proofpoint.

RESUMO DA SOLUÇÃO

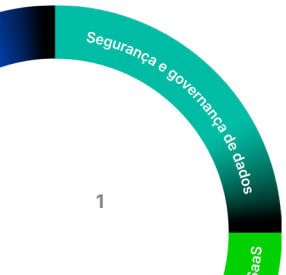
Proofpoint Data Loss Prevention

Transforme a sua arquitetura e o seu programa de segurança de dados.

Principais vantagens

- Evite perda de dados em e-mail, nuvem e endpoints
- Acelere a resolução de incidentes, inclusive triagem de alertas de DLP, investigações e resposta
- Implemente rapidamente, expanda automaticamente e simplifique a manutenção
- Cumpra requisitos de privacidade de dados nos Estados Unidos e em outras regiões

Este conjunto de soluções é parte da plataforma integrada Human-Centric Security da Proofpoint que atende as quatro áreas de risco baseado em pessoas.



Os funcionários de hoje em dia colocam dados em risco de cada vez mais maneiras. Eles utilizam, cada vez mais, ferramentas de produtividade não aprovadas, como inteligência artificial generativa (GenAI). Eles também utilizam dispositivos pessoais para acessar os aplicativos de nuvem de suas organizações. As equipes de segurança de dados estão tendo cada vez mais dificuldades para acompanhar essa tendência, pois precisam fazer mais com menos para assegurar a privacidade dos dados. Ao mesmo tempo, as consequências das violações de dados para as empresas estão se tornando mais onerosas. Resultados negativos incluem perdas financeiras, danos à reputação e falta de conformidade regulatória. As organizações precisam de uma visibilidade melhor sobre seus dados de e-mail, nuvem e endpoint e sobre o comportamento de seus usuários. Porém, ferramentas tradicionais de prevenção de perda de dados (DLP) não satisfazem essas necessidades. O pior é que elas frequentemente são compartimentadas, caras e difíceis de manter e de expandir.

Com as soluções de prevenção de perda de dados (DLP) da Proofpoint, você pode transformar a sua arquitetura e o seu programa de segurança de dados. Nossas soluções seguem uma abordagem adaptável de DLP. Com isso, você pode resolver perdas de dados relacionadas a pessoas nos seus canais de e-mail, nuvem e endpoint com mais efetividade e eficiência.

A Proofpoint identifica conteúdo confidencial com precisão e oferece visibilidade detalhada sobre o comportamento dos usuários. Um console único e unificado ajuda você a gerenciar alertas e a investigar incidentes em todos os canais. Com análises poderosas, você pode avaliar rapidamente o risco para os dados, chegar a vereditos de alta fidelidade e tomar as providências apropriadas. Nossas soluções baseiam-se em uma arquitetura nativa de nuvem, com controles de privacidade modernos e um agente altamente estável. Essas se expandem automaticamente e são de fácil implantação e manutenção.

Reduza o risco à segurança dos dados em e-mail, nuvem e endpoints

Visibilidade profunda sobre o comportamento dos usuários

A Proofpoint monitora como os seus funcionários interagem com os dados no e-mail, em endpoints gerenciados e não gerenciados e em aplicativos de nuvem, como Microsoft 365, Google Workspace e Salesforce. Nós oferecemos insights sobre as intenções dos usuários, ajudando você a responder adequadamente ao risco para os dados. Nós também detectamos e evitamos vazamentos de dados confidenciais. Como exemplos podemos citar a cópia de arquivos para uma unidade USB não autorizada ou a tentativa de fazer upload para uma pasta de nuvem pessoal.

Por meio de integrações com LDAP e Active Directory, a Proofpoint ajuda você a definir e a aplicar dinamicamente políticas granulares de criptografia de e-mail. Nós também coletamos telemetria sobre os seguintes comportamentos:

- **Manipulação de arquivos** — como renomeação de arquivos com dados confidenciais ou alteração de extensões de arquivos
- **Uso de sites e aplicativos** — como download e instalação de ferramentas de backup de dados ou de hackeamento obtidas na Web
- **Comportamentos perigosos dos usuários mais arriscados** — como manipulação do Registro do Windows para desativar controles de segurança

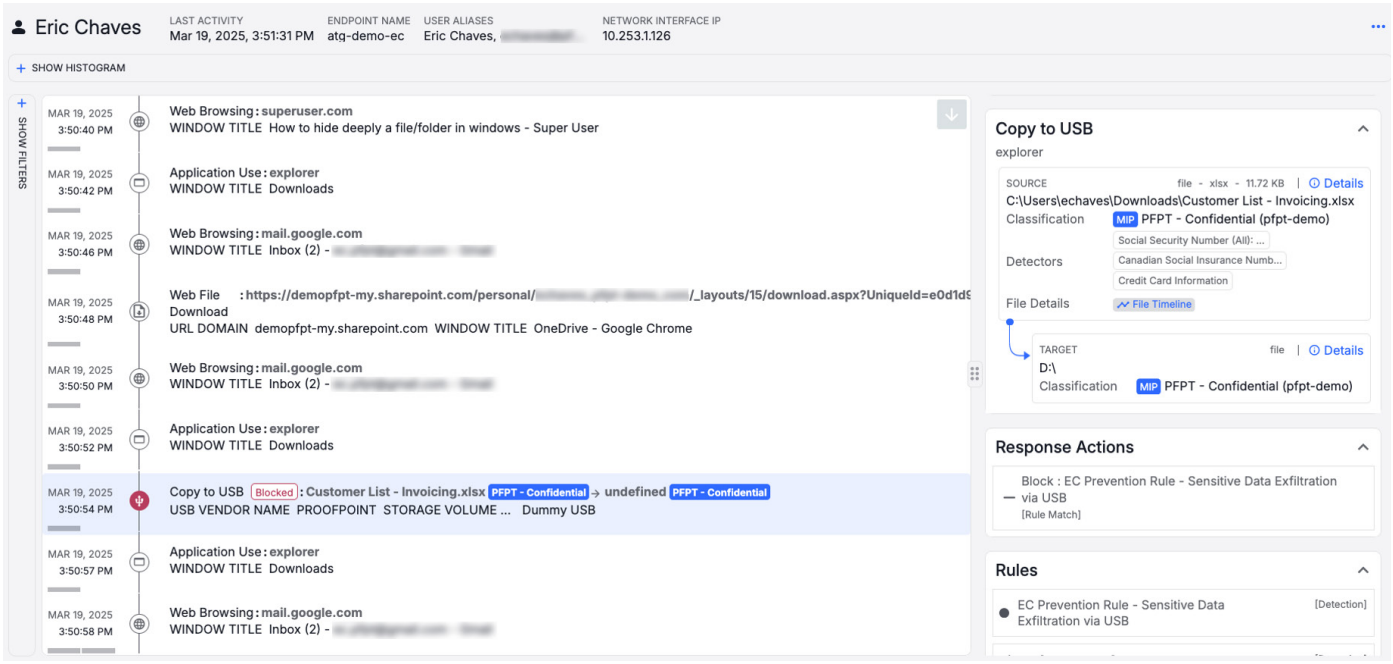


Figura 1. Nessa imagem de tela do console do Data Security Workbench, um usuário visita um site chamado “Como ocultar profundamente um arquivo/pasta no Windows”. Em seguida, o usuário faz o download de um arquivo da unidade de Sharepoint da empresa. Finalmente, o usuário copia um arquivo confidencial chamado “Customer List – invoicing.xlsx” (Lista de clientes – faturamento) para uma unidade USB. A cronologia do comportamento do usuário e a identificação do conteúdo confidencial indicam para um analista que o usuário está tentando contornar a política da empresa e que investigações adicionais são necessárias.

Identificação precisa de conteúdo

A Proofpoint utiliza métodos avançados de identificação de conteúdo para proteger os seus dados. Na nuvem, por exemplo, a correspondência de dados exata e o reconhecimento óptico de caracteres (OCR) podem detectar números de registros médicos em imagens. Isso pode ajudar um fornecedor de serviços de saúde, por exemplo, a reduzir os falsos positivos e negativos.

Você pode criar políticas de DLP com classificadores para grandes modelos de linguagem (LLM). Isso protege conteúdos confidenciais recém-desenvolvidos sem classificação prévia — o que poupa tempo. Ao combinar classificadores de LLM com correspondência de padrões, é possível reduzir os falsos positivos.

Alertas com detalhamento de LLM ajudam a categorizar documentos. Por exemplo, quando uma correspondência de padrões em números de CPF dispara um alerta, a Proofpoint pode identificar se o documento é um formulário de restituição de imposto de renda, a ficha de um paciente ou um pedido de empréstimo. Isso acelera a sua triagem e as suas investigações.

Imposição de políticas adaptáveis

Com insights sobre o comportamento dos usuários e a movimentação de dados confidenciais, você pode responder ao risco para os dados com mais precisão. A Proofpoint evita a perda de dados confidenciais em prompts de GenAI. Nossas soluções instruem os usuários a mudar seus comportamentos, viabilizando um uso aceitável da inteligência artificial. Elas corrigem automaticamente o amplo compartilhamento de arquivos em aplicativos de nuvem. Elas também incentivam o usuário a justificar a cópia de dados confidenciais para uma pasta de nuvem ou para uma unidade de rede.

Com políticas adaptáveis, você pode monitorar mais rigorosamente os usuários de alto risco. Isso proporciona um contexto mais detalhado e uma compreensão melhor das intenções dos seus usuários. Em vez de ajustar políticas manualmente, você pode automatizar as suas respostas a comportamentos arriscados. Com essas políticas dinâmicas, é possível coletar metadados adicionais e evidências visuais das atividades dos usuários quando um alerta é gerado. Com maior visibilidade e insights decisivos, você economiza um tempo valioso de investigação e reduz o seu custo total de propriedade.

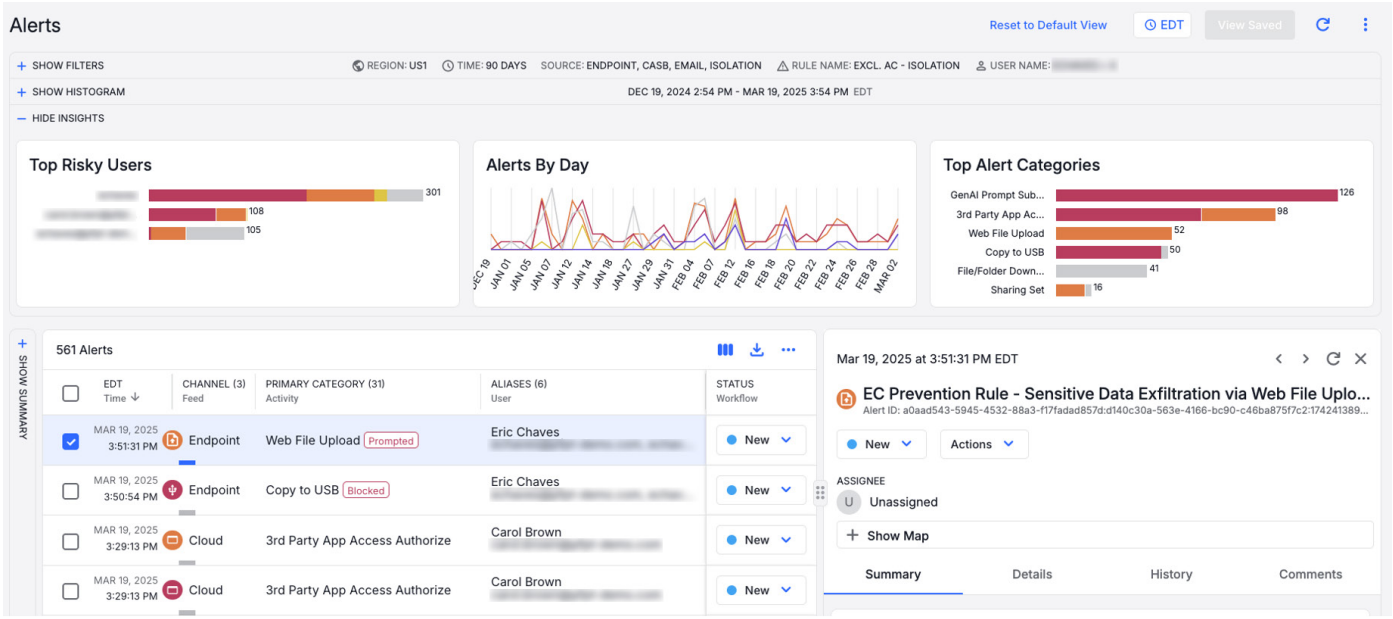


Figura 2. O Data Security Workbench simplifica o gerenciamento de alertas em e-mail, nuvem e endpoints sem que você precise alternar entre vários consoles. Neste exemplo, um analista filtrou os alertas de um usuário específico. O Workbench mostra que o usuário fez upload de dados confidenciais para sua conta de e-mail corporativa e, em seguida, tentou copiar um arquivo para uma unidade USB antes de ser bloqueado.

Reduza os custos operacionais e acelere a resolução de incidentes

Operações de DLP eficientes em múltiplos canais

Equipes de segurança que utilizam ferramentas de DLP tradicionais ou compartimentadas podem ter investigações demoradas e deixar passar violações de políticas. Para proporcionar uma visibilidade completa e unificada do risco aos dados em múltiplos canais, a Proofpoint coleta telemetria de aplicativos de nuvem, endpoints e e-mail. Isso simplifica a triagem de alertas nos vários canais e acelera a investigação e a resposta. O console Data Security Workbench oferece análises poderosas, visualizações intuitivas e fluxos de trabalho eficientes que ajudam você a:

- Investigar as interações dos usuários com os dados em uma visualização cronológica para determinar a intenção e a gravidade do risco (veja a figura 1)
- Triar e correlacionar alertas (veja a figura 2)
- Rastrear a linhagem de um arquivo, desde sua criação, passando por modificações e compartilhamentos
- Coordenar a resposta a incidentes
- Utilizar relatórios executivos predefinidos para demonstrar eficácia e cobertura e gerar relatórios personalizados para fins de auditoria
- Implementar e gerenciar políticas de DLP consistentes e controles de administração para acesso a dados e privacidade nos vários canais

Segurança de dados proativa

O Data Security Workbench tem um recurso sofisticado de pesquisa e filtragem. Isso ajuda você a criar explorações personalizadas para gerenciar riscos de perda de dados proativamente. Você pode pesquisar tentativas de vazamento de dados e outras atividades arriscadas, como o uso de aplicativos de GenAI não aprovados. A visão cronológica das atividades dos usuários ajuda você a compreender o quem, o quê, o onde, o quando e o porquê de cada incidente de segurança.

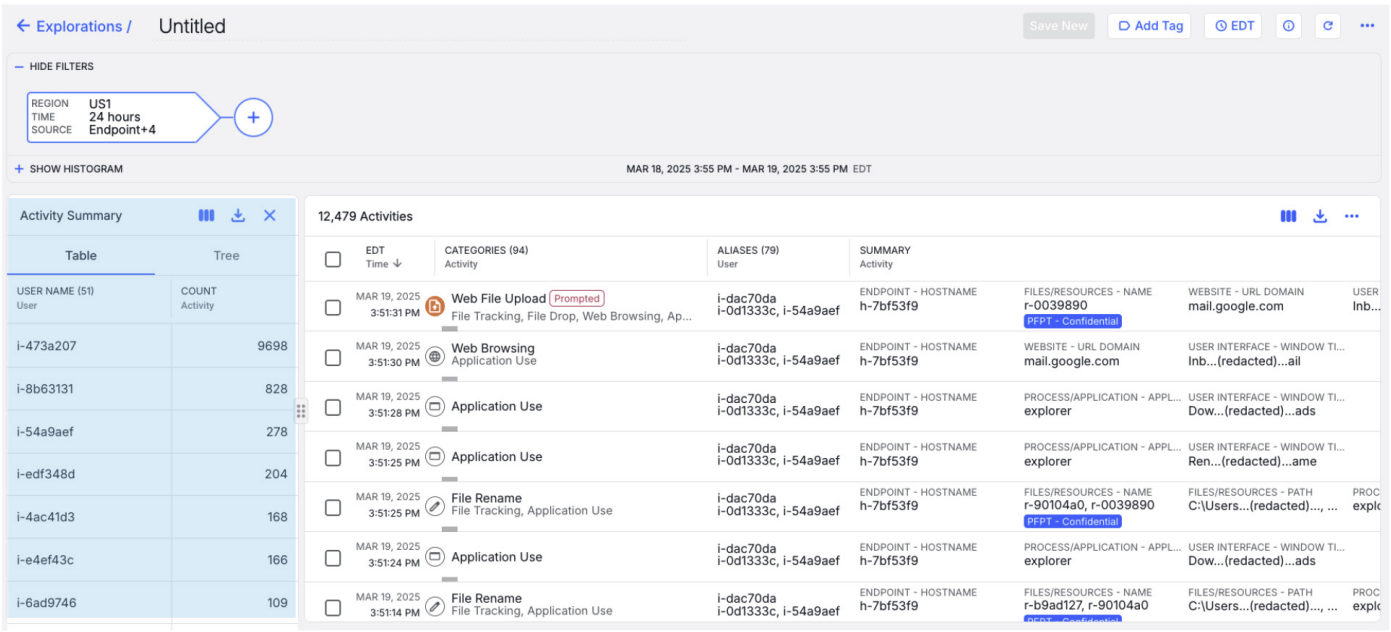


Figura 3. Conforme indicado, o console anonimiza os nomes dos usuários. Isso assegura a privacidade dos usuários sob investigação e elimina o viés do analista.

Viabilize a agilidade empresarial com uma arquitetura moderna

Disponíveis na forma de serviços, nossas soluções poupam um tempo valioso. Elas são implementadas rapidamente, expandidas automaticamente e isso facilita sua manutenção. Elas são modulares, com serviços compartilhados incorporados na nuvem. Nossas soluções nativas de nuvem para múltiplos locatários contam com uma API e são altamente expansíveis. Elas podem comportar centenas de milhares de usuários por locatário. A plataforma da Proofpoint viabiliza integrações via API com parceiros de ecossistema, como Microsoft, Okta, Splunk, ServiceNow e mais.

Controles granulares de privacidade de dados

Embora a Proofpoint ofereça um console nativo de nuvem global, ela pode armazenar dados em múltiplas regiões. Você pode utilizar controles de acesso com base em atributos para gerenciar alertas e investigações sobre funções e cargos regionais. Você também pode mascarar dados confidenciais e anonimizar dados de identificação de usuário (veja a figura 3). Isso ajuda você a cumprir requisitos de privacidade de dados e residência específicos de cada região.

Agente de endpoint altamente estável

Nosso agente leve em modo de usuário é estável e de implantação rápida. Ele é único em sua capacidade de detectar perda de dados e melhorar sua visibilidade sobre ameaças internas em potencial. Você pode mudar o comportamento do agente modificando as políticas na plataforma. Diferentemente de agentes em modo de kernel, o agente da Proofpoint proporciona uma experiência de usuário confiável. Isso elimina tíquetes de suporte e poupa tempo aos seus administradores.

Reduza o tempo de valorização com nossos conhecimentos

Evitar a perda de dados não é fácil. Isso requer conhecimentos técnicos e de produtos e uma compreensão profunda de governança e gerenciamento de dados. A Proofpoint pode ser sua parceira confiável na jornada rumo a um programa de DLP bem-sucedido. Nossos serviços aplicados oferecem os conhecimentos de que você necessita para otimizar o seu investimento em tecnologia, apoiar suas operações contínuas e amadurecer a sua estratégia de proteção de dados.

Principais recursos e capacidades das soluções de DLP da Proofpoint

Compare nossas soluções para encontrar a que melhor atende a sua organização.

PRINCIPAIS RECURSOS E CAPACIDADES	PROOFPOINT DLP TRANSFORM	PROOFPOINT DLP TRANSFORM ADVANCED	ADD-ONS
Contexto detalhado sobre usuários e arquivos	✓	✓	
Caça a ameaças para detecção/investigação proativa	✓	✓	
Um único agente em modo de usuário para ameaças internas e DLP	✓	✓	
Detecções detalhadas de DLP (RegEx, OCR, IDM, EDM) e classificação de MIP	✓	✓	
Monitoramento e detecção de movimentos de arquivos com linhagem de dados	✓	✓	
API, modalidades de proxy normal e reverso	✓	✓	
Ampla detecção de aplicativos de nuvem	✓	✓	
Configuração de DLP e gerenciamento de alertas unificado	✓	✓	
Controles granulares de acesso e de privacidade de dados	✓	✓	
Integração com o ecossistema de segurança (SIEM/SOAR/Teams)	✓	✓	
Detecção e análise de dados confidenciais em mensagens e anexos de e-mail		✓	
Criptografia dinâmica de e-mails externos ou internos		✓	
Impressão digital de documentos confidenciais no e-mail		✓	
Prevenção de perda de dados acidental ou intencional via e-mail à base de inteligência artificial			✓
Descoberta e classificação de armazenamento de dados			✓
Detecção e correção do risco de exposição em armazenamentos de dados			✓
Captura visual de ameaças internas			✓

proofpoint.

A Proofpoint, Inc. é uma empresa líder em cibersegurança e conformidade que protege as organizações em seus maiores riscos e seus ativos mais valiosos: sua equipe. Com um pacote integrado de soluções baseadas em nuvem, a Proofpoint ajuda empresas do mundo todo a deter ameaças direcionadas, proteger seus dados e tornar seus usuários mais resilientes contra ataques cibernéticos. Organizações líderes de todos os portes, incluindo 85% das empresas da Fortune 100, contam com a Proofpoint para obter soluções de segurança e conformidade centradas nas pessoas e que minimizem seus riscos mais críticos em e-mail, nuvem, redes sociais e Web. Mais informações estão disponíveis em www.proofpoint.com/br.

Conecte-se com a Proofpoint: LinkedIn

DESCUBRA A PLATAFORMA DA PROOFPOINT →