases e cofres de credenciais isolados por tenant. MFA obrigatório, log de auditoria integral, sem dados sensíveis do cliente persistidos além da janela de 15 dias. Controles de infraestrutura herdam as certificações do provedor de nuvem; controles de aplicação são da CSURFACE.

O que a plataforma *não* faz

Não opera **dentro** do perímetro do cliente. Não instala agente em servidor, endpoint ou nuvem do cliente. Não exige abertura de regra de firewall para entrada. Não exfiltra payload de aplicação. Não atua como WAF, EDR ou SIEM.

Integrações opcionais com nuvem, CIEM ou WAF, quando contratadas, ampliam visibilidade interna sem alterar o modelo central de operação externa.

PLATAFORMA CSURFACE · 02 · CAPACIDADES

Quatro capacidades em uma plataforma única · Machine Learning e camada agêntica

Descoberta contextual por Machine Learning, telemetria contínua de ameaças, monitoramento de credenciais com validação ativa e validação de exploitabilidade — operando sobre o mesmo inventário e o mesmo modelo de dados.

Datasheet 2026
CSURFACE

Machine Learning & Camada Agêntica

Descoberta contínua da superfície externa com Machine Learning analisando dezenas de sinais por ativo e camada agêntica de propriedade. Cobertura típica acima de 95% com taxa de falso positivo de ≤ 5%.

Threat Sensor

Telemetria própria de emerging threats correlacionando NVD, índices de probabilidade de exploração, catálogos de exploração ativa, exploit ativo e indicadores de campanha. Atualização contínua da fila de priorização — recálculo em até 24h após mudança de sinal.

Credential Leak Monitor

Monitoramento de breach databases, dark web e repositórios públicos com validação ativa não-destrutiva. Confirmação da validade da credencial antes do alerta — reduzindo falso positivo e mobilização desnecessária.

Exposure Validation

Validação de exploitabilidade real das vulnerabilidades expostas. Diferencia "vulnerável" de "explorável no contexto observado" — eliminando o ruído de CVEs presentes mas não acessíveis pelo vetor publicado.

Contextualização de ativos · Machine Learning em três dimensões

Cada ativo descoberto é automaticamente classificado em três dimensões — **setor da indústria**, **área de negócio proprietária** e **categoria do ativo** — para que a plataforma decida sua importância para a organização sem dependência de classificação manual. A inferência de propriedade interna acelera a triagem: o alerta chega à equipe certa pré-atribuído.

Pipeline de discovery · Machine Learning e camada agêntica

Para cada ativo observado, a plataforma analisa **dezenas de sinais** em dimensões distintas — cada dimensão contribuindo com pistas sobre a propriedade do ativo e sua relação com a organização. A saída de uma camada alimenta a próxima, com refinamento progressivo: o que sobe à camada seguinte é mais confiável do que entrou.

O resultado é um **score de confiança por ativo** que sintetiza todas as camadas — sem dependência de classificação manual, com decisão auditável em cada etapa.

> **Camada agêntica de decisão.** Sobre os modelos opera um agente autônomo que avalia os resultados, resolve conflitos entre sinais convergentes e divergentes e decide a atribuição final de propriedade. O agente reduz ao máximo o esforço humano necessário — eliminando o falso positivo na origem, com precisão acima de **95%** em organizações analisadas. O feedback humano, quando ocorre, alimenta a próxima rodada do modelo, reduzindo ainda mais a necessidade de interação futura.

Integrações nativas

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

Modelo de feedback humano

Quando o analista revisa um alerta e ajusta atribuição, severidade ou status, esse sinal entra em **loop** com a camada de ML — o modelo aprende a cada interação. A consequência operacional é que a necessidade de intervenção humana **cai progressivamente** ao longo do tempo de uso, à medida que o agente incorpora as preferências e o contexto específicos daquele tenant.

Conheça a plataforma na prática — Solicitar análise