csurface

WHITEPAPER · JANELA DE EXPOSIÇÃO

# Cinco dias para o exploit · trinta para o próximo scan

Em três anos, o tempo médio entre a publicação de uma vulnerabilidade e o primeiro exploit caiu de 32 para 5 dias — e o ciclo da gestão de vulnerabilidades tradicional, pontual e mensal, não acompanha mais.

| CAPACIDADE | PÚBLICO | EDIÇÃO |
| --- | --- | --- |
| **Gestão Contínua de Exposição** | **CISO · Risco · GVUL · SOC** | **2026** |

| LEITURA | CLASSIFICAÇÃO | FONTE |
| --- | --- | --- |
| **14 páginas** | **Público** | **Plataforma CSURFACE** |

SUMÁRIO EXECUTIVO

# O exploit está mais rápido — e a sua janela está aberta

A tese deste whitepaper em uma página, com dados da telemetria de emerging threats da CSURFACE: a velocidade da exploração e o ciclo da gestão de vulnerabilidades já não se encontram.

Whitepaper 2026
CSURFACE

EXPLOITS EM ≤ 5 DIAS · 2024 VS. 2020

**+183%**

153 CVEs explorados em ≤ 5 dias em 2024 — contra 54 em 2020[1]

CICLO TÍPICO DE GVUL

**30 dias**

scan mensal — o intervalo mínimo entre fotografias

ZERO-DAYS ANTES DO DISCLOSURE · 2026*

**52%**

dos zero-days observados em 2026 já foram explorados antes da publicação do CVE — contra 21% em 2025[1]

A telemetria de emerging threats da CSURFACE registra que **153 CVEs foram explorados em ≤ 5 dias após o disclosure em 2024** — quase três vezes os 54 de 2020. Em 2026, apenas nos primeiros meses, já são 81. O salto ocorreu em 2024 e a faixa anual estabilizou em um patamar estruturalmente mais alto do que em qualquer ano anterior. A aceleração é o que a telemetria registrou ano após ano.

A gestão de vulnerabilidades tradicional, baseada em scans periódicos, opera em um ritmo herdado de outra era. Um ciclo mensal — já considerado bom em muitas organizações — entrega uma fotografia do parque a cada 30 dias. O ciclo trimestral ou anual entrega uma fotografia ainda mais defasada. Entre uma fotografia e a próxima, a janela de exposição permanece aberta — e o atacante dispõe de tempo suficiente para entrar.

Este whitepaper analisa a aceleração da exploração ao longo dos últimos três anos, expõe o gap matemático entre a velocidade do atacante e o ciclo do tradicional, e apresenta a abordagem da CSURFACE — descoberta contínua, threat sensor e priorização dinâmica — para fechar essa janela em horas, não em semanas.

**A tese.** Janela de exposição é o intervalo entre o momento em que uma vulnerabilidade se torna explorável e o momento em que a organização aplica o controle correspondente. Ela só pode ser fechada por um instrumento que opere na mesma cadência do atacante — contínua, e não pontual.

### O que este whitepaper cobre

- A aceleração da exploração — tendência de 3 anos, com dados públicos.
- Cinco casos públicos recentes — exploração em horas e dias.
- A anatomia da janela de exposição e por que o ciclo pontual não fecha.
- A abordagem da CSURFACE — threat sensor, descoberta e priorização contínuas.

A ACELERAÇÃO · PARTE 01

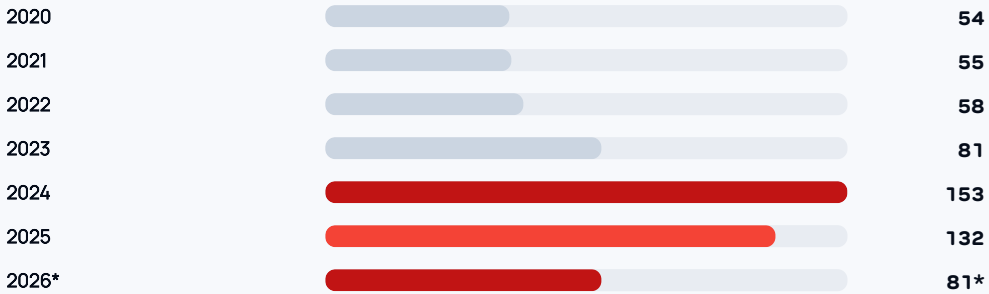
# De 54 para 153 em quatro anos · o salto do exploit rápido

O número de CVEs explorados em ≤ 5 dias após a divulgação quase triplicou entre 2020 e 2024 — leitura do sensor próprio de emerging threats da CSURFACE.



### Número absoluto de CVEs explorados em ≤ 5 dias · por ano

A telemetria de emerging threats da CSURFACE acompanha, ano a ano, o número absoluto de CVEs cuja exploração em produção foi observada em até 5 dias após a divulgação pública. A série de sete anos mostra um regime estruturalmente novo a partir de 2024 — quase três vezes a base de 2020:




Fonte: telemetria de emerging threats da CSURFACE. *2026 cobre apenas os primeiros meses do ano. O salto entre 2023 (81) e 2024 (153) marca a entrada em um regime estruturalmente diferente — corroborado pelo Mandiant M-Trends 2024, que reporta queda da mediana de TTE para 5 dias.[2]

### O que a CSURFACE observou nos últimos três anos

1. **Volume de CVEs em alta.** A NVD publicou 18.362 CVEs em 2020. Em 2025, foram **48.126** — quase 2,6× o volume de cinco anos antes. A pressão sobre as filas de remediação aumentou em proporção.
2. **Zero-days dobrou em 2024.** A CSURFACE registrou 57 zero-days em 2023, **103 em 2024** e 89 em 2025. Em 2026, já são 64 nos primeiros meses — ritmo que projeta um novo recorde anual.
3. **Exploração antes do disclosure.** Em 2025, 21% dos zero-days foram explorados antes de o CVE tornar-se público. Em 2026, **52%** — mais da metade. O atacante chega antes do registro existir.
4. **Salto em 2024 — não foi pontual.** O número de exploits em ≤ 5 dias passou de 81 (2023) para 153 (2024) — um crescimento de 88% em um ano. 2025 registrou 132; 2026, em poucos meses, já chega a 81. A faixa anual estabilizou em um patamar estruturalmente novo.

**A implicação.** A passagem de 54-81 para 132-153 exploits rápidos por ano é estrutural, não conjuntural. Ela reflete uma reorganização do ecossistema ofensivo — automação, exploração assistida por IA, especialização e mercado de exploits — que não retrocederá. O instrumento defensivo precisa operar em uma escala temporal comparável.

EXPLORAÇÃO DINÂMICA · PARTE 02

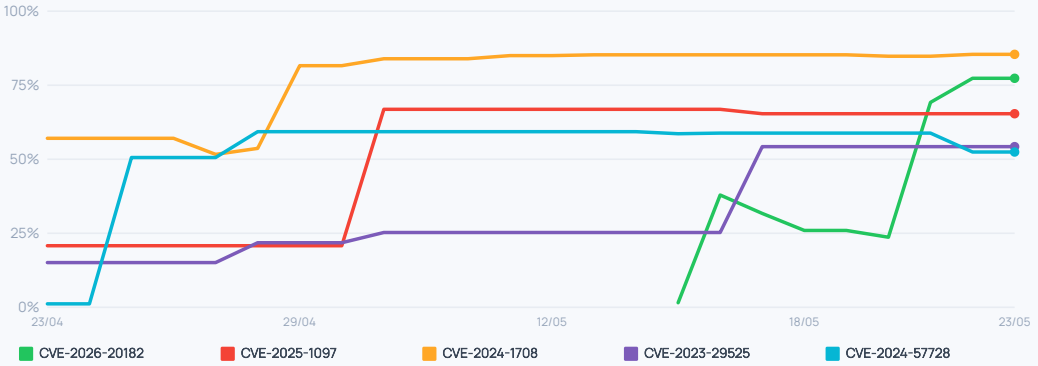
# CVEs dormentes que despertaram · o que o CVSS sozinho ignora

Cinco vulnerabilidades reais cuja probabilidade de exploração mais que dobrou nas últimas semanas — observadas pela telemetria de emerging threats da CSURFACE.



**Por que isto importa.** O CVSS expressa a gravidade *teórica* da falha — atribuído na publicação e raramente atualizado. O **índice de probabilidade de exploração** expressa a probabilidade real de exploração nos próximos 30 dias e muda diariamente. Uma vulnerabilidade pode dormir por meses com probabilidade de exploração baixa e, em poucos dias, ter o índice multiplicado em 10× ou 50× quando exploits, PoCs ou campanhas surgem. Quem prioriza apenas por CVSS perde esse movimento.

## PROBABILIDADE DE EXPLORAÇÃO · 30 DIAS · 5 CVES COM MAIOR CRESCIMENTO




### As cinco vulnerabilidades do gráfico

| CVE | PRODUTO AFETADO | PROBABILIDADE MÍN → ATUAL | SINAIS |
|---|---|---|---|
| **CVE-2026-20182** | Cisco Catalyst SD-WAN Manager | **1,6% → 77,3%** | ATIVA EXPLOIT |
| **CVE-2025-1097** | Kubernetes ingress-nginx | **20,8% → 65,4%** | rising |
| **CVE-2024-1708** | ConnectWise ScreenConnect | **51,7% → 85,4%** | ATIVA EXPLOIT |
| **CVE-2023-29525** | XWiki Platform | **15,1% → 54,3%** | dormente em 2023, reativado |
| **CVE-2024-57728** | SimpleHelp Remote Access | **1,2% → 52,4%** | ATIVA |

Fonte: telemetria de emerging threats da CSURFACE. Captura diária do índice de probabilidade de exploração, do catálogo de exploração ativa e da disponibilidade pública de exploit. Snapshot: 23 de maio de 2026.

### O que o CVSS sozinho não vê

A CVE-2026-20182 (Cisco Catalyst SD-WAN Manager) tinha probabilidade de exploração de **1,56%** em 15 de maio. Sete dias depois, o índice estava em **77,32%** — sem nenhuma alteração no CVSS. Uma fila baseada apenas em CVSS, recalculada uma vez por mês, manteria essa CVE no meio do bloco. Uma fila dinâmica a empurra ao topo no dia em que o sinal aparece.

**Priorização inteligente e contínua.** A CSURFACE compõe a fila combinando índice de probabilidade de exploração atual, delta de 30 dias, catálogo de exploração ativa, exploit público e telemetria de exploração ativa — refletindo o presente da ameaça, não um score atribuído meses antes.

CASOS PÚBLICOS · PARTE 02

# Sete incidentes recentes · exploração em horas e dias

Sete incidentes públicos com exploração em massa dentro de até 15 dias após o disclosure — todos pós-CVE, todos dentro do ciclo de scan da maioria das organizações.



**O padrão por trás dos sete casos.** Cada incidente abaixo foi explorado em produção dentro de uma janela de até **15 dias após o disclosure público** — em vários casos, em **menos de 24 horas**. Todos pós-CVE, todos dentro do intervalo de um scan mensal. Nenhum deles seria capturado a tempo por GVUL tradicional.

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

Divulgada em 9 de dezembro de 2021. Cloudflare e Cisco Talos registraram tentativas de exploração em larga escala nas primeiras horas após o disclosure. RCE remoto não-autenticado em milhões de aplicações Java. Continuou sendo explorada em produção por meses após o patch.

**Tempo até exploração em massa · ≤ 24 horas**

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

Divulgada em 30 de março de 2022. PoC público em 24 horas, exploração ativa em ~48 horas após disclosure. Mass exploitation por botnets Mirai variants observada por múltiplos vendors. RCE em Spring Framework — stack web amplamente adotado em corporações.

**Tempo até exploração em massa · 24-48 horas**

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

Divulgada em 6 de abril de 2022. Sophos, Rapid7 e Morphisec detectaram exploração ativa por ~3 dias após o disclosure, com cryptominers e shells reversos. RCE via template injection em Workspace ONE Access — alvo de operações de movimentação lateral em redes corporativas.

**Tempo até exploração em massa · ~3 dias**

CRÍTICO **F5 BIG-IP · CVE-2022-1388**

Divulgada em 4 de maio de 2022. PoCs públicos em ~4 dias, exploração ativa em massa por volta de 9 de maio. Bypass de autenticação no iControl REST permitia RCE com privilégio root. Centenas de instâncias expostas comprometidas em poucos dias.

**Tempo até exploração em massa · ~5 dias**

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

Divulgada em 10 de outubro de 2023. Exploração em massa pós-disclosure observada em ~10 a 14 dias — afetando Boeing, Comcast e dezenas de outras. Captura de sessão sem autenticação adicional, com bypass efetivo de MFA via cookie roubado.

**Tempo até exploração em massa · ~10-14 dias**

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

Divulgada em 19-20 de fevereiro de 2024 pela ConnectWise. Bypass de autenticação trivial (criação de usuário admin via path manipulation). Mass exploitation observada em menos de 24 horas — Huntress, Sophos e CISA emitiram alertas urgentes.

**Tempo até exploração em massa · ≤ 24 horas**

CRÍTICO **CrushFTP · CVE-2024-4040**

Divulgada em 19 de abril de 2024. CrowdStrike e Rapid7 detectaram exploração ativa em horas. Path traversal permitia leitura de arquivos sensíveis sem autenticação, incluindo configurações e segredos. Centenas de instâncias expostas comprometidas no primeiro dia.

**Tempo até exploração em massa · ≤ 24 horas**

ATENÇÃO **A conclusão: antecipar deixa de ser refinamento**

Os sete incidentes compartilham um denominador: o intervalo entre disclosure e exploração em massa foi medido em **horas ou dias**, nunca em semanas. Qualquer defesa que opere em ciclo mensal — ou pior, trimestral — chega depois. A capacidade de antecipar o exploit, captando o sinal de risco antes da exploração, deixa de ser diferencial e torna-se a **única arquitetura viável** de gestão de exposição.

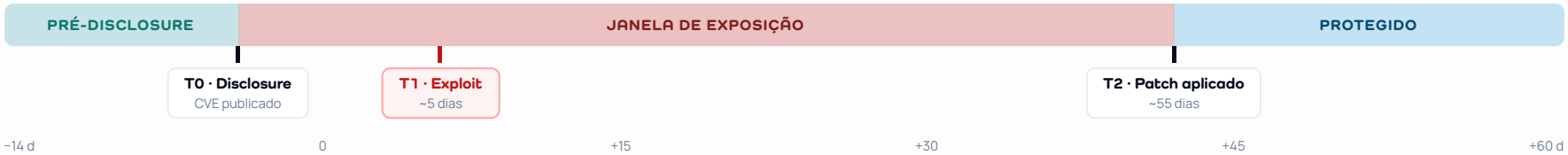
JANELA DE EXPOSIÇÃO · PARTE 03

# Anatomia da janela · do disclosure ao patch aplicado

Quatro marcos definem a janela de exposição. O intervalo entre o segundo e o quarto é onde o ataque acontece.



**Definição operacional.** Janela de exposição é o intervalo durante o qual uma vulnerabilidade é explorável na superfície de uma organização — começa quando o exploit se torna viável e termina quando o controle correspondente é aplicado. Quanto maior a janela, maior a probabilidade de exploração.




## Os quatro marcos da janela

0. **Pré-disclosure.** A vulnerabilidade existe no código e pode estar sendo explorada por atores com conhecimento privilegiado — zero-day. Para a defesa, esse período é invisível por definição. Em 2023, vários incidentes começaram nessa zona.
1. **Disclosure (T0).** O CVE é publicado, com ou sem patch disponível. A informação se torna pública — e o relógio do atacante começa a correr na mesma velocidade do relógio da defesa.
2. **Exploit observado (T1).** O primeiro exploit é registrado em produção. Em 2023, a mediana entre T0 e T1 foi de **5 dias** — em muitos casos, menos de 24 horas. Aqui se abre a fase mais perigosa da janela.
3. **Patch aplicado (T2).** A organização aplica o controle no ativo afetado. O Verizon DBIR observa, ano após ano, uma **mediana próxima de 55 dias** entre disclosure e correção em produção.[4]

**O cálculo da janela aberta.** Mediana de exploit em **5 dias**, mediana de remediação em **55 dias**. A janela é o intervalo entre os dois — **~50 dias por vulnerabilidade crítica**, em média, para a organização típica que opera no ciclo tradicional de gestão de vulnerabilidades.

## A pergunta defensiva

Se o exploit chega em 5 dias e o patch aplicado leva 55, a defesa tem três alavancas técnicas para reduzir a janela:

- **Antecipar a detecção** — observar a exposição antes do disclosure, via inteligência de ameaça e telemetria de borda.
- **Priorizar o que está sendo explorado** — não tratar todas as CVEs igualmente.
- **Encurtar o ciclo de descoberta e validação** — passar de fotografia mensal para fluxo contínuo.

A CURVA HISTÓRICA · PARTE 04

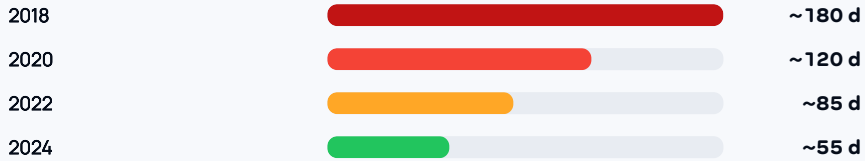
# Adoção de ASM × tempo de remediação · uma correlação inversa

À medida que plataformas de ASM ganharam adoção em mercados maduros, o tempo médio de remediação caiu. O movimento ocorreu nos EUA e na Europa. O Brasil ainda está na curva.



**A coincidência que não é coincidência.** Entre 2018 e 2024, o tempo médio de remediação de CVEs críticas em organizações dos EUA e da Europa caiu de cerca de 180 para 55 dias — uma redução de aproximadamente 70%. No mesmo período, o mercado global de Attack Surface Management cresceu a uma taxa composta anual estimada em ~27-29% (CAGR), atingindo um múltiplo de cerca de 4,5× o tamanho de 2018. Os dois movimentos são, em grande medida, o mesmo movimento.

### Mediana de tempo até remediação · CVEs críticas




Fontes: Edgescan Vulnerability Stats Report (séries 2019-2023), Verizon DBIR 2024. Mediana global; mercados EUA e Europa.

### Mercado de ASM · multiplicador acumulado vs. 2018


Fontes: MarketsandMarkets, Allied Market Research, 360iResearch (séries 2022-2030 normalizadas para base 2018). CAGR estimado: ~27-29%.

### A correlação observada

A queda do tempo de remediação não foi linear nem uniforme. Mercados que cedo adotaram ASM dedicado — EUA e Europa Ocidental — concentraram a maior parte da redução. Indústrias com regulação forte (finanças, defesa, infraestrutura crítica) puxaram a curva. Quando duas curvas opostas se cruzam com essa consistência ao longo de seis anos, a correlação deixa de ser hipótese e passa a ser leitura razoável: a adoção de plataformas especializadas em descoberta contínua e priorização dinâmica é o instrumento técnico que tornou possível encurtar a janela.

Não é o único fator — automação de pipelines, telemetria de cloud e maturação de processos contribuíram. Mas ASM é o componente que, nos mesmos seis anos, saiu de categoria nicho para item de orçamento padrão em programas de segurança corporativos.

**Brasil · onde está o atraso.** A adoção de ASM especializado no Brasil concentra-se no setor financeiro, puxada pela regulação BACEN. Fora dele, a maioria das organizações ainda opera o ciclo tradicional de gestão de vulnerabilidades — mensal ou trimestral. O tempo médio de remediação no mercado brasileiro permanece em uma faixa observada nos EUA e Europa em 2020-2021, com defasagem estimada de 3 a 4 anos em relação à curva mais avançada.

**O ASM adjacente × o ASM especializado.** Grandes plataformas de TI corporativa (Microsoft Defender, Tenable, Qualys, Rapid7) incorporaram módulos de External Attack Surface Management ao redor do produto principal. Esses módulos cobrem inventário e, em alguns casos, descoberta. Não foram desenhados, contudo, com foco em **velocidade de detecção** e **priorização dinâmica em tempo real** — diferença que separa o produto adjacente do produto dedicado, e que determina se a janela de exposição será de dias ou de meses.

O PARADIGMA PONTUAL · PARTE 04

# A gestão de vulnerabilidades tradicional · uma fotografia que envelhece

O ciclo de scan anual e mensal foi desenhado para um mundo em que o exploit chegava em meses — não em dias.



### O que o ciclo pontual entrega — e o que ele perde

A gestão de vulnerabilidades tradicional opera em ciclos. O scanner é programado para varrer o parque em uma cadência fixa — anual em muitas organizações, trimestral nas mais maduras, mensal nas que mais investem em segurança. Cada execução é uma fotografia: registra o estado do parque no instante em que o scan rodou.

Entre uma fotografia e a próxima, a realidade muda. Novos ativos sobem em nuvem. Configurações são alteradas. Bibliotecas recebem versões. Vulnerabilidades novas são divulgadas. Tudo isso fica fora do registro até a próxima execução do scanner — e, ao chegar lá, junta-se ao fluxo de descobertas que entra na fila de remediação.

Esse modelo funciona quando a velocidade do atacante é comparável à cadência do scan. Em 2015, com tempo médio de exploit acima de 100 dias, um scan mensal estava razoavelmente alinhado à ameaça. Em 2023, com exploit em 5 dias, a fotografia mensal mostra um estado que já não existe mais — e a janela permanece aberta entre fotografias.

### O gap matemático · janela aberta por ciclo de GVUL

| CADÊNCIA DO SCAN | JANELA MÁXIMA ENTRE SCANS | VS. EXPLOIT EM 5 D |
|---|---|---|
| **Anual** | 365 dias | 73× a janela do atacante |
| **Trimestral** | 90 dias | 18× a janela do atacante |
| **Mensal** | 30 dias | 6× a janela do atacante |
| **Semanal** | 7 dias | 1,4× a janela do atacante |
| **Contínuo** | < 1 dia | aderente à ameaça |

O scan rodando uma vez por mês deixa a organização em uma janela seis vezes maior que a do atacante mediano. Em ativos críticos, essa proporção é a diferença entre detectar uma vulnerabilidade antes ou depois da exploração.

**O delay adicional do processo.** O scan é apenas o ponto de partida. Triagem, atribuição, janela de manutenção, validação e re-scan estendem o ciclo total. Em organizações de médio porte, a mediana entre detecção e remediação de uma CVE crítica permanece em torno de **55 dias**, segundo o Verizon DBIR — mesmo quando o scan opera mensalmente.[4]

O CUSTO DA JANELA · PARTE 05

# O preço de uma janela aberta · em dias e em reais

A janela de exposição é, em essência, uma métrica de risco financeiro — quanto maior, mais alta a probabilidade e o custo do incidente.



**194 dias**
tempo médio para identificar uma violação · IBM Cost of a Data Breach 2024 [5]

**R$ 7,19 mi**
custo médio de uma violação no Brasil — média de 2024

**–R$ 4,9 mi**
redução média de custo quando a detecção ocorre em menos de 200 dias vs. mais de 200

### A correlação entre janela e custo

O IBM Cost of a Data Breach Report 2024 documenta, ano após ano, uma correlação inequívoca: **quanto maior o tempo entre o comprometimento e a detecção, maior o custo final do incidente**. Organizações que detectaram e contiveram em menos de 200 dias gastaram, em média, US$ 4,93 milhões — ante US$ 5,46 milhões nas que levaram mais de 200 dias. A diferença é estrutural.

O motivo é matemático. Um atacante com mais tempo dentro do perímetro tem mais ativos descobertos, mais privilégios acumulados, mais dados acessados e mais tempo para preparar a movimentação lateral e a exfiltração. Cada dia de janela aberta amplia, simultaneamente, a probabilidade e a magnitude da perda.

Janela de exposição, nessa leitura, constitui o **parâmetro central** que liga a postura técnica de uma organização à sua exposição financeira. Reduzi-la é a alavanca mais direta de redução de custo esperado.

**O custo da janela na linguagem do CFO.** Cada dia de janela aberta tem um custo esperado proporcional à probabilidade de exploração naquele dia e ao impacto financeiro do incidente correspondente. Para uma vulnerabilidade crítica em ativo de produção, esse custo diário pode ser estimado em milhares de reais por dia exposto — composição que se torna a base do cálculo de ROI da remediação.

### O efeito composto sobre o portfólio

Em uma organização com centenas de ativos e dezenas de vulnerabilidades críticas em aberto a qualquer momento, o custo da janela é cumulativo. Não basta avaliar a janela de um ativo — é necessário somar o custo esperado de cada janela aberta no portfólio.

A redução média de 50 dias para 10 dias de janela em uma vulnerabilidade crítica corresponde, em ALE, a uma redução de aproximadamente **80%** da exposição esperada daquela vulnerabilidade. Aplicada ao portfólio inteiro, a redução de janela torna-se a alavanca de maior retorno do programa de segurança.

MONITORAMENTO CONTÍNUO · PARTE 06

# O novo paradigma · quatro princípios do monitoramento contínuo

Não é o scan rodando mais vezes. É um modelo operacional diferente, em que descoberta, avaliação e priorização operam em fluxo.

Whitepaper 2026
CSURFACE

**O que monitoramento contínuo não é.** Não é rodar o scanner com mais frequência. Um scan mensal acelerado para semanal continua sendo o mesmo paradigma — fotografia, fila, ciclo. Monitoramento contínuo é uma **mudança de modelo operacional**: descoberta em fluxo, postura observada em tempo real, priorização dirigida por ameaça ativa, e ação disparada por evento.

## OS QUATRO PRINCÍPIOS DO MONITORAMENTO CONTÍNUO

1. **Descoberta em fluxo**
   Cada novo ativo, cada mudança de configuração e cada novo componente entra automaticamente no escopo no momento em que aparece — sem esperar a próxima rodada do scanner.

2. **Postura observada**
   A avaliação de postura é refeita continuamente, ativo por ativo, a cada alteração observada no estado externo.

3. **Priorização por ameaça ativa**
   A ordem da fila é determinada pela ameaça real e observada. Quem está sendo explorado agora sobe à frente; o score estático de uma CVE publicada meses antes cede posição.

4. **Ação disparada por evento**
   Mudanças relevantes geram alertas que alimentam diretamente o ciclo de remediação — sem precisar esperar o próximo relatório periódico.

### O que muda na operação

No modelo pontual, a equipe de GVUL espera o scan, recebe um relatório com centenas de achados, faz triagem por score estático, atribui responsabilidade e abre tickets. O ciclo se repete na próxima execução.

No modelo contínuo, a equipe trabalha sobre **um fluxo de eventos significativos** — novos ativos, mudanças de postura, vulnerabilidades novas em produção, evidência de exploração ativa contra organizações pares. Cada evento traz seu contexto e sua prioridade já calculados; a triagem deixa de ser exercício de varredura e passa a ser de decisão.

**Frameworks que pedem monitoramento contínuo.** O modelo contínuo é o que múltiplos frameworks já recomendam há mais de uma década. **NIST CSF** (DE.CM-8: continuous vulnerability scans), **CIS Controls v8** (Control 7: Continuous Vulnerability Management), **ISO 27001:2022** (A.8.8: gestão de vulnerabilidades técnicas em base contínua) e **PCI DSS 4.0** (Req. 6.3.1: identificar vulnerabilidades continuamente) já estabelecem o padrão. A defasagem está na implementação, não na norma.

O PAPEL DA CSURFACE · PARTE 07

# Como a CSURFACE fecha a janela

Descoberta contínua + threat sensor + priorização dinâmica — os três instrumentos pelos quais a plataforma opera na cadência do atacante.



### Descoberta contínua da superfície externa

A plataforma mapeia a superfície externa da organização em fluxo — cada novo subdomínio, cada novo certificado, cada nova exposição entra automaticamente no escopo no momento em que se torna observável. Não há janela de scan: o intervalo entre o aparecimento de um ativo novo e a sua entrada no inventário é tipicamente de horas.

É essa base que torna possível tudo o resto — sem descoberta contínua, o threat sensor e a priorização dinâmica operariam sobre um inventário que envelhece.

### Threat sensor · sinal de ameaça em tempo real

O threat sensor da CSURFACE observa, em tempo real, a **atividade de exploração observada** contra a superfície monitorada: tentativas de exploração, inteligência de exploits publicados, indicadores de campanha em curso, telemetria de fontes externas. O resultado é uma leitura de ameaça que reflete o presente da exploração — não a estimativa estática de um score publicado meses antes.

É essa leitura que decide a ordem da fila: vulnerabilidades sob exploração ativa sobem ao topo, mesmo quando seu CVSS é menor que outras pendentes.

### O contraste com o ciclo pontual

| DIMENSÃO | CICLO PONTUAL | CSURFACE |
|---|---|---|
| Cadência de descoberta | Mensal / trimestral | Contínua |
| Postura externa | Snapshot do scan | Observada |
| Priorização | CVSS estático | Threat sensor |
| Recalibragem | Próxima execução | Em fluxo |
| Time-to-detect mediano | 15-30 dias | < 24 horas |

**O resultado em janela.** A combinação reduz a janela de exposição típica de uma vulnerabilidade crítica em ativo monitorado de **~50 dias** (cenário tradicional) para a **cadência de remediação interna da organização** — porque a detecção deixa de ser o gargalo. A janela passa a depender apenas da velocidade interna de aplicação do controle.

APLICAÇÃO E CONFORMIDADE · PARTE 08

# O mesmo trabalho que protege e comprova

Monitoramento contínuo é o que múltiplas regulações já exigem. Aplicá-lo atende, em um só esforço, à proteção e à evidência regulatória.



### Requisitos regulatórios e normativos

| NORMA | REQUISITO | ADERÊNCIA |
|---|---|---|
| **BACEN 4.557** | Gestão de risco operacional · monitoramento contínuo de vulnerabilidades | Atendido |
| **NIST CSF** | DE.CM-8 · varreduras contínuas de vulnerabilidades | Atendido |
| **CIS Controls v8** | Control 7 · Continuous Vulnerability Management | Atendido |
| **ISO 27001:2022** | A.8.8 · gestão de vulnerabilidades técnicas em base contínua | Atendido |
| **PCI DSS 4.0** | Req. 6.3.1 · identificar vulnerabilidades continuamente | Atendido |
| **LGPD · Art. 46** | Medidas técnicas aptas a proteger dados pessoais | Suporta |

A leitura "atendido" indica que o monitoramento contínuo da CSURFACE entrega, na prática, o requisito técnico que cada norma estabelece. A aderência formal depende do escopo contratado e da política interna da organização.

**Conformidade como subproduto.** O trabalho técnico de monitoramento contínuo entrega, no mesmo movimento, a evidência que cada uma dessas normas exige — um inventário verificável, datado e auditável de cada descoberta, alteração e remediação. A organização deixa de manter duas operações paralelas (uma para o controle, outra para a evidência) e passa a operar com uma trilha única.

### O argumento para o comitê de auditoria

O comitê de auditoria não pede ferramenta — pede **evidência de controle operando**. Em um modelo pontual, a evidência é o relatório do scan mensal. Em um modelo contínuo, a evidência é a trilha que mostra, para cada vulnerabilidade crítica, o tempo entre o aparecimento da exposição, a detecção e a remediação.

Em organizações reguladas — BACEN, B3, ANS —, essa trilha passa a ser a base do KRI (Key Risk Indicator) de janela de exposição, comparável trimestre a trimestre.

APÊNDICE · FONTES

# Metodologia e fontes

As referências externas que sustentam os dados deste whitepaper.



## Referências

1. **Telemetria de emerging threats da CSURFACE.** Pipeline próprio de monitoramento que correlaciona CVE (NVD), índice de probabilidade de exploração, catálogo de exploração ativa, observação de exploração ativa e telemetria de campanha. Série histórica 2020-2026 (parcial) usada nos gráficos da página 3 e nos KPIs do sumário executivo. Funnel de CVE: publicação NVD → monitorados → probabilidade de exploração > 10% → exploração confirmada → TTE ≤ 5 dias → zero-day.
2. **Mandiant M-Trends 2024.** Relatório anual da Mandiant (Google) sobre tendências de ameaça. Edição de abril de 2024 (dados de 2023) registra mediana de Time-to-Exploit de 5 dias, corroborando o salto observado pela telemetria da CSURFACE em 2024.
3. **Google Threat Analysis Group + Mandiant.** Relatório conjunto sobre zero-days. Documenta crescimento sustentado de zero-days explorados em produção e atribuição parcial a fornecedores comerciais de vigilância.
4. **Verizon DBIR 2024 e 2025.** Análise anual de incidentes corporativos. DBIR 2024 reporta crescimento de 180% em violações originadas em exploração de vulnerabilidade; DBIR 2025 projeta aceleração específica em dispositivos de borda.
5. **IBM Cost of a Data Breach Report 2024.** Relatório anual com base em incidentes investigados em mais de 600 organizações em 17 países. Mediana global de identificação de violação: 194 dias.
6. **MOVEit Transfer · CVE-2023-34362.** Incidente reportado pela Progress Software em junho de 2023. Estimativas de impacto agregadas por Emsisoft e Bleeping Computer.

## Nota metodológica

As contagens de CVEs com exploração rápida (TTE ≤ 5 dias) citadas neste whitepaper são produzidas pela telemetria de emerging threats da CSURFACE, computadas sobre o universo total de CVEs publicadas na NVD a cada ano. A metodologia combina o feed NVD com sinal de exploração ativa, índice de probabilidade de exploração e catálogo de exploração ativa, e produz um funnel anual desde 2020. A mediana de TTE em dias, publicada pela Mandiant nos relatórios M-Trends, é usada como referência corroborativa.

As medianas de tempo até remediação citadas seguem a metodologia do Verizon DBIR, que computa o intervalo entre disclosure e correção efetiva em ambiente de produção, considerando o conjunto de organizações com incidentes investigados no ano.

Os dados específicos de cada caso (Log4Shell, MOVEit, Citrix Bleed, Confluence, Ivanti Connect Secure) seguem as comunicações dos próprios fornecedores e as análises técnicas publicadas por equipes de pesquisa em segurança (Cloudflare, Cisco Talos, Microsoft Threat Intelligence, Volexity).

**O que este whitepaper não cobre.** Este material é educacional e descritivo. Não constitui projeção atuarial, recomendação jurídica ou regulatória. Os números mencionados são valores medianos de população observada; a aplicação a uma organização específica requer modelagem da própria janela com base na sua superfície, postura e telemetria.

PRÓXIMOS PASSOS

# Feche a janela antes do próximo exploit

A gestão contínua de exposição é uma das capacidades da plataforma CSURFACE — uma plataforma de Continuous Exposure Management. Em arquitetura integrada, reúne descoberta contínua da superfície externa com Machine Learning, análise da cadeia digital de fornecedores, validação de exploitabilidade, inteligência de ameaças com priorização dinâmica, monitoramento de credenciais vazadas e quantificação financeira de risco. Opera de forma integralmente externa — sem agente e sem instalação —, com integrações opcionais de nuvem, WAF e CIEM disponíveis para organizações que buscam maior profundidade de visibilidade.

**Meça a janela do seu parque**

Em uma análise preliminar gratuita, a CSURFACE mapeia a superfície externa da organização e reporta a janela de exposição observada nos ativos críticos.

**Use a calculadora de risco**

Estime o impacto financeiro da sua janela de exposição com a calculadora pública da CSURFACE, calibrada por benchmark de mercado.

**Leia o whitepaper de Threat Intel**

O detalhamento da priorização dinâmica — como o índice de probabilidade de exploração, o catálogo de exploração ativa e o threat sensor da CSURFACE compõem a fila real de remediação.

**Quer ver a janela de exposição dos seus ativos — gratuitamente?**

Solicitar análise gratuita