

Proofpoint Collaboration Security Prime

Segurança de colaboração completa e contínua para a era da IA

Principais destaques

- Bloqueia a mais ampla variedade de ameaças com eficácia de 99,999%
- Contém o comprometimento de conta em minutos, independentemente da ameaça ter origem no e-mail, em outros vetores ou provir de um fornecedor comprometido
- Reduz os cliques em links maliciosos do mundo real em 40% no prazo de seis meses após a implantação
- Impede a impostura e desativa domínios parecidos antes que cheguem aos seus clientes
- Reduz o custo total de propriedade em 40% por meio da consolidação da plataforma

Esse conjunto de soluções faz parte da plataforma integrada Human-Centric Security da Proofpoint, protegendo pessoas e dados no espaço de trabalho agêntico.

Visão geral

A IA transformou o cenário para todos. Os atacantes estão usando essa tecnologia para lançar ataques mais inovadores e personalizados, com maior sofisticação e escala. Campanhas como as de comprometimento de e-mail corporativo (BEC, na sigla em inglês) aumentaram 27%, e o phishing gerado por IA agora produz uma taxa de cliques 4,5 vezes maior do que o phishing tradicional. Os usuários tornaram-se mais suscetíveis ao conteúdo gerado por IA, enquanto os defensores estão sobrecarregados com triagem de alertas e ferramentas fragmentadas.

As organizações precisam de uma abordagem fundamentalmente diferente, criada para a era agêntica, em que ferramentas e assistentes com inteligência artificial se integram à força de trabalho estendida em e-mail, mensagens e aplicativos em nuvem, expandindo a superfície de ataque que os atacantes já estão explorando.

Infelizmente, muitas organizações são forçadas a adotar uma abordagem de segurança fragmentada, baseada em produtos isolados. No entanto, isso cria lacunas adicionais em suas defesas, isola as equipes e aumenta a complexidade operacional.

Para se defenderem dos atuais ataques escalados por IA em vários canais e estágios, bem como proteger interações confiáveis — sejam entre pessoas, entre pessoas e assistentes de IA ou entre pessoas e aplicativos de nuvem — as organizações precisam de uma abordagem mais holística. O Proofpoint Collaboration Security Prime pode ajudar. O Proofpoint Prime unifica a detecção e a resposta a ameaças em todo o espaço de trabalho agêntico.

Ele ajuda você a:

- Detectar novas ameaças geradas por IA mais cedo, com maior visibilidade em toda a superfície de ataque.
- Bloquear com confiança, graças à precisão líder do setor e à baixa taxa de falsos positivos.
- Oferecer proteção contínua abrangendo pré-entrega, pós-entrega, navegador e cobertura de agentes.
- Proteger as comunicações empresariais onde quer que elas aconteçam, sejam em chats, aplicativos ou agentes.
- Conter o comprometimento de conta em minutos, e não em dias.

Detecte ameaças novas mais cedo, com mais visibilidade

Novos ataques gerados por IA estão se espalhando mais rápido do que as defesas tradicionais conseguem interceptá-los. Como resultado, estão contornando filtros tradicionais e alcançando pessoas por e-mail, plataformas de colaboração e aplicativos de nuvem.

O Proofpoint Collaboration Security Prime preenche essa lacuna com proteção contínua em todo o ciclo de vida da ameaça, desde a arquitetura de e-mail pré-entrega até pós-entrega, e desde o momento do clique até o login, em todos os canais onde as pessoas trabalham.

O Proofpoint Prime protege contra a mais ampla gama de ameaças, inclusive:

- Phishing avançado, inclusive phishing de credenciais e phishing de telefonema de retorno.
- BEC e falsificação da identidade do CEO
- Entrega de malware
- Ataques com códigos QR
- Ataque de telefonia (Telephone-Oriented Attack Delivery, TOAD)
- Bombardeio de e-mail
- Ransomware
- Sequestros de contas
- Abuso de serviços legítimos
- Ataques gerados por IA e técnicas de exploração de IA, como injeção de prompts

No cerne dessa proteção está o Proofpoint Nexus AI, o mecanismo de detecção mais avançado do setor. Treinado com um dos maiores conjuntos de dados do setor, o Proofpoint Nexus AI avalia mais de 1.000 atributos por mensagem. Ele combina cinco tipos de modelos — modelos de linguagem, gráficos de relacionamentos, autoaprendizagem, inteligência sobre ameaças e visão computacional — que trabalham em conjunto e aprendem continuamente com cada veredito.

O resultado é uma eficácia de detecção de 99,999% e a menor taxa de falsos positivos do setor, permitindo que ameaças reais sejam bloqueadas sem sobrecarregar as equipes com ruído.

Defendase contra o comprometimento de contas

O comprometimento de contas não se limita a e-mails de phishing. A IA está facilitando para os agentes maliciosos a expansão de ataques a credenciais muito além da caixa de entrada, seja gerando páginas de login convincentes e idênticas em cada detalhe ou contornando a autenticação por múltiplos fatores utilizando bombardeio automatizado de prompts.

Em um ambiente de trabalho orientado pela colaboração e auxiliado por agentes, é fundamental impedir essas ameaças em todas as etapas: antes, durante e depois do comprometimento.

O Proofpoint Collaboration Security Prime ajuda a prevenir o comprometimento de contas antes que ele aconteça. O SSO Password Guard do Proofpoint Prime detecta quando funcionários reutilizam suas senhas corporativas em sites não

corporativos, fechando um dos pontos de entrada mais comuns para ataques baseados em credenciais e estendendo a proteção além do e-mail para o próprio navegador.

Quando a prevenção não é suficiente, o Proofpoint Prime detecta o comprometimento de conta assim que este ocorre. O Proofpoint Prime correlaciona a identidade e os sinais pós-acesso no Microsoft 365, Google Workspace e Okta para identificar contas que apresentem sinais de comprometimento.

Assim que um comprometimento de conta é identificado, o Proofpoint Prime ajuda você a investigá-lo e a realizar a contenção em minutos, e não em dias, limitando o raio de impacto antes que um atacante possa se infiltrar mais no ambiente.

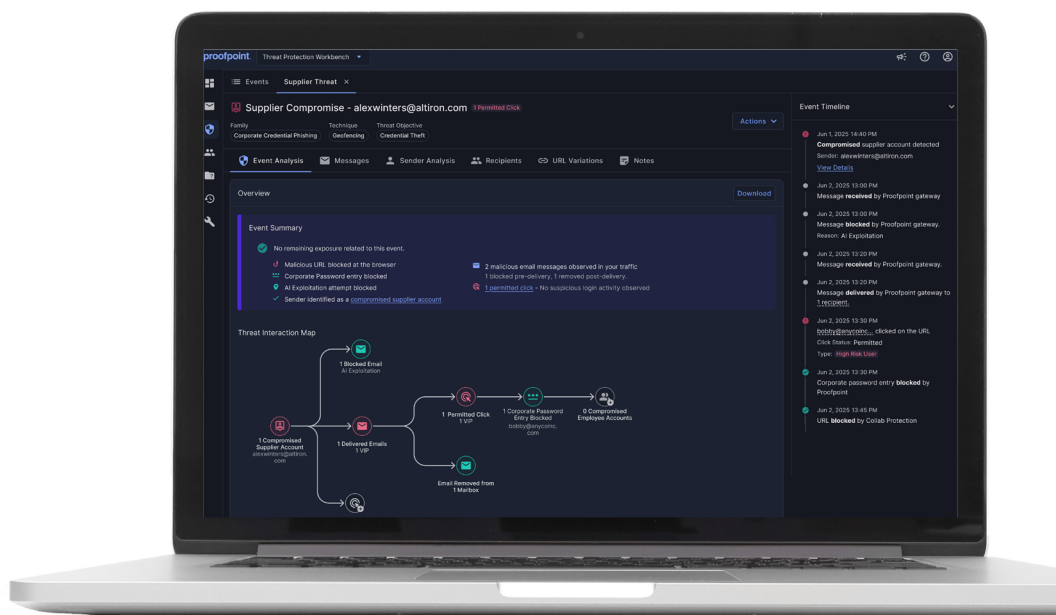


Figura 1. O Proofpoint Collaboration Security Prime bloqueia e correlaciona ameaças nos canais de e-mail, mensagens, colaboração, nuvem e fornecedores.

Os modelos do Proofpoint Nexus® AI são treinados com base em um dos maiores e mais diversificados conjuntos de dados de toda a cibersegurança.

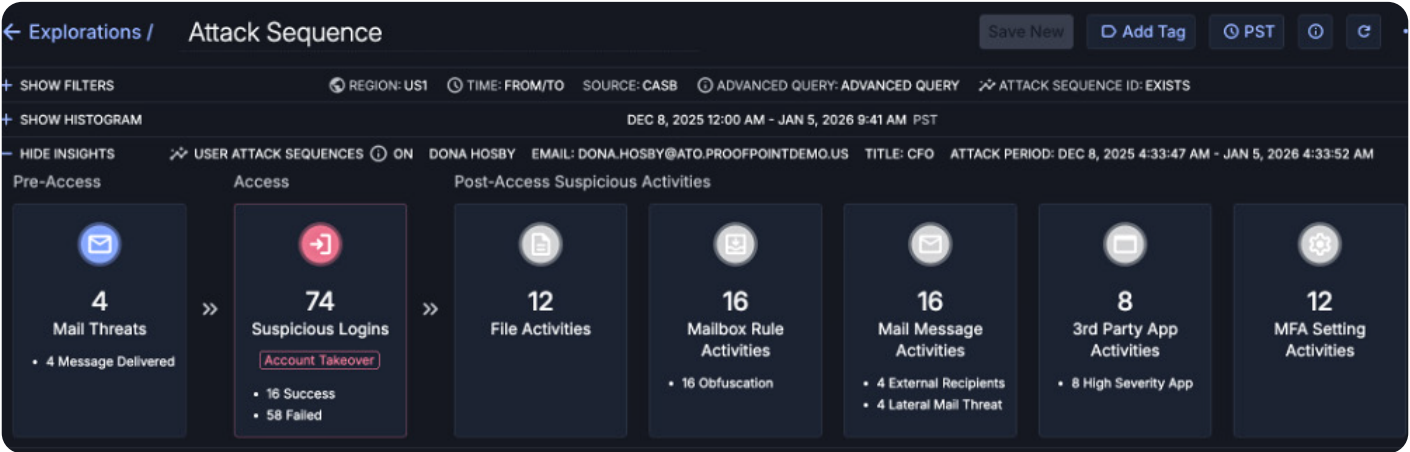


Figura 2. O Proofpoint Collaboration Security Prime oferece visibilidade sobre as sequências de ataque e automatiza a contenção.

Proteja suas comunicações empresariais confiáveis

Os atacantes costumam usar táticas de impostura para se inserir em comunicações comerciais confiáveis, seja por meio de falsificação de domínios direta, uso de domínios parecidos ou comprometimento de contas de fornecedores. Quando sua organização ou seus parceiros são alvo de falsificação de identidade ou são comprometidos, seus funcionários e clientes ficam em risco e sua marca pode sofrer sérios danos.

O Proofpoint Collaboration Security Prime pode ajudar a mitigar proativamente esses riscos de impostura. Ele oferece visibilidade total sobre todos os e-mails enviados através dos seus domínios confiáveis, inclusive os enviados por terceiros. Você tem acesso não só a ferramentas poderosas, mas também a consultores especializados que o orientam em cada etapa da implementação da autenticação de e-mail. Isso ajuda você a obter total conformidade com o DMARC e a evitar que atacantes falsifiquem seus domínios.

Nossa proteção vai além de e-mails gerados por usuários e inclui um ambiente seguro e dedicado para o encaminhamento de mensagens geradas por aplicativos, bem como e-mails enviados por provedores de SaaS de terceiros em seu nome.

Quando se trata de ameaças de fornecedores, o Proofpoint Prime protege seus funcionários de serem explorados por atacantes que utilizam contas de terceiros comprometidas. Ele identifica atividades suspeitas originadas em contas de fornecedores e aplica proteções adaptáveis, como indicadores de alerta e isolamento de URLs, para reduzir o risco sem interromper as comunicações empresariais legítimas.

O Proofpoint Prime também oferece capacidades avançadas de descoberta de domínios parecidos. Ele monitora dinamicamente a Internet em busca de domínios parecidos com o seu. Também fornece informações detalhadas sobre seus dados de registro, bem como possíveis usos indevidos.

Não paramos apenas na detecção. Podemos atuar em seu nome para derrubar domínios e URLs maliciosos, aproveitando nossos sólidos relacionamentos com instituições de registro, provedores de hospedagem e autoridades de domínios de nível superior (TLD). Nossos profissionais gerenciam todo o processo, permitindo que as suas equipes se concentrem nas operações essenciais da sua empresa.

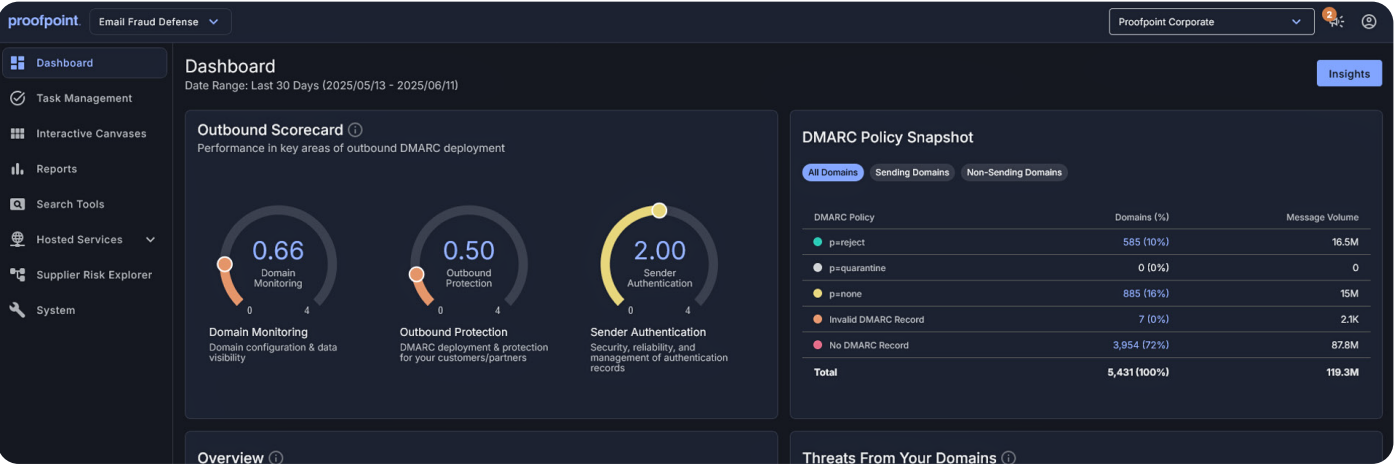


Figura 3. O Proofpoint Collaboration Security Prime oferece visibilidade sobre ameaças de impostura, como falsificação de domínios e registro de domínios parecidos maliciosos.

Reforce a resiliência humana com orientações baseadas no risco

À medida que o trabalho se torna mais colaborativo e dinâmico, as pessoas devem se tornar mais resilientes contra ataques cibernéticos. Isso exige ir além do treinamento orientado por conformidade e incluir o gerenciamento do risco humano — educação imediata que reflète a maneira como os usuários trabalham e os riscos reais que eles enfrentam.

O Proofpoint Collaboration Security Prime desenvolve a resiliência humana de forma sistemática, não por meio de treinamentos pontuais, mas por meio de um ciclo contínuo atrelado a riscos reais.

Tudo começa com direcionamento. O Human Resilience Workbench reúne sinais de comportamento e risco de toda a plataforma, identificando automaticamente usuários de alto risco, novos contratados e clicadores contumazes para que as equipes de segurança possam concentrar sua atenção no que é mais importante.

A partir daí, o Proofpoint Prime reforça comportamentos mais seguros no momento em que o risco é maior. Utilizando a tecnologia ThreatFlip com inteligência artificial, ele converte ameaças reais e ativas em simulações instantâneas com um único clique, mostrando aos funcionários exatamente como os ataques se apresentam assim que eles encontram um, e não semanas depois em um módulo de treinamento genérico.

Finalmente, o Proofpoint Prime comprova o impacto. Pontuações de risco e índices comparativos oferecem aos administradores uma visão clara de onde o comportamento está melhorando e onde ainda existem lacunas. Organizações que utilizam essa abordagem observam uma redução de 40% nos cliques em links maliciosos do mundo real em um período de seis meses, o que demonstra que é a resiliência, e não apenas a conscientização, que promove mudanças duradouras.

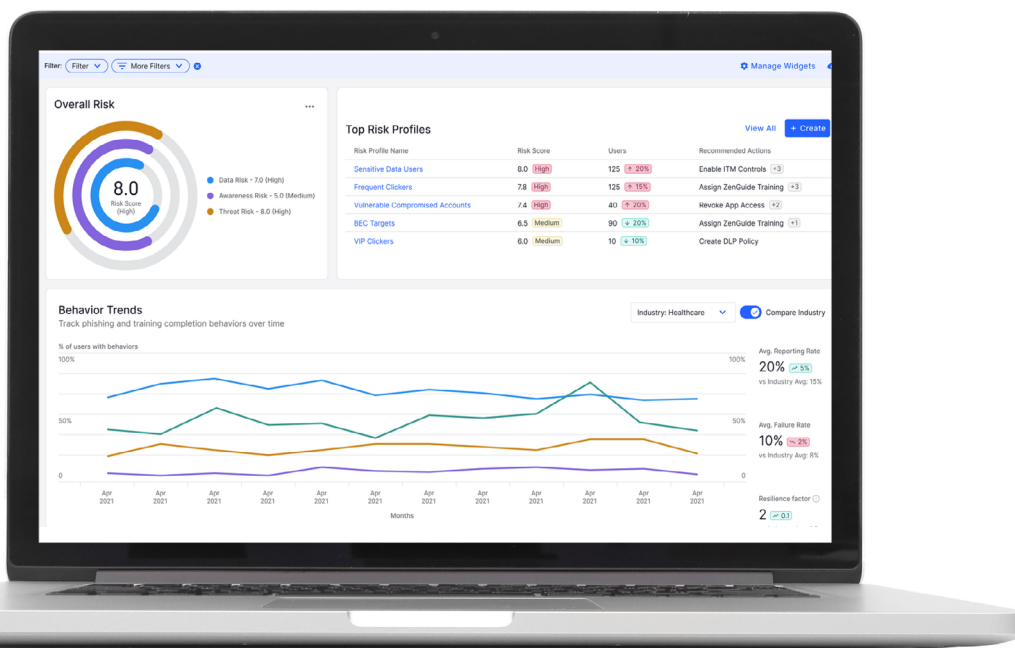


Figura 4. O Proofpoint Collaboration Security Prime oferece visibilidade sobre o comportamento real dos usuários, o que viabiliza um aprendizado direcionado e baseado no risco.

Simplifique as operações de segurança

À medida que as ameaças se expandem além do e-mail para ferramentas de colaboração, plataformas de nuvem e ecossistemas de fornecedores, as equipes de segurança são pressionadas a fazer mais com menos. Nesse ambiente, soluções pontuais desconectadas não facilitam as coisas. Elas não só aumentam a complexidade, como também aumentam os tempos de resposta e elevam os custos operacionais. Tudo isso torna mais difícil reduzir o risco em escala.

O Proofpoint Collaboration Security Prime simplifica as operações de segurança ao unificar detecção e investigação de ameaças, além de automatizar fluxos de trabalho e resposta. O Threat Protection Workbench usa integrações nativas para reunir insights de detecção e análise forense de ataques de e-mail, mensagens, plataformas de colaboração, contas de nuvem e ecossistemas de fornecedores. Isso permite que as equipes investiguem incidentes e executem ações decisivas — tudo a partir de um único espaço de trabalho unificado para máxima eficiência.

O Proofpoint Prime também ajuda as equipes a priorizar de forma eficaz. O Threat Interaction Map correlaciona ameaças e eventos de segurança em pontos de controle — e fornece um mapa visual dos caminhos de ataque. Isso permite que os analistas identifiquem rapidamente os incidentes mais críticos. Paralelamente a isso, ele inspeciona automaticamente mensagens denunciadas por usuários, corrige conteúdo malicioso e fornece feedback aos usuários. Como resultado, o esforço manual é reduzido enquanto o comportamento seguro do usuário é reforçado.

O resultado é uma resposta mais rápida e menor complexidade operacional. E a sua equipe de segurança pode fazer mais com menos, sem sacrificar a proteção.

Escolha o nível certo de proteção

O Proofpoint Collaboration Security Prime está disponível em vários níveis. Isso permite alinhar a proteção ao perfil de risco e às necessidades operacionais da sua organização. Cada nível acrescenta algo em relação ao anterior.

A cobertura é expandida, de ameaças de e-mail básicas a canais de colaboração, comprometimento de contas, redução do risco humano e proteção avançada de marcas.

Veja os recursos disponíveis na próxima página.



Saiba mais em **proofpoint.com/br**

Sobre a Proofpoint. Inc. A Proofpoint, Inc. é líder global em cibersegurança centrada em pessoas e agentes, protegendo a forma como pessoas, dados e agentes de IA se conectam por e-mail, nuvem e ferramentas de colaboração. A Proofpoint é uma parceira confiável de mais de 80 empresas da Fortune 100, mais de 10.000 grandes corporações e milhões de organizações menores, ajudando a combater ameaças, prevenir perda de dados e desenvolver resiliência, tanto de pessoas quanto de fluxos de trabalho de IA. A plataforma de segurança de colaboração e de dados da Proofpoint ajuda organizações de todos os tamanhos a proteger e capacitar suas equipes para que possam adotar a IA de forma segura e confiável. Saiba mais em www.proofpoint.com/br.

Conecte-se com a Proofpoint: [LinkedIn](#)

Proofpoint é uma marca registrada ou marca comercial da Proofpoint, Inc. nos Estados Unidos e/ou em outros países. Todas as demais marcas comerciais contidas neste documento são propriedade de seus respectivos donos.

Todos os níveis da solução Proofpoint Collaboration Security estão disponíveis tanto para implantações de SEG quanto de API. A disponibilidade de recursos pode variar conforme o modelo de implantação.

	Recursos disponíveis	Proofpoint Core Email Protection	Proofpoint Collaboration Security Tier 2	Proofpoint Collaboration Security Tier 3	Proofpoint Collaboration Security Prime
Segurança de e-mail	Proteção contra BEC, phishing, phishing de retorno de chamada e malware	✓	✓	✓	✓
	Solução de detecção multicamada alimentada pelo Nexus AI	✓	✓	✓	✓
	Dados de ameaças incomparáveis de mais de 2,8 M de clientes	✓	✓	✓	✓
	Análise de anexos e URLs em área restrita (sandbox)	✓	✓	✓	✓
	Recriação e análise de URLs em área restrita (sandbox) no momento do clique	SEG	SEG	SEG	SEG
	Isolamento de cliques suspeitos em URLs recriados	VAPS*	Todos os usuários*	Todos os usuários*	Todos os usuários*
	Detecção de spam e graymail	✓	✓	✓	✓
	Tags contextuais de advertência de e-mail	✓	✓	✓	✓
	Higiene de e-mail adaptável que aprende automaticamente com base no comportamento do usuário	✓	✓	✓	✓
	Políticas de roteamento de e-mail configuráveis	SEG	SEG	SEG	SEG
Proteção contra ameaças em múltiplos canais e estágios	Remediação automática de mensagens	✓	✓	✓	✓
	Automatização da caixa de correio para denúncia de abuso	✓	✓	✓	✓
	Inteligência global e sobre perpetradores de ameaças e Very Attacked People (VAP)™	✓	✓	✓	✓
	Detecção e correção de contas de nuvem comprometidas		✓	✓	✓
Resiliência humana e conscientização quanto à segurança	Bloqueio de URLs maliciosos enviados por meio de aplicativos de mensagens e colaboração		✓	✓	✓
	Detecção de uso indevido de senhas corporativas em sites arriscados ou não autorizados		✓	✓	✓
	Proteção contra comprometimento de contas de fornecedor		✓	✓	✓
	Orientação de usuários com educação automatizada baseada no risco			✓	✓
Proteção contra impostura	Aumento da conscientização dos funcionários com simulações baseadas em ameaças do mundo real			✓	✓
	Conversão de ameaças ativas em simulações seguras			✓	✓
	Detecção e priorização de usuários sob risco com base em comportamentos, telemetria de ameaças e funções			✓	✓
Proteção contra impostura	Prevenção de abuso de marcas por meio de autenticação de e-mail				✓
	Detecção e correção de domínios parecidos maliciosos				✓
	Retransmissão segura de e-mails de aplicativo (250 GB)				✓

SEG = Apenas implantação gateway de e-mail seguro

* = Disponível apenas para implantações de SEG.