csurface

RELATÓRIO ANUAL · CYBER EXPOSURE

Estado da Exposição Digital

Edição 2026 — Como a superfície de ataque cresce, como a ameaça acelera, e por que a distância entre as duas é o verdadeiro risco. Dados agregados e anônimos de dezenas de organizações.

ORGANIZAÇÕES NA BASE **68 + 16 detalhadas**	ATIVOS EXTERNOS MAPEADOS **122 mil**	PERÍODO **2026**
CLASSIFICAÇÃO **Público**	EDIÇÃO **1ª — Anual**	FONTE **Plataforma CSURFACE**

SUMÁRIO EXECUTIVO

A leitura em três partes

O que os dados deste relatório dizem — e a única conclusão para a qual eles convergem.

Edição 2026
CSURFACE

OPERAM EM 2+ NUVENS
75%
superfície dispersa por múltiplos provedores

EXPLOIT PÚBLICO APÓS A FALHA
5 dias
tempo médio até existir código de ataque

VULNERABILIDADE HÁ 5+ ANOS
68%
das organizações analisadas

Este relatório reúne, de forma **agregada e anônima**, o que a CSURFACE observou ao mapear a superfície de ataque externa de dezenas de organizações — 68 com descoberta concluída na plataforma e 16 submetidas a análise detalhada. Nenhuma empresa é identificada.

Primeiro: a superfície cresce sem governo. Ela não é um inventário organizado — espalha-se por várias nuvens, por ambientes provisionados às pressas e raramente desligados, por componentes de terceiros embutidos em cada aplicação. Três em cada quatro organizações operam ativos em duas ou mais nuvens; metade, em três ou mais. E o que entra quase nunca é mantido: 68% carregam uma vulnerabilidade aberta há mais de cinco anos.

Segundo: a ameaça acelera. Um exploit público funcional surge, em média, cinco dias depois de uma falha ser divulgada; a exploração ativa, em noventa. As classes de falha mais exploradas são, em sua maioria, falhas de aplicação web — exatamente a camada que 71% das aplicações analisadas deixam sem WAF.

Terceiro: o risco mora na distância entre as duas curvas. A defesa adiciona e esquece ativos numa escala de anos. O atacante arma exploits numa escala de dias. O incidente é a interseção previsível dessas duas velocidades sobre o mesmo ativo desgovernado — ocorrência de natureza estrutural, estatisticamente esperada onde a defesa fica atrás da ameaça.

A conclusão deste relatório. Nenhuma das duas curvas se resolve isoladamente. Descobrir tudo sem priorizar sobrecarrega a equipe; priorizar ameaças sem enxergar a superfície inteira protege apenas o que já era conhecido. Reduzir o risco exige **descoberta contínua da superfície** e **inteligência de ameaças** operando juntas, sem interrupção.

Base de dados

Organizações com descoberta concluída	**68**
Análises detalhadas de superfície	**16**
Setores representados	**11**
Ativos externos mapeados	**122.095**
Vulnerabilidades analisadas	**2.361**
Ameaças emergentes monitoradas	**2.954**

Setores das análises detalhadas: automotivo, educação, governo, indústria, logística, ordem profissional, previdência, saúde, serviços, tecnologia e varejo.

Toda a análise é externa e passiva. Dados anonimizados; nenhuma organização é identificada.

PARTE 01

A superfície cresce — e cresce sem governo

Do que é feita a superfície de ataque externa e por que ela se expande mais rápido do que qualquer inventário.

Edição 2026
CSURFACE

ATIVOS EXTERNOS
122 mil
em 68 organizações

ORGANIZAÇÕES RELACIONADAS
1.068
descobertas pela plataforma

COMPONENTES DE TERCEIROS
2,8×
por ativo próprio exposto

Distribuição dos ativos externos por tipo

Provedores de nuvem por organização

Análise

A superfície de ataque externa não é um inventário organizado. Ela se acumula. Cada time de produto publica uma aplicação, cada área de negócio contrata um SaaS, cada aquisição traz a infraestrutura herdada de outra empresa — e quase nada disso é removido depois.

O dado mais revelador é o da nuvem: **três em cada quatro organizações** distribuem ativos por dois ou mais provedores, e metade por três ou mais. Cada ambiente acrescenta um console próprio, um padrão de configuração próprio e uma fronteira de gestão própria. Tratados em **silos isolados**, com ferramentas, padrões e equipes distintas por provedor, esses ambientes geram visões parciais que raramente se reconciliam: a superfície real existe fragmentada entre múltiplos consoles, e nenhuma das visões parciais representa o todo.

A dependência de terceiros amplia o efeito: cada aplicação web exposta carrega múltiplos componentes da cadeia de fornecedores — scripts, CDNs e bibliotecas embutidos no código que expandem a superfície sem aparecer em nenhum inventário.

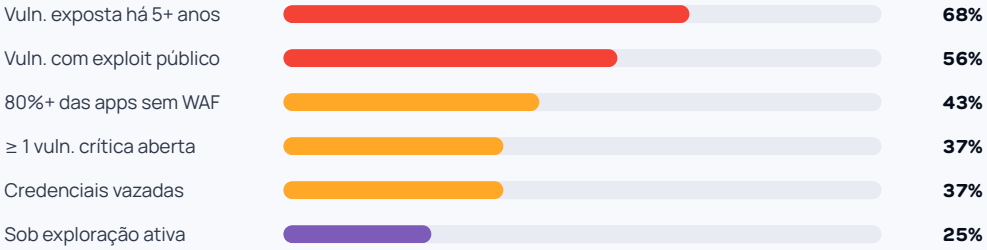
Por que isso importa. Inventário é a base de todo programa de segurança. Sem saber o que existe, toda priorização, todo teste e toda resposta operam sobre uma base incompleta — e o que ficou de fora continua exposto.

PARTE 02

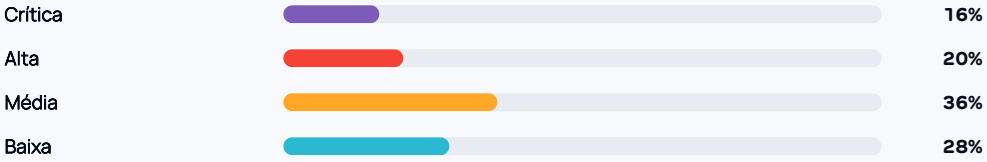
O que a superfície acumula

Os achados que se repetem de empresa para empresa — e quase sempre são antigos.

Frequência dos achados — % das empresas analisadas



Distribuição das 2.361 vulnerabilidades por severidade



Severidade não é prioridade

INDICADOR DE EXPLORAÇÃO	REPRESENTATIVIDADE
Com exploit público disponível	**5,7%** das vulns
Comprovadamente exploradas	**1,8%** das vulns
Conjunto realmente prioritário	**7,5%** das vulns

Das 2.361 vulnerabilidades, apenas uma fração tem exploração comprovada — e é nessa fração que um atacante começa.

O tempo de exposição é o problema. Em 68% das organizações há uma vulnerabilidade aberta há mais de cinco anos; a mais antiga registrada passava de uma década. A idade média das exposições supera seis anos. Trata-se de um passivo silencioso: vulnerabilidades antigas que permaneceram fora do radar dos inventários e dos ciclos de correção. O backlog de remediação, medido em anos, é incompatível com a velocidade da ameaça.

Análise

Os mesmos achados se repetem de empresa para empresa, e quase sempre são **antigos**. A superfície cresce e acumula. O que entra raramente é removido; o que falha raramente é corrigido.

O volume de vulnerabilidades engana. O que separa um inventário de risco de uma lista interminável é a inteligência de exploração: saber quais falhas têm exploit, quais estão sendo usadas, quais têm probabilidade real de ataque. Sem esse filtro, a equipe trata o que é barulhento — não o que é perigoso.

PARTE 03

Do outro lado, a ameaça não espera

O ritmo da exploração observado no recorte de maior risco — fração de aproximadamente 1% das vulnerabilidades, selecionada por threat intelligence, exploit intelligence e Machine Learning.

Sobre o recorte. A plataforma da CSURFACE detecta o universo completo de vulnerabilidades em cada ativo monitorado. Os números desta parte referem-se à fração de aproximadamente **1% com maior potencial de gerar incidente** — identificada pelo cruzamento de **threat intelligence**, **exploit intelligence** e **Machine Learning** sobre essa base. É sobre esse recorte priorizado que se mede o ritmo da exploração no mundo real.

AMEAÇAS EMERGENTES MONITORADAS
2.954
recorte priorizado · alta severidade

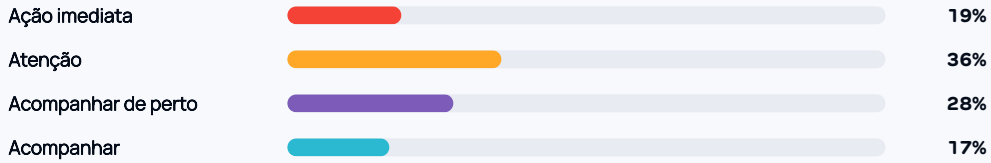
EXPLOIT PÚBLICO EM
5 dias
tempo médio após a divulgação

EXPLORAÇÃO ATIVA EM
90 dias
tempo médio até ataque no mundo real

EM EXPLORAÇÃO REAL
809
confirmadas exploradas no mundo

Classes de falha mais exploradas (CWE)

Prioridade real — categorização SSVC



Análise

Enquanto a superfície se acumula em silêncio, a ameaça do outro lado se move em **ritmo industrial**. Um exploit público funcional surge, em média, cinco dias após a divulgação de uma falha. Em parte dos casos o exploit vem antes do aviso: entre as ameaças críticas monitoradas há centenas exploradas como zero-day.

A mira do atacante é precisa. Cinco das seis classes de falha mais exploradas são falhas de **aplicação web** — injeção, path traversal, upload de arquivo. É exatamente a camada que, na Parte 02, aparece sem WAF em 71% das aplicações analisadas. A curva da ameaça aponta para o ponto mais desprotegido da defesa.

E severidade não é prioridade: mesmo num conjunto onde toda falha é grave — CVSS médio 9,0 — a categorização SSVC classifica apenas **19% como ação imediata**. Ler indicadores de exploração qualquer equipe consegue; o difícil é cruzar essa inteligência com a superfície real e saber, a cada semana, quais ameaças alcançam os próprios ativos.

A lista não para de crescer. O catálogo de vulnerabilidades comprovadamente exploradas é atualizado toda semana — uma única semana recente registrou 12 novas entradas. Uma varredura trimestral perde a janela inteira. Só o monitoramento contínuo detecta a falha na semana em que ela se torna uma ameaça confirmada.

A CONCLUSÃO

O encontro — onde o incidente nasce

O que o volume de ameaças tem a ver com os relatórios de superfície.

Edição 2026
CSURFACE

A AMEAÇA ATACA

5 dias

tempo médio entre uma falha ser divulgada e existir um exploit público funcional para ela.

×

A PORTA FICA ABERTA

5+ anos

tempo que a vulnerabilidade mais antiga permanece exposta em 68% das empresas analisadas.

A análise

Tudo. É essa a resposta para o que o volume de ameaças tem a ver com os relatórios de superfície. Cada ativo desgovernado da Parte 01 — um ambiente em nuvem esquecido, um componente de terceiro, uma aplicação sem WAF — é uma porta. A Parte 03 diz que portas são encontradas e atacadas em dias. Os relatórios da Parte 02 dizem que essas portas ficam abertas por anos.

Lado a lado, os dois conjuntos de dados convergem em uma só conclusão. A defesa adiciona ativos mais rápido do que consegue inventariá-los, e remove ou corrige quase nada — o tempo de exposição se mede em **anos**. O atacante arma um exploit em **dias**.

Um incidente, portanto, é a interseção previsível de duas curvas: uma superfície que cresce desordenada e nunca encolhe, e uma ameaça que só acelera. O incidente é apenas a vez em que as duas se cruzam no mesmo ativo — quase sempre um ativo ausente do inventário.

O que fecha a distância entre as duas curvas

Não se corrige uma superfície que não se enxerga, nem se vence a velocidade da ameaça no esforço manual. Fechar essa distância exige duas capacidades operando juntas e sem parar:

Descoberta contínua — que encontra cada porta, inclusive os ambientes em nuvem, o shadow IT e os ativos ausentes do inventário.

Inteligência de ameaças e exploits — que diz quais portas estão sendo atacadas agora, e reordena a fila de prioridade conforme a ameaça evolui.

Uma sem a outra deixa a janela aberta. É a combinação contínua das duas — descoberta e inteligência no mesmo modelo de dados — que transforma exposição em risco gerenciável.

csurface

CONTINUOUS EXPOSURE MANAGEMENT

Da exposição desordenada à ação priorizada.

A CSURFACE é uma plataforma única de gestão de superfície de ataque externa. Ela reúne, sob um só modelo de dados, as duas capacidades que este relatório mostra serem inseparáveis: descobrir tudo o que está exposto e saber, em tempo real, o que a ameaça vai explorar primeiro.

Descoberta contínua
Mapeia toda a superfície externa a partir do domínio raiz — nuvem, shadow IT, cadeia de terceiros e ativos esquecidos. Sem agentes, sem listas a fornecer.

Classificação por Machine Learning
Atribui cada ativo à organização, elimina o falso positivo de propriedade e classifica por criticidade de negócio. Um inventário com contexto.

Inteligência de ameaças e exploits
Cruza cada exposição com índices de exploração ativa e ameaças emergentes — a fila de prioridade reflete o risco real e se reordena sozinha.

Validação de explorabilidade
Confirma o que é de fato explorável, com teste ativo externo onde há cobertura e detecção passiva no restante da superfície.

Monitoramento de credenciais
Acompanha credenciais corporativas vazadas em violações e na dark web, com alerta em horas — não em meses.

Quantificação de risco
Capacidade em desenvolvimento: vai traduzir o risco técnico em valor financeiro, para que a diretoria decida com base em números, não em alertas técnicos.

Veja onde a sua empresa está nesse retrato.

Receber a análise preliminar da minha empresa →