CSURFACE

WHITEPAPER · DIGITAL SUPPLY CHAIN

A ameaça silenciosa na sua cadeia digital

Dezenas de terceiros executam código na sua aplicação — e nenhum sinal quando um deles muda de dono, é comprometido ou expira. Antes do próximo Polyfill.io, mapeie a cadeia digital até três níveis de profundidade.

CAPACIDADE	PÚBLICO	EDIÇÃO
Cadeia Digital de Fornecedores	CISO · Risco · AppSec	2026

LEITURA	CLASSIFICAÇÃO	FONTE
16 páginas	Público	Plataforma CSURFACE

SUMÁRIO EXECUTIVO

Sua aplicação roda código que não é seu

A tese deste whitepaper, em uma página — o que executivos precisam saber antes do detalhe técnico.

SITES AFETADOS PELO POLYFILL.IO

100 mil+

domínios serviam o script malicioso sem saber

VULNERABILIDADES VINDAS DE DEPENDÊNCIAS

80%

em apps web modernas, e não do código próprio

PROFUNDIDADE DO MAPEAMENTO CSURFACE

3 níveis

da dependência direta ao subfornecedor do subfornecedor

Em junho de 2024, o domínio **polyfill.io** — utilizado por mais de 100 mil sites para distribuir scripts JavaScript — passou a injetar código malicioso após a mudança de titularidade. A maior parte das organizações afetadas desconhecia essa dependência. Não havia vínculo contratual direto: o Polyfill.io era subfornecedor de um subfornecedor, integrado ao código anos antes por equipes que já não estavam na organização.

O caso não é uma exceção. Aplicações modernas executam, em tempo real, código que pertence a dezenas de terceiros — **CDNs, scripts de analytics, APIs SaaS, bibliotecas com dependências transitivas**. Cada um desses elementos é uma porta. E a maior parte delas não aparece em nenhum inventário de fornecedores.

Este whitepaper analisa o caso Polyfill.io como exemplo arquetípico, percorre **outros incidentes públicos** detectáveis externamente (MageCart na British Airways, Ticketmaster via Inbenta, Sea Turtle, subdomain takeover), constrói **dois cenários críticos** — tomada de cookie de sessão via subdomain takeover e *second-grade takeover* de domínio expirado — e apresenta a abordagem da CSURFACE: o mapeamento técnico e contínuo da cadeia digital até **três níveis de profundidade**, com diagramas práticos em web e DNS e leituras dedicadas a gestor, engenheiro e analista.

A tese. Toda aplicação executa código de terceiros. Cada biblioteca, cada CDN e cada API integrada representa uma dependência herdada — sujeita a mudança de titularidade, comprometimento ou expiração sem notificação. O que não é mapeado de forma contínua não pode ser gerido nem defendido.

O que este whitepaper cobre

- O caso Polyfill.io e três incidentes públicos do mesmo padrão.
- As frentes técnicas — scripts, DNS, cabeçalhos e cookies.
- Dois cenários críticos: cookie + subdomain takeover; second-grade takeover.
- O mapeamento da CSURFACE em três níveis e a leitura por perfil.

O CASO POLYFILL.IO · PARTE 01

Um domínio mudou de dono — e 100 mil sites não perceberam

A anatomia de um incidente público de cadeia digital de fornecedores, do alerta ignorado ao código malicioso.

Whitepaper 2026
CSURFACE

O que aconteceu

O **Polyfill.io** era uma CDN open-source que distribuía "polyfills" — fragmentos de JavaScript destinados a prover funcionalidades modernas em navegadores mais antigos. O serviço era gratuito e obteve ampla adoção na comunidade de desenvolvimento web.

No início de 2024, o domínio foi adquirido por um novo operador. O criador original do projeto, Andrew Betts, **alertou publicamente** que o domínio havia trocado de mãos e não era mais confiável. O alerta passou despercebido — porque não havia monitoramento.

Em junho de 2024, scripts maliciosos passaram a ser servidos pelo domínio: rastreamento, redirecionamentos para sites de apostas e potencial roubo de credenciais. Cloudflare e Google reagiram bloqueando o domínio em seus serviços — mas o estrago já se acumulava havia semanas.

Por que o impacto foi tão amplo

1. **A dependência era desconhecida.** Em muitos sites o script havia sido adicionado anos antes, por alguém que já não estava na empresa. Era uma dependência invisível.
2. **A propriedade não era monitorada.** Não havia processo que acompanhasse mudanças de dono de fornecedores transitivos — exatamente o evento que disparou o ataque.
3. **CSP permissiva.** A maioria dos sites operava sem uma Content-Security-Policy restritiva capaz de barrar a execução de um script alterado.
4. **SCA não cobria HTML/JS público.** As ferramentas de análise de composição olhavam dependências de gerenciadores de pacote, não scripts carregados em tempo de execução pelo navegador.

O sinal que faltou. O criador do projeto comunicou publicamente que o domínio havia mudado de titularidade. O sinal de alerta estava disponível. A lacuna foi a ausência de um mecanismo capaz de monitorar mudanças de propriedade em fornecedores transitivos e encaminhar esse aviso às equipes de segurança das organizações consumidoras.

O padrão se repete. O Polyfill.io não é um caso isolado: é a manifestação de um problema estrutural. Toda dependência transitiva integrada sem monitoramento contínuo representa um vetor equivalente — sujeito à mesma cadeia de eventos quando o controle de sua titularidade muda de mãos.

CÓDIGO QUE NÃO É SEU · PARTE 02

A cadeia digital tem seis frentes — e quase nenhuma é mapeada

O problema geral por trás do caso Polyfill.io: do que é feita a dependência de terceiros em uma aplicação moderna.

87%
das aplicações web modernas operam com 50 ou mais dependências diretas

80%
das vulnerabilidades de uma app web vêm de dependências, não do código próprio

94 dias
é o tempo médio até descobrir credenciais comprometidas na cadeia de fornecedores

Do que se compõe a dependência

Aplicações modernas executam, em tempo real, código que pertence a dezenas de terceiros — e referenciam, no DNS, dezenas de outros domínios externos. Esse risco se distribui por **seis frentes técnicas** que uma plataforma de ASM detecta a partir do perímetro externo, sem agente nem instrumentação interna.

Cada frente segue um padrão próprio de adoção e de falha. Tratá-las com um único controle — questionário, SCA ou CSP isolada — é o que produz a invisibilidade que o Polyfill.io tornou pública.

O custo da invisibilidade. Ataques que exploram dispositivos de borda e VPNs gerenciados por terceiros cresceram cerca de oito vezes em relação ao ano anterior. Aproximadamente **30% dos breaches de 2025** envolveram um terceiro — e o tempo médio até a descoberta de credenciais comprometidas na cadeia de fornecedores é de 94 dias.

Fontes: Snyk State of Open Source 2024; OWASP; Verizon DBIR 2025; IBM Cost of a Data Breach 2025 — relatórios públicos.

As seis categorias de risco da cadeia digital

CRÍTICO **1 · JavaScript de terceiros no navegador**
Gerenciadores de tag, scripts de analytics, A/B testing, polyfills, pixels e widgets — qualquer código executado no browser do cliente. Categoria do Polyfill.io e da família MageCart.

CRÍTICO **2 · Relacionamentos de confiança em DNS**
Registros SPF (e seus includes), MX e NS externos, CNAMEs apontando para domínios de terceiros, registros DKIM — a cadeia de autoridade do seu domínio principal.

ATENÇÃO **3 · Subdomínios e recursos de nuvem referenciados**
CNAMEs apontando para serviços de nuvem (AWS S3, Azure App Service, Heroku, GitHub Pages, Fastly) — superfície clássica de subdomain takeover quando o recurso de origem é desalocado.

ATENÇÃO **4 · APIs e endpoints chamados em runtime**
APIs SaaS, webhooks, pixels de rastreamento, endpoints de pagamento, integrações de e-mail transacional — toda chamada externa que a aplicação executa em tempo real.

ATENÇÃO **5 · Cabeçalhos e proteções HTTP**
CSP, SRI, CORS, HSTS, flags de cookie (Secure, HttpOnly, SameSite) — a postura técnica que decide o desfecho quando um dos terceiros acima é comprometido.

CRÍTICO **6 · Domínios em estado degradado**
Expiração próxima, mudança recente de WHOIS, transferência de operador, certificado em renovação atípica — sinais antecipados de takeover ou second-grade na cadeia.

OUTROS CASOS REAIS · PARTE 03 · SCRIPTS E CDN

O Polyfill.io não foi o primeiro

Três incidentes públicos anteriores que seguiram o mesmo padrão — um terceiro embutido na cadeia digital, comprometido sem aviso à organização consumidora.

O padrão por trás dos casos. Em ambos os incidentes a seguir, o ataque entrou por um componente que a organização-alvo havia integrado anos antes, sem mecanismo posterior de monitoramento. O vetor difere — script direto na página de pagamento ou comprometimento de um fornecedor inteiro de widget —, mas a estrutura é a mesma, e a detecção externa é equivalente: a renderização headless da página identifica qualquer mudança no conteúdo entregue pelo terceiro.

British Airways · MageCart (2018)

Entre 21 de agosto e 5 de setembro de 2018, atacantes injetaram **22 linhas de JavaScript** na página de pagamento do site e do aplicativo da British Airways. O script capturava número de cartão, nome, endereço e CVV em tempo real e os enviava a um servidor controlado por terceiros. A injeção partiu da cadeia digital: um componente JavaScript de fornecedor já integrado ao site foi modificado para incluir o skimmer, sem alteração visível à equipe interna.

O ataque durou aproximadamente **15 dias** antes de ser detectado. Cerca de **380.000 transações** foram comprometidas.

Impacto. Multa de **£20 milhões** pelo ICO sob GDPR (2020) — inicialmente proposta em £183 milhões. Compensações cíveis a clientes, dano reputacional duradouro. O regulador apontou ausência de monitoramento técnico do JavaScript de terceiros como falha central da empresa.

Ticketmaster · via Inbenta (2018)

Em **junho de 2018**, a Ticketmaster divulgou que páginas de pagamento de seus sites estavam servindo um script malicioso havia aproximadamente nove meses. O script não estava embutido diretamente no código da Ticketmaster: era servido pelo widget de chat de atendimento da **Inbenta**, fornecedor integrado às páginas de pagamento.

A Inbenta confirmou comprometimento de sua infraestrutura. O JavaScript que ela hospedava — carregado em tempo real pelo navegador na origem legítima do fornecedor — foi alterado para incluir um skimmer. Aproximadamente **40.000 clientes** tiveram dados expostos.

Impacto. Multa de **£1,25 milhão** pelo ICO. Vetor distinto do caso BA: o que foi comprometido foi um **fornecedor inteiro** de aplicação, não o código da Ticketmaster. O JavaScript carregado pelo navegador continuava vindo da origem legítima do fornecedor — com toda a confiança de cadeia herdada.

Como a CSURFACE detecta esta categoria

A categoria de scripts e CDN é a mais visível externamente — e a mais bem coberta pela **renderização headless**. A plataforma carrega cada página da organização como um navegador real, registra todo JavaScript de origem externa executado, calcula o hash de cada arquivo recebido e o compara com a baseline.

Para cada script de terceiro identificado, a CSURFACE mantém: a origem (domínio e CDN), o WHOIS atual, o hash do conteúdo entregue e o histórico de mudanças. Qualquer alteração — domínio que troca de dono, hash que muda, CDN que redireciona — vira alerta em até **24 horas**.

Resultado. Os dois incidentes desta página seriam detectados antes do impacto material — o caso BA, pela detecção da injeção no JavaScript da página de pagamento; o Ticketmaster/Inbenta, pela mudança de hash no script carregado da origem do fornecedor.

OUTROS CASOS REAIS · PARTE 03 · DNS, MX E DOMÍNIOS

A cadeia digital também vive no DNS

Subdomínios apontando para recursos abandonados, provedores de DNS comprometidos, registros órfãos — uma classe de risco que não aparece em nenhum repositório de código.

Onde mora o risco no DNS. Aplicações modernas dependem de dezenas de nomes — subdomínios próprios, registros que apontam para serviços de nuvem, provedores externos de DNS e e-mail, includes de SPF. Cada um desses nomes é, em si, um nó da cadeia digital. Quando o controle de um deles é perdido — porque o recurso foi desalocado, o domínio expirou ou o provedor foi comprometido —, a confiança que apontava para ele continua válida, mas serve agora a quem assumir o controle.

Subdomain takeover via CNAME órfão

O padrão mais comum: um subdomínio da organização — por exemplo, **blog.empresa.com.br** — aponta, via registro CNAME, para um serviço de nuvem (Heroku, AWS S3, GitHub Pages, Azure App Service). O serviço foi desalocado em algum momento, mas o CNAME permaneceu. Qualquer pessoa pode então recriar o recurso de nuvem com o mesmo nome, e o subdomínio passa a servir o conteúdo dela — sob o nome de confiança da organização.

Documentado em centenas de relatos públicos no HackerOne, com casos de Microsoft, Uber, Shopify, Starbucks e múltiplas organizações de grande porte. Recursos abandonados em **Azure, AWS, Heroku, GitHub Pages e Fastly** são os mais frequentemente afetados.

Impacto. Phishing autenticado sob domínio real, distribuição de malware sob HTTPS válido, roubo de cookies em domínios irmãos (ver cenário hipotético, página 8). Detectado tipicamente apenas após exploração por pesquisadores ou atacantes.

Sea Turtle · sequestro de DNS upstream (2017-2019)

Campanha de Estado-nação documentada pela Cisco Talos. Atacantes comprometeram **provedores de DNS** em pelo menos 13 países — sobretudo no Oriente Médio e Norte da África — e modificaram registros NS e A de organizações-alvo: governos, empresas de energia, agências de inteligência. Com o DNS sequestrado, redirecionaram o tráfego para infraestrutura controlada por eles e emitiram certificados TLS válidos sob os nomes das vítimas, permitindo a captura de credenciais em sessões aparentemente legítimas.

Mais de **40 organizações** em 13 países foram identificadas como alvo direto.

Impacto. Captura silenciosa de credenciais e tráfego de organizações estratégicas; comprometimento de cadeias inteiras de e-mail oficial; uso de certificados válidos para evitar detecção por TLS pinning ou inspeção manual.

MX e SPF apontando para domínios órfãos

Variação menos visível, mas comum: registros **MX** ou includes de **SPF** da organização — ou de fornecedores integrados — apontam para domínios de terceiros que foram desativados ou expiraram. O registro continua publicado e válido. Se o domínio for re-registrado por um atacante, ele passa a ser uma origem autorizada para receber e-mails (MX) ou para enviar e-mails autenticados em nome da organização (SPF include).

O caso bancário detalhado na **página 9** é a manifestação mais grave desse padrão — um SPF include apontando para domínio de fornecedor de e-mail marketing expirado.

Impacto. Recepção de e-mail destinado ao subdomínio órfão (recuperação de senha, faturas, comunicações de fornecedor); ou envio de phishing massivo autenticado por SPF como se fosse a organização legítima — abordado em detalhe na próxima sessão.

OUTROS CASOS REAIS · PARTE 03 · HEADERS E PROTEÇÕES

Não basta o que a aplicação carrega — importa o que ela permite

Quatro configurações de cabeçalho e cookie cuja ausência ou permissividade determina se o navegador resistirá ou amplificará um ataque de cadeia.

Whitepaper 2026
CSURFACE

Por que esta seção existe. As três páginas anteriores trataram do que está na cadeia digital — scripts, dependências, registros DNS. Esta página trata das proteções do navegador que decidem o desfecho quando um desses elementos é comprometido. Em quase todos os casos públicos, uma proteção bem configurada teria reduzido significativamente o impacto ou bloqueado a exploração.

Content-Security-Policy permissiva ou ausente

A CSP define, no cabeçalho HTTP, quais origens podem carregar scripts, estilos e conexões. Uma política restritiva barra a execução de scripts de origens não autorizadas; uma permissiva (com wildcards ou `unsafe-inline`) ou ausente deixa o navegador aceitar qualquer script.

A CSP protege contra **injeção de origens novas** — XSS, ou um fornecedor servindo de uma origem inédita. **Não** protege, contudo, quando a origem já autorizada é, ela própria, comprometida (caso Polyfill.io). Para esse cenário, a defesa direta é o **SRI**, no bloco ao lado.

Impacto. Sem CSP restritiva, qualquer script de qualquer origem é executado. Um único componente comprometido na cadeia digital obtém controle total da página — leitura de formulários, exfiltração de cookies não-HttpOnly, redirecionamento.

CORS com wildcard ou origem refletida

O cabeçalho `Access-Control-Allow-Origin` determina quais origens podem ler respostas de uma API autenticada. Configurado com `*` ou refletindo dinamicamente a origem da requisição (sem validação), permite que qualquer site externo execute requisições autenticadas em nome do usuário logado — desde que o navegador envie cookies — e leia o resultado.

Esse padrão amplifica ataques de cadeia: um script comprometido em qualquer origem pode ler dados sensíveis da API da organização-alvo, mesmo quando hospedado em outro domínio.

Impacto. Vazamento de dados autenticados — saldos, históricos, perfis — para qualquer origem que execute código no navegador do usuário, incluindo origens da cadeia digital comprometidas.

Subresource Integrity (SRI) ausente

SRI é um atributo HTML que carrega, junto à tag `<script src="...">`, um hash criptográfico do conteúdo esperado. O navegador calcula o hash do arquivo recebido e o compara antes de executar. Se o conteúdo do servidor de origem mudou — porque a CDN foi alterada, comprometida ou substituída —, o navegador recusa a execução.

Sem SRI, o navegador aceita qualquer conteúdo que o servidor da CDN devolver. Uma swap como a do Polyfill.io passa silenciosamente.

Impacto. A alteração de um arquivo na CDN — propositadamente ou por comprometimento do fornecedor — executa sem qualquer sinal de aviso. SRI é a defesa criptográfica direta contra a categoria de risco do Polyfill.io.

Cookies sem flags de proteção

Cookies de sessão devem ser configurados com três flags: **Secure** (somente HTTPS), **HttpOnly** (não acessível via JavaScript) e **SameSite** (Lax ou Strict — restringe envio em requisições entre sites). A ausência de qualquer uma delas amplia o impacto de um comprometimento na cadeia digital.

HttpOnly, em particular, é a defesa crítica contra captura via JavaScript injetado — um vetor comum em todos os casos da página 5. Sua ausência transforma um XSS ou um script comprometido em tomada de conta direta.

Impacto. Sem HttpOnly, qualquer script da cadeia digital — legítimo ou comprometido — pode ler o cookie de sessão e enviá-lo a um endpoint controlado pelo atacante. É o vetor central do cenário hipotético da próxima página.

CENÁRIOS CRÍTICOS · PARTE 04 · CENÁRIO 01

Subdomain takeover + cookie emitido para o parent domain

Como um subdomínio esquecido apontando para um recurso de nuvem desalocado se transforma em tomada de conta em escala — sem alerta, sem MFA, sem rastro fácil.

Whitepaper 2026
CSURFACE

O cenário. Uma instituição financeira opera **app.banco.com.br** como aplicação crítica, com autenticação e MFA. Para suportar single sign-on entre serviços internos, o **cookie de sessão é emitido para o parent domain** — `Domain=.banco.com.br`. A organização opera dezenas de subdomínios; um deles — uma página promocional de campanha encerrada em 2022 — aponta, via CNAME, para um bucket de nuvem que foi desalocado. O registro DNS permaneceu publicado.

A cadeia de eventos do ataque

1. **Reconhecimento.** O atacante enumera subdomínios públicos de `banco.com.br` e identifica `promo2022.banco.com.br` apontando, via CNAME, para um bucket de nuvem cujo nome não está registrado. O subdomínio é elegível a takeover.
2. **Tomada do recurso.** O atacante registra o bucket com o mesmo nome no provedor de nuvem. O CNAME existente passa a resolver para infraestrutura controlada por ele. O subdomínio é servido sob HTTPS válido — o provedor emite certificado para o nome solicitado.
3. **Publicação do payload.** O atacante hospeda no bucket uma página HTML simples com um script de captura — leitura de `document.cookie` e envio ao endpoint do atacante via `fetch()`. Como a vítima visitará um subdomínio de `banco.com.br`, o navegador anexará o cookie emitido para `.banco.com.br`.
4. **Atração da vítima.** O link `promo2022.banco.com.br` ainda aparece em e-mails de marketing antigos, materiais arquivados, redirects internos não revogados e em respostas indexadas em mecanismos de busca. Basta uma fração das vítimas clicar para o ataque ter escala material.
5. **Captura e abuso.** O navegador da vítima — já autenticado em `app.banco.com.br` em outra aba — envia o cookie de sessão ao subdomínio comprometido. Se o cookie não tem **HttpOnly**, o JavaScript do atacante o lê e o exfiltra. O atacante autentica-se em `app.banco.com.br` usando o cookie capturado — **após o MFA, porque a sessão já está estabelecida**.

Por que este cenário é particularmente grave. O atacante opera *depois* do MFA — a sessão capturada já é autenticada. A requisição parte do IP da vítima ou de IP similar, o que dificulta a detecção por SIEM. O subdomínio comprometido tem HTTPS válido e nome real da organização. E o vetor é silencioso: nenhum log da aplicação principal mostra a captura — ela ocorre em um subdomínio fora do monitoramento.

As três condições simultâneas

O cenário só funciona quando três condições coexistem na organização:

1. Um subdomínio órfão apontando para recurso de nuvem desalocado — disponível para takeover.

2. Cookie de sessão emitido para o parent domain — anexado a todos os subdomínios.

3. Cookie sem flag HttpOnly — legível por JavaScript no navegador.

Cada condição, isoladamente, é uma decisão técnica defensável em algum contexto. A composição das três é a vulnerabilidade — e nenhuma análise de aplicação isolada a vê.

Como a CSURFACE detecta. A descoberta contínua mapeia todos os subdomínios públicos da organização; a inspeção identifica CNAMEs apontando para recursos desalocados (subdomain takeover); a análise headless registra o escopo e flags dos cookies da aplicação principal. As três condições viram um único alerta crítico, antes do atacante chegar lá primeiro.

CENÁRIOS CRÍTICOS · PARTE 04 · CENÁRIO 02

Second-grade takeover · quando o domínio do fornecedor expira

O takeover de primeiro grau atinge um subdomínio próprio. O de segundo grau atinge um domínio inteiro da cadeia — geralmente de um fornecedor — que expirou e foi re-registrado. Toda confiança herdada passa, sem alarme, ao novo dono.

Whitepaper 2026
CSURFACE

O conceito. Um domínio de terceiro — fornecedor de e-mail marketing, parceiro de campanha, CDN, integrador encerrado — expira por falta de renovação, encerramento de operação, divestiture em M&A ou simples esquecimento. A organização consumidora, porém, mantém registros DNS, includes de SPF, CNAMEs e referências de scripts apontando para esse domínio. O domínio é re-registrado por um atacante. Toda a confiança herdada — autenticação SPF, execução de script, recebimento de e-mail — passa instantaneamente ao novo controlador, sem qualquer alarme técnico do lado da organização.

O caso · banco com SPF autorizando domínio de fornecedor já expirado

Um banco contratou, em 2018, um fornecedor de e-mail marketing — `envio-camp.com.br` — para disparar comunicações transacionais e promocionais. Para que essas mensagens passassem pelos filtros anti-spam, o banco incluiu o domínio do fornecedor em seu registro SPF:

```
v=spf1 include:_spf.envio-camp.com.br include:_spf.outras.com.br ~all
```

Anos depois, o fornecedor encerrou operação. O include, contudo, permaneceu no SPF do banco — o domínio não constava em nenhum inventário de fornecedores ativos, e o conteúdo do registro não era revisado.

Nos **primeiros dias de operação** da CSURFACE no banco, o mapeamento da cadeia de domínios referenciados na configuração externa identificou que `envio-camp.com.br` **já estava expirado** — o domínio autorizado pelo include do SPF encontrava-se, naquele momento, livre para registro público por qualquer parte. O alerta foi escalado à equipe de segurança, que removeu o include do SPF antes que um terceiro re-registrasse o domínio. **O vetor foi neutralizado antes de poder ser explorado.**

O que estaria em risco sem a detecção. Com o include ativo e o domínio re-registrado por terceiro, o atacante publicaria `_spf.envio-camp.com.br` autorizando os próprios IPs e enviaria e-mails autenticados por SPF como se fosse o banco. Filtros anti-spam aceitariam — SPF passa, IP autorizado. Centenas de milhares de e-mails de phishing autenticados poderiam ser entregues aos clientes do banco; roubo de credenciais em escala; exposição regulatória junto ao BACEN e à ANPD (LGPD). O sinal — a expiração do domínio na cadeia — esteve público por mais de um ano. Foi exatamente esse sinal que a plataforma capturou.

Outras variações do mesmo padrão

CNAME para domínio expirado. Um subdomínio aponta para `cdn-do-fornecedor.com`, fornecedor que encerrou em 2021. O domínio expira; o atacante registra e passa a servir scripts ou páginas sob o nome da organização-cliente.

MX para domínio expirado. Um subdomínio (`fatura.empresa.com.br`) tem registro MX apontando para servidor de fornecedor extinto. O atacante registra o domínio e recebe e-mails endereçados a esse subdomínio — incluindo recuperação de senha, faturas e comunicações de fornecedores.

Script src para domínio expirado. Páginas legadas carregam, via `<script src>`, um arquivo de um domínio que não existe mais. O atacante registra o domínio e executa código sob o nome de confiança da página hospedeira — vetor equivalente ao do Polyfill.io.

DKIM órfão. Um registro DKIM apontando para chave pública em domínio extinto pode ser sequestrado, permitindo ao atacante assinar e-mails como se fosse a organização legítima.

Como a CSURFACE detecta. A plataforma monitora continuamente todos os domínios referenciados na configuração externa da organização — incluindo includes de SPF, MX, CNAMEs, NS e referências em scripts. Para cada um, observa estado de registro, data de expiração e mudanças de propriedade no WHOIS. A expiração iminente — ou consumada — de um domínio na cadeia é alerta crítico, levado às equipes antes de o re-registro ser possível.

POR QUE O TRADICIONAL FALHA · PARTE 03

O questionário não vê código

Por que as abordagens tradicionais de TPRM e SCA cobrem o contrato — e deixam de fora o risco técnico real.

Três lacunas das abordagens tradicionais

Questionários de fornecedores não veem código. A gestão de risco de terceiros (TPRM) tradicional avalia fornecedores por meio de questionários autodeclarados. Isso atende a requisitos de conformidade, mas diz pouco sobre o risco real: não se preenche um questionário sobre cada uma das dezenas de dependências de npm de uma aplicação.

SAST e SCA tradicionais olham apenas o código próprio e as dependências de gerenciador de pacote. Não enxergam o JavaScript injetado em tempo de execução por um gerenciador de tag, não veem a CDN externa que serve um arquivo crítico e não acompanham mudanças de propriedade de domínio.

A CSP é uma defesa, não um diagnóstico. Uma Content-Security-Policy bem configurada barra scripts não listados. Mas a maioria dos sites começa com uma política permissiva e nunca a restringe — e a CSP, por si só, não revela quais scripts a aplicação realmente carrega.

A lacuna comum. Nenhuma das abordagens tradicionais foi concebida para inspecionar o que a aplicação executa em tempo real, tampouco para monitorar de forma contínua a postura e a titularidade dos fornecedores após a formalização dos contratos.

Onde cada abordagem para

O QUE PRECISA SER VISTO	TPRM / SCA TRADICIONAL	MAPEAMENTO CSURFACE
JavaScript carregado em runtime	Não cobre	**Renderização headless**
CDN externa de arquivo crítico	Não cobre	**Mapeada por inspeção**
Mudança de propriedade de domínio	Não cobre	**Alerta de WHOIS**
Dependências transitivas além do N1	Parcial	**Três níveis**
Postura externa real do fornecedor	Autodeclarada	**Verificada externamente**
Frequência da avaliação	Pontual / anual	**Contínua**

O resultado prático. A organização mantém um repositório de questionários preenchidos e um indicador formal de conformidade — enquanto as dependências técnicas de maior risco jamais foram inspecionadas e permanecem sem monitoramento após a formalização dos contratos.

MAPEAMENTO EM 3 NÍVEIS · PARTE 04

Da dependência direta ao subfornecedor do subfornecedor

A abordagem da CSURFACE: três níveis de profundidade técnica, mapeados e monitorados continuamente.

A CADEIA DIGITAL, DESDOBRADA · TRÊS NÍVEIS DE PROFUNDIDADE TÉCNICA

1 · N1 · Dependências diretas
Para cada ativo descoberto, a plataforma identifica o JavaScript carregado em tempo de execução via análise headless, os manifestos de pacote em repositórios públicos, as APIs chamadas em runtime e os webhooks recebidos.

2 · N2 · Subfornecedores
Para cada fornecedor de Nível 1, a CSURFACE mapeia as dependências dele: quais CDNs usa, quais APIs chama e onde hospeda a infraestrutura. A dependência transitiva de uma biblioteca também é desdobrada aqui.

3 · N3 · Subfornecedor do subfornecedor
A profundidade máxima que os dados públicos permitem — o ponto em que estava o Polyfill.io: o operador do domínio, o IP e a CDN que de fato servem o código ao navegador do usuário.

NÍVEL 1 · DEPENDÊNCIA DIRETA

Sua aplicação
contrata o fornecedor de marketing

O contrato que a organização conhece e que aparece no inventário de fornecedores.

NÍVEL 2 · SUBFORNECEDOR

Fornecedor de marketing
embute o script de polyfill na página

A dependência herdada — adicionada por terceiros, sem contrato direto com a organização.

NÍVEL 3 · SUBFORNECEDOR DO SUBFORNECEDOR

polyfill.io
domínio operado por um terceiro · IP e CDN desconhecidos

O nó que mudou de dono e passou a servir código malicioso — invisível até a cadeia ser desdobrada.

Sinais monitorados continuamente · para cada nó da cadeia

CRÍTICO Mudanças de propriedade (WHOIS)
Alerta quando um domínio da cadeia troca de dono — o sinal exato que faltou no caso Polyfill.io.

ATENÇÃO Postura externa do fornecedor
Vulnerabilidades e configurações expostas no perímetro de cada nó da cadeia.

ATENÇÃO Mudanças de DNS
Alterações em registros NS, MX e A que indiquem redirecionamento de infraestrutura.

CRÍTICO Credenciais vazadas
Credenciais do fornecedor à venda ou expostas em fóruns e repositórios públicos.

ATENÇÃO Certificados
Renovações, troca de emissor e proximidade de expiração de cada certificado.

CRÍTICO Divulgações de incidente
Anúncios públicos de comprometimento do próprio fornecedor.

A análise headless executa a renderização completa da página, incluindo scripts dinâmicos; o monitoramento opera de forma contínua, sem agente instalado no ambiente do cliente.

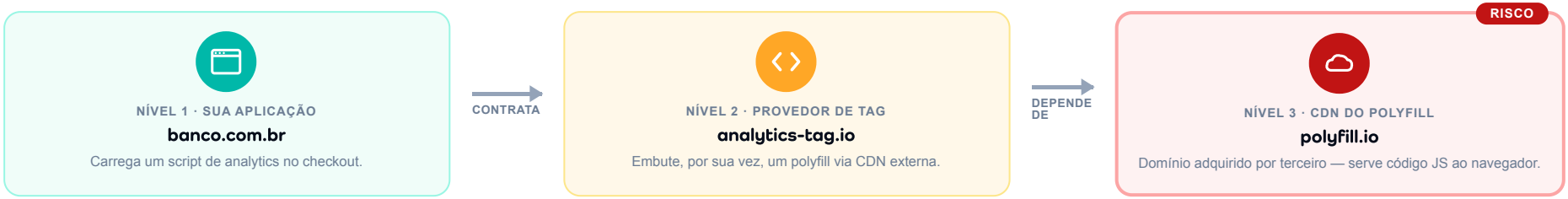
MAPEAMENTO EM 3 NÍVEIS · PARTE 05 · DIAGRAMAS

Dois diagramas práticos · web e DNS

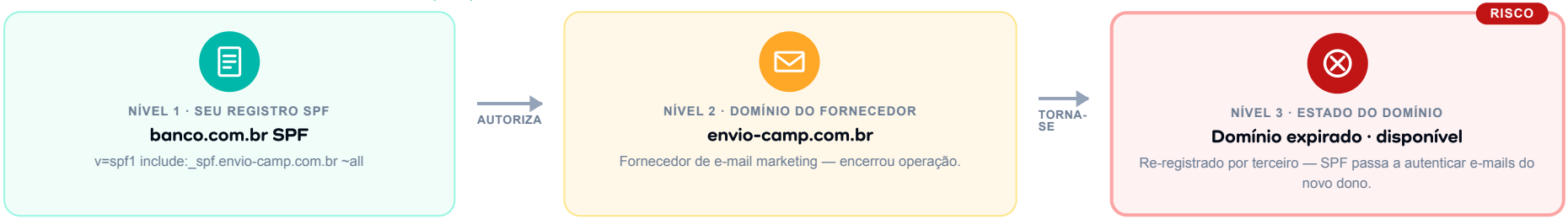
A mesma estrutura de três níveis aplicada a duas categorias distintas — código de página e registro de e-mail. Em ambas, o risco vive no terceiro nível.

O padrão é estrutural, não categórico. Em ambos os exemplos, a organização contrata um fornecedor de Nível 1, este fornecedor depende, por sua vez, de um Nível 2, e o risco real surge em um Nível 3 não mapeado pela organização — mas que decide o desfecho.

EXEMPLO 01 · CADEIA DE SCRIPTS NO NAVEGADOR



EXEMPLO 02 · CADEIA DE AUTORIDADE DO E-MAIL (SPF)



Onde a CSURFACE detecta este padrão. A descoberta contínua mapeia ambas as cadeias — JavaScript em runtime (renderização headless) e domínios em configuração externa (SPF includes, CNAME, MX, NS, scripts src). Para cada nó nos três níveis, a plataforma observa estado de registro, titularidade no WHOIS, mudanças de DNS e variações de conteúdo. O sinal — mudança de propriedade, expiração iminente, alteração de hash — chega à equipe antes da exploração.

LEITURA POR PERFIL · PARTE 06

A mesma cadeia digital, três cortes diferentes

Gestores, engenheiros e analistas precisam de cortes distintos do mesmo dado para decidir, configurar e responder a ameaças na cadeia digital de fornecedores.

Por que existem três cortes. O risco de cadeia digital atravessa três camadas organizacionais com horizontes diferentes — capital, configuração e operação. O **gestor** precisa do número agregado em reais para deliberar e prestar contas; o **engenheiro** precisa do detalhe técnico para corrigir; o **analista** precisa do contexto e dos indicadores para responder em tempo real. Sem essa segmentação, o mesmo relatório atende mal os três.

Para o gestor · CISO, gerente de risco

O que importa. Exposição financeira agregada, aderência ao apetite de risco aprovado, conformidade com normas aplicáveis (BACEN, LGPD, NIS2, PCI DSS) e métricas de cobertura — quantos fornecedores estão sob monitoramento, quantos alertas críticos estão abertos, quanto tempo levou da detecção à resolução.

O que recebe da CSURFACE. Painel executivo com inventário consolidado de fornecedores em três níveis, alertas críticos em aberto, comparação ao apetite, evidência auditável para o comitê. Relatórios periódicos que podem ser apresentados ao conselho sem tradução técnica adicional.

Como age. Aprova investimento de remediação com base no trade-off de redução de exposição. Comunica posição da organização ao conselho, ao regulador e ao auditor com dados verificáveis. Compara a postura interna à de pares do setor.

Para o engenheiro · AppSec, DevSecOps

O que importa. Detalhes técnicos completos do achado — qual script foi alterado, qual hash mudou, qual subdomínio aponta para qual recurso desalocado, qual SPF include referencia qual domínio expirado. O vetor de exploração, o contexto na arquitetura e o caminho de remediação.

O que recebe da CSURFACE. Alertas técnicos com contexto completo — domínio afetado, recurso de origem, evidência da mudança (hash antes/depois, WHOIS antes/depois), integração com pipelines de CI/CD e ticketing. Recomendação de correção concreta para cada categoria.

Como age. Remove a dependência problemática, configura CSP restritiva e SRI nos scripts críticos, atualiza registros SPF, retira CNAMEs órfãos, aplica flags `HttpOnly` e `SameSite` em cookies de sessão. Documenta a mudança no inventário técnico.

Para o analista · SOC, resposta a incidentes

O que importa. Contexto da ameaça em tempo real — indicadores de comprometimento, atividade observada nos componentes da cadeia, correlação com inteligência de ameaças, sinais de exploração ativa em organizações pares do setor.

O que recebe da CSURFACE. Alertas correlacionados com inteligência de ameaças e com a postura externa do fornecedor, indicação de exploração em andamento, contexto temporal (quando o sinal apareceu, quando mudou, quem mais foi afetado), enriquecimento de IOCs para investigação.

Como age. Investiga atividade anômala originada de componentes externos, conduz contenção quando o vetor é confirmado, comunica internamente, escala ao engenheiro para correção e ao gestor para deliberação. Mantém a trilha forense.

APLICAÇÃO E RESULTADOS · PARTE 05

Prevenindo o próximo Polyfill.io

Um caso de uso representativo e o que esperar nas primeiras semanas de operação.

INVENTÁRIO TRADICIONAL

1×

fornecedores conhecidos e declarados em contrato — CDN, analytics, A/B, chat, AdTech.

→

APÓS O MAPEAMENTO EM 3 NÍVEIS

49×

componentes na cadeia digital real — invisíveis até a cadeia ser desdobrada.

O QUE A CSURFACE OBSERVA · DADOS PRÓPRIOS DA PLATAFORMA

2,8×
fornecedores diretos (Nível 1) para cada ativo próprio em inventário

11×
expansão da cadeia somando subfornecedores (Nível 2)

49×
tamanho real da cadeia desdobrada até o Nível 3

Caso de uso · e-commerce de médio porte

Uma operação de e-commerce com 12 sites, três frontends (web, web mobile e B2B) e mais de 80 scripts JavaScript externos no DOM ativou o mapeamento da CSURFACE. Na primeira semana, a plataforma desdobrou a cadeia até o terceiro nível — **multiplicando em mais de 40× o número de fornecedores** que constava no inventário tradicional. Três alertas críticos foram emitidos:

CRÍTICO **Script do polyfill.io ainda ativo**
Um gerenciador de tag, em uma página antiga, ainda apontava para o domínio — nunca removido após o incidente público.

ATENÇÃO **Domínio de CDN de chat expirando em 11 dias**
Com risco de ser registrado por um terceiro e passar a servir código sob o nome de confiança.

CRÍTICO **Pixel de rastreamento com novo dono**
Fornecedor mudou de propriedade dois meses antes — alteração de WHOIS detectada pela plataforma.

Time-to-value

- **Dia 1** — onboarding; o crawl headless inicial é concluído em poucas horas.
- **Dia 3** — inventário completo de dependências nos três níveis.
- **Semana 1** — monitoramento contínuo ativo; primeiro alerta a cada mudança.
- **Mês 1+** — operação contínua, com painel de risco por fornecedor.

Quer descobrir o tamanho da sua cadeia digital — gratuitamente?

Em uma análise preliminar sem custo, a CSURFACE mapeia os três níveis de fornecedores para um dos seus ativos públicos e devolve o relatório técnico completo.

Mapear minha cadeia →

CONFORMIDADE · PARTE 06

O mesmo trabalho que protege e comprova

Como o mapeamento contínuo da cadeia digital atende a requisitos regulatórios sem esforço adicional.

Requisitos regulatórios atendidos

NORMA	REQUISITO	COMO O MAPEAMENTO CONTRIBUI
BACEN 4.557	Avaliação contínua de fornecedores críticos	**Monitoramento contínuo, não pontual**
ISO 27001	Relacionamento com fornecedores (Anexo A)	**Inventário técnico verificável**
NIST CSF	Supply Chain Risk Management	**Mapeamento em três níveis**
PCI DSS 4.0	Gestão de provedores de serviço (Req. 12.8)	**Lista de terceiros sempre atual**
EU NIS2	Gestão de risco de cadeia de suprimentos	**Evidência de avaliação contínua**

Aplicável a operações sujeitas a cada regulação; a NIS2 vale para organizações com operação na União Europeia.

Conformidade como subproduto. O mapeamento contínuo da cadeia digital não é um esforço paralelo ao de conformidade. O inventário técnico, verificável e sempre atualizado é, ao mesmo tempo, o controle de segurança e a evidência que o auditor pede — sem retrabalho.

Do questionário à evidência técnica

O modelo tradicional comprova conformidade com um repositório de questionários autodeclarados. O mapeamento da CSURFACE substitui esse modelo por um inventário técnico continuamente atualizado:

- Cada fornecedor identificado por inspeção, não por declaração.
- Cada mudança registrada com data e tipo de evento.
- Cada alerta crítico documentado da detecção à resolução.

O resultado é uma trilha de auditoria que descreve a cadeia efetivamente existente — e não a cadeia presumida com base em declarações autodeclaradas.

PRÓXIMOS PASSOS

Descubra o subfornecedor antes que ele descubra você

A análise da cadeia digital de fornecedores é uma das capacidades da plataforma CSURFACE — uma plataforma de Continuous Exposure Management. Em uma 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 e monitoramento de credenciais vazadas. 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.

Mapeie um dos seus sites
Em uma sessão técnica de 30 minutos, a CSURFACE executa o mapeamento da cadeia digital de um ativo de sua escolha nos três níveis de profundidade.

Use a calculadora de risco
Estime a perda anual esperada do seu setor com a calculadora de risco da CSURFACE, calibrada por benchmark de mercado.

Leia o whitepaper de ML Discovery
Descoberta contínua da superfície externa com Machine Learning — a base sobre a qual o mapeamento de fornecedores opera.

Veja a sua cadeia digital real — mapeada até três níveis de profundidade

Receber análise preliminar gratuita