CSURFACE

WHITEPAPER · ATTACK SURFACE MANAGEMENT

Você só enxerga uma parte da sua superfície de ataque

ML-Powered Discovery: como identificar o que as plataformas de enumeração de subdomínios não revelam — Shadow IT, infraestrutura herdada, APIs não documentadas e a cadeia digital de fornecedores.

CAPACIDADE	PÚBLICO	EDIÇÃO
Attack Surface Management	CISO · Security Engineering	2026

LEITURA	CLASSIFICAÇÃO	FONTE
11 páginas	Público	Plataforma CSURFACE

SUMÁRIO EXECUTIVO

A descoberta de ativos é um problema de inteligência

A tese deste whitepaper, em uma página — o essencial antes do detalhamento técnico.

INCIDENTES POR ATIVO NÃO GERENCIADO

74%

das organizações relataram incidentes causados por ativos desconhecidos ou não gerenciados[1]

ATAQUES VIA ATIVO EXPOSTO

69%

sofreram um ataque originado em ativo exposto na internet, desconhecido ou não gerenciado[2]

DESCOBERTA COM MACHINE LEARNING

2–3×

mais ativos que a enumeração de subdomínios — e, em superfícies dispersas, muito além

A maioria das ferramentas de Attack Surface Management (ASM) parte de uma premissa frágil: a de que enumerar subdomínios a partir de listas públicas é suficiente para cobrir a superfície de ataque. A prática demonstra o contrário. A maior parte da superfície real encontra-se fora dessas listas — **Shadow IT contratado sem o conhecimento da área de TI, infraestrutura herdada de fusões e aquisições, APIs não documentadas e ambientes de homologação expostos**.

Pesquisas de mercado independentes convergem nesse diagnóstico. Levantamento global da Trend Micro com mais de dois mil líderes de segurança aponta que **74% das organizações sofreram incidentes causados por ativos não gerenciados**[1]; estudo da Enterprise Strategy Group registra que **69% foram alvo de um ataque originado em um ativo exposto e desconhecido**[2]. O que permanece fora do inventário constitui a porção da superfície sobre a qual não há observação — o ponto cego operacional sobre o qual nenhum controle pode atuar.

Este whitepaper apresenta a abordagem da CSURFACE: o **ML-Powered Discovery**, que combina coleta passiva de sinais públicos, correlação por uma stack de motores de Machine Learning, detecção de Shadow IT e mapeamento da cadeia digital de fornecedores — sem agente, sem instalação e sem trabalho manual por ativo.

A tese. A descoberta de ativos é um problema de inteligência. A correlação de sinais por Machine Learning revela o que fontes isoladas — como o DNS público — não alcançam. E o que permanece fora do inventário permanece sem proteção.

O que este documento cobre

- Por que a superfície de ataque cresceu — e por que as ferramentas não acompanharam.
- As quatro lacunas estruturais da enumeração por wordlist.
- As quatro técnicas que compõem o ML-Powered Discovery, com destaque para o motor de correlação.
- Um caso de uso representativo e os indicadores de resultado esperados.

O CENÁRIO · PARTE 01

A superfície expandiu — as ferramentas, não

Do que se compõe a superfície de ataque em 2026 e por que o inventário tradicional já nasce incompleto.

SUPERFÍCIE DE ATAQUE · ~2014

Pequena e estável

DNS público | Servidores de e-mail | VPN

→

SUPERFÍCIE DE ATAQUE · 2026

Dispersa por toda a operação

DNS público | E-mail | VPN | SaaS & Shadow IT | APIs não documentadas | Múltiplas nuvens | Heranças de M&A | Cadeia de fornecedores | Ambientes efêmeros & low-code

74%
das organizações sofreram incidentes causados por ativos desconhecidos ou não gerenciados[1]

69%
foram alvo de um ataque originado em um ativo exposto e desconhecido[2]

~40%
da infraestrutura corporativa permanece invisível à equipe de TI[4]

Por que a superfície cresce sem governo

A superfície de ataque externa não é um inventário organizado — ela se acumula. Cada equipe de produto publica uma aplicação, cada área de negócio contrata um SaaS, cada aquisição incorpora a infraestrutura herdada de outra empresa. A ausência de processos formais de desativação faz com que esse acúmulo raramente seja revertido.

Segundo a Unit 42 (Palo Alto Networks), a superfície de uma organização incorpora, em média, **mais de 300 novos serviços por mês**[5]. Um inventário mantido manualmente não acompanha esse ritmo: torna-se incompleto na medida em que é concluído.

O resultado é uma lacuna estrutural entre a superfície que a organização *acredita* ter e a que de fato expõe. Ativos ausentes do inventário permanecem sem observação, sem priorização e sem resposta — e constituem o vetor preferencial de entrada para o atacante.

Por que isso importa. O inventário é a base de todo programa de segurança. Sem o conhecimento do que existe, a priorização, os testes e a resposta a incidentes operam sobre uma base incompleta — e o que ficou de fora permanece exposto.

O custo de não enxergar. O custo médio de uma violação de dados no Brasil alcançou **R$ 7,19 milhões** em 2025, segundo o IBM Cost of a Data Breach 2025[3]. A sanção administrativa da LGPD pode chegar a 2% do faturamento, limitada a R$ 50 milhões. A descoberta contínua reduz a probabilidade de incidente ao eliminar pontos cegos — e a cada redução de probabilidade corresponde uma redução direta e proporcional da exposição financeira esperada.

LIMITAÇÕES ATUAIS · PARTE 02

Por que a enumeração de subdomínios não basta

As plataformas de ASM do mercado baseiam-se em enumeração de subdomínios — um método que resolve o caso óbvio e falha onde o risco se concentra.

O que as plataformas de enumeração de subdomínios fazem

As plataformas de ASM disponíveis no mercado baseiam-se, em essência, na enumeração de subdomínios: listas de prefixos comuns (**mail.**, **dev.**, **staging.**, **api.**), permutações do nome da empresa e consultas a fontes públicas.

Esse método localiza **mail.empresa.com** e **staging.empresa.com**. Não localiza:

- **api-gtw-prd-v3-fc8a.empresa.com** — identificador gerado automaticamente.
- **tenant-b3b9e0.empresa.com** — subdomínio multi-tenant.
- Um domínio adquirido em fusão, com convenção de nomes distinta.
- SaaS hospedado em terceiros — **empresa.atlassian.net**, **empresa.salesforce.com**.

O ponto cego é estrutural. A enumeração de subdomínios localiza apenas o que alguém previamente imaginou que existiria. O risco relevante encontra-se justamente naquilo que não foi previsto — e que, por isso, não foi procurado.

As quatro lacunas da enumeração de subdomínios

1. **Shadow IT em SaaS de terceiros.** As áreas de marketing, RH e vendas contratam ferramentas que criam URLs públicas vinculadas à empresa. Nenhuma lista genérica as identifica.
2. **Convenções de nomenclatura próprias na nuvem.** Cada equipe provisiona recursos com o seu próprio padrão de nomes, ao qual uma lista genérica não tem acesso.
3. **Heranças de fusões e aquisições.** Os domínios de empresas adquiridas permanecem ativos por anos, sem governança — e a enumeração de subdomínios não conhece a organização incorporada.
4. **Ambientes efêmeros.** Pull requests geram ambientes de pré-visualização com URLs únicas, e pipelines de CI/CD criam hostnames a cada execução.

Cada uma dessas lacunas representa, na prática, um ponto de entrada ausente de qualquer inventário — não catalogado, não monitorado e, portanto, não corrigido.

A ABORDAGEM CSURFACE · PARTE 03

O motor de correlação — quando o WHOIS não basta

Coleta passiva de sinais públicos e correlação por Machine Learning — as duas primeiras camadas do Discovery.

ML-POWERED DISCOVERY · O PROCESSO DE DESCOBERTA

1. **Coleta passiva** — Sinais públicos, sem tocar a infraestrutura.
2. **Coleta ativa** — Verificação ativa e não-intrusiva dos candidatos.
3. **Correlação por ML** — Estima a probabilidade de propriedade de cada ativo.
4. **Revisão humana** — Especialistas decidem os casos ambíguos.
5. **Stack de tecnologias** — Identificação ativa das tecnologias de cada ativo.
6. **Vulnerabilidades e exposição** — Mapeamento das falhas e exposições de cada ativo.

O WHOIS deixou de ser prova de propriedade. Atualmente, a maioria dos domínios opera sob proteção de privacidade ou redação dos dados de registro, o que mantém o titular real oculto. A consulta ao WHOIS, isoladamente, não estabelece mais a quem um ativo pertence — a determinação de propriedade passou a exigir inferência, não simples consulta.

01. Coleta passiva de sinais

A descoberta inicia-se de forma inteiramente passiva. A CSURFACE reúne e cruza um amplo conjunto de informação pública disponível na internet — um universo de sinais consideravelmente mais largo do que o DNS público sobre o qual as plataformas tradicionais se apoiam.

Nenhum pacote é enviado à infraestrutura da organização nesta etapa: a coleta é não-intrusiva e não gera ruído nos ativos analisados. Essa base ampla de evidências é a matéria-prima sobre a qual o motor de correlação atua.

Quanto mais larga e diversa a base de sinais, maior a capacidade do motor de correlação de distinguir o que pertence à organização do que não pertence — com a consequente redução de atribuições incorretas e ampliação da cobertura real da superfície.

02. O motor de correlação — uma stack de Machine Learning

Se o WHOIS não responde mais à pergunta sobre propriedade, a CSURFACE a responde por correlação. A informação pública coletada alimenta uma **stack de motores de Machine Learning** — cada um com características próprias, treinado para uma leitura distinta dos dados — que operam de forma combinada.

O objetivo é comum a todos: identificar padrões e estimar a **probabilidade de um ativo pertencer à organização** analisada. A decisão final resulta do consenso da stack — é esse arranjo coletivo, e não um modelo isolado, que sustenta a precisão.

Cada atribuição vem acompanhada da **probabilidade** e das evidências que a sustentam — trata-se de um resultado auditável, que a equipe de segurança pode verificar e contestar.

Precisão mensurada. Em operação combinada, a stack de correlação alcança um **score F1 agregado superior a 0,900**. Com esse nível de confiança, a plataforma identifica a propriedade de domínios, organizações, aplicações web, FQDNs, endereços IP e demais classes de ativo.

O QUE A CSURFACE OBSERVA · DADOS PRÓPRIOS DA PLATAFORMA

122 mil
ativos externos descobertos em 68 organizações analisadas pela plataforma

1.068
organizações relacionadas — subsidiárias e coligadas — reveladas pela descoberta

até 173
organizações relacionadas mapeadas a partir de um único domínio raiz

A ABORDAGEM CSURFACE · PARTE 03

Shadow IT, cadeia de fornecedores e o resultado mensurável

As duas técnicas restantes — e o que a abordagem muda, lado a lado com a enumeração tradicional.

03. Detecção de Shadow IT

A plataforma identifica o SaaS de terceiros conectado à organização — ferramentas contratadas pelas áreas de negócio que criam presença pública vinculada à empresa. Esse Shadow IT, invisível ao inventário oficial, é reconhecido pela correlação de múltiplos indícios públicos que o associam ao cliente.

04. Mapeamento da cadeia de fornecedores

Para cada ativo descoberto, a plataforma mapeia as APIs externas chamadas, os CDNs e o JavaScript de terceiros, os provedores de nuvem compartilhados e as bibliotecas embutidas — a cadeia digital de fornecedores que expande a superfície sem constar de qualquer inventário.

Especialista, não acessório. Para as grandes plataformas de segurança, o produto central é o scanner e a gestão de vulnerabilidades; o módulo de ASM foi acrescentado posteriormente, como um componente acessório que apenas alimenta o motor já existente — e no qual a velocidade e a precisão da descoberta não constituem prioridade. A CSURFACE adota a posição oposta: a descoberta é o produto. A plataforma foi concebida como um instrumento dedicado a manter o cliente ciente da sua exposição no menor tempo e com a maior precisão possíveis.

Diferenciadores mensuráveis

CRITÉRIO	ENUMERAÇÃO DE SUBDOMÍNIOS	CSURFACE · ML DISCOVERY
Cobertura típica da superfície	30–40%	**80–95%**
Detecção de Shadow IT	Limitada ou inexistente	**Ativa**
Esforço manual por ativo	3–10 horas	**Zero**
Frequência	Pontual / agendada	**Contínua, 24/7**
Profundidade da cadeia de fornecedores	Um nível, quando há	**Até três níveis**
Entrada necessária	Lista de ativos conhecida	**Apenas o domínio raiz**

Faixas observadas em descobertas conduzidas pela plataforma CSURFACE; ver nota metodológica na página 10. O resultado varia conforme o tamanho e a dispersão da superfície de cada organização.

APLICAÇÃO E RESULTADOS · CASO 01

Uma startup de ERP: de 84 a 570 ativos

O que um inventário de gestão de vulnerabilidades deixava de fora — e que a descoberta contínua tornou visível e priorizável.

INVENTÁRIO PELA GESTÃO DE VULNERABILIDADES

84

ativos — o que a empresa acreditava ser toda a sua exposição externa.

→

MAPEADO PELA CSURFACE

570

ativos na superfície real — **quase 7×** o inventário conhecido.

O caso

Uma startup de software ERP acompanhava a sua exposição externa por uma plataforma tradicional de gestão de vulnerabilidades. O inventário registrava **84 ativos**, e a equipe acreditava que esse número representava a totalidade da sua superfície de ataque.

Em poucos minutos de descoberta com a CSURFACE, a superfície real revelou-se composta por **570 ativos**. Entre o que estava exposto e fora do radar:

ATENÇÃO **Certificados digitais expirados**
Em serviços ainda acessíveis pela internet.

ATENÇÃO **Software em fim de vida (EoL)**
Ativos legados sem suporte do fornecedor nem correções de segurança.

CRÍTICO **Vulnerabilidades invisíveis**
Em ativos que o inventário sequer conhecia — logo, jamais avaliados.

CRÍTICO **Dados sensíveis expostos**
Erros de configuração que expunham dados de sistemas internos.

CRÍTICO **Painéis administrativos expostos**
De alto risco; deveriam estar restritos à rede interna.

Em conjunto, esses achados configuravam um perfil de risco significativamente superior ao nível aceitável pela organização — sem que qualquer um deles houvesse sido catalogado ou avaliado.

Por que passou despercebido

Uma plataforma tradicional de gestão de vulnerabilidades examina apenas o que lhe é informado: varre uma lista, não descobre a superfície. Tudo o que não constava da lista de 84 ativos permanecia, por definição, invisível.

Um padrão recorrente, não uma exceção. Segundo a Unit 42 (Palo Alto Networks), a superfície de ataque de uma organização incorpora, em média, **mais de 300 novos serviços por mês**[5]; e mais de **25% das exposições** envolvem infraestrutura crítica de TI — incluindo páginas de login administrativas acessíveis pela internet[5]. Um inventário estático torna-se progressivamente incompleto à medida que a superfície evolui.

O resultado

O ganho imediato foi a **visibilidade**: de 84 ativos presumidos para 570 reais, o risco deixou de ser invisível e passou a ser priorizável. A gestão efetiva da exposição pressupõe, como condição anterior, o conhecimento completo da superfície a gerir.

APLICAÇÃO E RESULTADOS · CASO 02

Um grande banco: empresas inteiras fora do inventário

Crescimento por aquisições, superfície em mudança constante e confiança excessiva nas ferramentas tradicionais.

O ponto de partida

O banco chegou à CSURFACE com três questões em aberto:

Sem visibilidade da superfície externa

Falta de controle sobre o que estava, de fato, exposto.

Confiança excessiva no tradicional

As ferramentas existentes só enxergavam o inventário já conhecido.

Risco na cadeia e nas aquisições

Cada empresa adquirida ampliava a superfície sem governança.

O que a descoberta revelou

Um grande banco — reconhecido pela atuação em asset management e por um histórico de grandes aquisições nos últimos anos, de operações de logística a redes de hotéis — convivia com uma superfície em mudança permanente. O ambiente corporativo, as múltiplas nuvens e cada nova aquisição passavam a ser responsabilidade do time de segurança cibernética.

Após algumas semanas com a plataforma CSURFACE, o banco identificou **estruturas de empresas inteiras — dentro e fora do país — que não estavam sob o seu radar**. Parte delas apresentava vulnerabilidades e exposições que exigiram intervenção urgente.

O volume e a dispersão superaram as estimativas internas: ativos distribuídos por múltiplas nuvens e estruturas corporativas inteiras que nenhuma equipe havia mapeado, sem responsável designado, sem monitoramento e sem qualquer processo de resposta estabelecido.

Correção dentro da janela crítica. Em um dos ativos, a plataforma detectou uma vulnerabilidade de impacto **9.8 (CVSS)** no mesmo dia da sua divulgação pública. O time de segurança foi alertado e a corrigiu ainda dentro do período crítico — quando a falha já era explorada massivamente na internet. Um incidente potencialmente severo foi evitado.

Adoção pela governança. As equipes de governança da segurança da informação (GSI) passaram a usar a plataforma para documentar e compreender organizações e ativos sobre os quais, até então, não havia qualquer visibilidade.

A leitura

Em uma organização que cresce por aquisição, a superfície de ataque muda mais rápido do que qualquer processo manual de inventário. A descoberta contínua deixa de ser conveniência e torna-se condição para governar o risco.

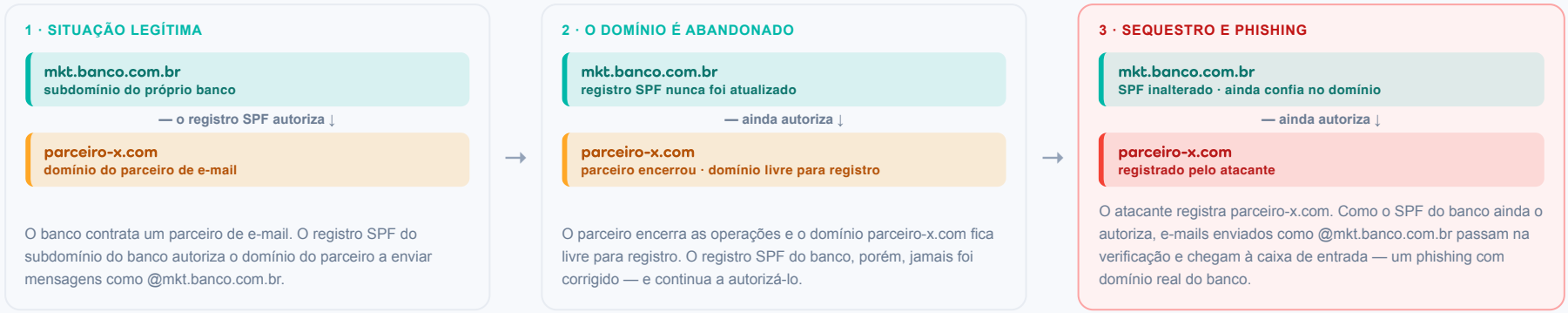
APLICAÇÃO E RESULTADOS · CASO COMPLEMENTAR

Anatomia de um phishing perfeito — evitado

Como um subdomínio não gerenciado e um registro SPF desatualizado criaram as condições para um phishing com infraestrutura legítima do banco.

O sequestro de um domínio autorizado no SPF

O risco nasce de uma distinção sutil entre **dois domínios diferentes**: o **subdomínio do próprio banco**, que contém o registro SPF, e o **domínio de um terceiro**, que esse registro autoriza a enviar e-mails. Quando o segundo é abandonado, o primeiro continua a confiar nele.



O vetor composto — SPF sequestrado somado ao subdomain takeover

A plataforma identificou, no mesmo banco, **subdomínios passíveis de takeover** — apontando para serviços de nuvem desativados e, por isso, reivindicáveis por terceiros. Combinadas, as duas falhas permitiriam um phishing quase indetectável: um e-mail enviado de um domínio legítimo do banco — via SPF sequestrado — contendo um link para outro domínio legítimo do banco — via subdomínio sequestrado. Para o correntista, todos os sinais apontariam para o banco verdadeiro.

O desfecho. Nenhuma das duas falhas era visível para as ferramentas tradicionais do banco — ambas viviam em ativos fora do inventário. A CSURFACE as sinalizou, e o banco corrigiu os registros e os subdomínios antes que fossem encontrados. A campanha real SubdoMailing — que chegou a enviar milhões de e-mails por dia a partir de domínios legítimos sequestrados[6] — confirma que a ameaça não é hipotética.

METODOLOGIA E FONTES

A origem de cada número

Como este documento distingue pesquisa de mercado pública de métricas observadas pela plataforma.

Nota metodológica

Este whitepaper combina duas naturezas de dado, mantidas distintas ao longo do texto:

Estatísticas de mercado. Atribuídas, no ponto de uso, a pesquisas públicas de terceiros e identificadas por marcador numérico. As referências completas constam ao lado.

Métricas da plataforma. Indicadores como a cobertura de 80 a 95% da superfície, o ganho de duas a três vezes em ativos descobertos e o score F1 agregado superior a 0,900 resultam de descobertas conduzidas pela própria plataforma CSURFACE. Variam conforme o tamanho e a dispersão da superfície de cada organização.

Nenhuma estatística é apresentada sem fonte. Os casos descritos baseiam-se em engajamentos reais e são anonimizados — nenhuma organização é identificada.

Material educacional. Este documento destina-se a fins informativos. As metodologias descritas refletem o estado da plataforma CSURFACE na data de publicação.

Referências

1. **Trend Micro.** Pesquisa global sobre incidentes de segurança causados por ativos não gerenciados, conduzida com mais de 2.000 líderes de segurança. 2025.
2. **Enterprise Strategy Group.** Pesquisa sobre exploração de ativos expostos na internet, desconhecidos ou não gerenciados. Reportada por SC Media.
3. **IBM.** Cost of a Data Breach Report 2025 — custo médio de violação de dados no Brasil: R$ 7,19 milhões.
4. **Gartner.** Análises sobre visibilidade de infraestrutura corporativa e External Attack Surface Management (EASM).
5. **Unit 42 (Palo Alto Networks).** 2024 Attack Surface Threat Research — exposições de infraestrutura conectada à internet e ritmo de crescimento da superfície de ataque.
6. **Guardio Labs.** SubdoMailing — investigação sobre o sequestro de subdomínios e registros SPF para campanhas de phishing em larga escala. 2024.

As estatísticas de mercado citadas têm caráter público. Os percentuais podem variar conforme a metodologia e o recorte amostral de cada estudo.

PRÓXIMOS PASSOS

A descoberta começa com um único domínio

O ML-Powered Discovery é uma das capacidades da plataforma CSURFACE — uma plataforma de Continuous Exposure Management. Numa plataforma integrada, ela reúne descoberta contínua da superfície externa, análise da cadeia digital de fornecedores, validação de exploitabilidade, inteligência de ameaças com priorização dinâmica e monitoramento de credenciais vazadas. Opera de forma inteiramente externa — sem agente e sem instalação —, com integrações opcionais de nuvem, WAF e CIEM para organizações que necessitam de maior profundidade analítica.

Receba a análise preliminar
Informe o domínio da sua empresa e receba, sem custo, um retrato dos ativos expostos descobertos pela plataforma.

Use a calculadora de risco
Estime a perda anual esperada (ALE) e o VaR do seu setor, com metodologia FAIR calibrada por benchmark de mercado.

Leia o próximo whitepaper
Cadeia Digital de Fornecedores — o caso Polyfill.io e como mapear dependências em três níveis.

Veja a sua superfície real — descoberta com o domínio raiz como única entrada

Receber análise preliminar gratuita