proofpoint.

RESUMO DA SOLUÇÃO

Proofpoint Enterprise DLP

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

Principais vantagens

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

Os trabalhadores atuais colocam dados em risco de várias maneiras. Eles usam dispositivos pessoais para acessar aplicativos de nuvem e compartilhar dados por e-mail, endpoints e ferramentas de colaboração. Além disso, ferramentas de IA generativa (GenAI) não aprovadas estão frequentemente acessíveis, bastando um clique no navegador. As equipes de segurança estão se esforçando mais para proteger a privacidade, manter a conformidade e apoiar uma adoção responsável da GenAI. As violações agora trazem consequências cada vez maiores em termos financeiros, de reputação e de auditoria.

As organizações precisam de melhor visibilidade sobre dados confidenciais. Elas também precisam ver como os usuários lidam com esses dados em e-mails, nuvem, endpoints e aplicativos de GenAI. No entanto, ferramentas tradicionais de prevenção de perda de dados (DLP) costumam ser isoladas, difíceis de expandir e inconsistentes entre canais. Elas também são incapazes de lidar com os riscos emergentes relacionados à IA.

O Proofpoint Enterprise DLP promove uma abordagem unificada e adaptável para prevenção de perda de dados (DLP). Ele ajuda a impedir a perda de dados causada por pessoas em e-mails, nuvem, endpoints e aplicativos de IA. Ele também ajuda as equipes de segurança a trabalharem de forma mais eficiente.

A Proofpoint identifica conteúdos confidenciais e mostra como os funcionários os utilizam. Um console unificado ajuda você a gerenciar alertas e a investigar incidentes em todos os canais. Análises e classificação por IA ajudam as equipes a avaliar o risco dos dados, tomar decisões mais precisas e agir rapidamente. A solução opera na nuvem, amplia-se por conta própria e é fácil de implantar e manter. Ela também possui controles de privacidade modernos e um agente altamente estável.

Reduza o risco de segurança de dados em vários canais

Uma visão clara do comportamento do usuário

A Proofpoint monitora como os trabalhadores usam dados em e-mails, endpoints gerenciados e não gerenciados, ferramentas de GenAI e aplicativos de nuvem. Isso inclui Microsoft 365, Google Workspace e Salesforce. Revela a intenção do usuário e detecta e previne o vazamento de dados. Exemplos incluem copiar arquivos para um pendrive USB não autorizado, fazer upload de arquivos confidenciais para uma pasta de nuvem pessoal ou compartilhar informações confidenciais por meio de prompts de IA.

A Proofpoint ajuda as organizações a adotarem a GenAI de forma segura. Ela detecta, bloqueia e redige dados confidenciais antes que estes sejam compartilhados com aplicativos de IA autorizados ou não autorizados. As equipes podem impor políticas em aplicativos de IA para navegador e desktop. Remediação inteligente e experiências orientadas ajudam os usuários a se manterem produtivos.

A Proofpoint monitora e controla:

- Uploads de arquivos para aplicativos de IA
- Atividades de copiar e colar que envolvam dados confidenciais
- Prompts de IA com informações reguladas ou proprietárias
- Anexos confidenciais compartilhados por e-mail e ferramentas de colaboração em nuvem
- Comportamentos arriscados de usuários em endpoints e serviços de nuvem

A Proofpoint integra-se com LDAP e Active Directory. Você pode usar grupos desses diretórios para definir e aplicar dinamicamente políticas detalhadas de criptografia de e-mail. Nossa solução rastreia comportamentos como:

- **Alterações em arquivos**, inclusive renomeação de arquivos que contenham dados confidenciais ou alteração de suas extensões de arquivo
- **Uso de sites e aplicativos incomuns**, inclusive downloads de ferramentas de hackeamento ou de backup de dados
- **Ações perigosas executadas por usuários de alto risco**, inclusive manipulação do Registro do Windows para desativar controles de segurança

Identificação precisa de conteúdo e classificação impulsionada por IA

A Proofpoint melhora a precisão da detecção com mais de 110 classificadores de IA prontos para uso. Estes identificam categorias de documentos e adicionam contexto empresarial aos alertas de DLP. Eles trabalham com correspondência de padrões, correspondência exata de dados (EDM), correspondência de documentos indexados (IDM), reconhecimento óptico de caracteres (OCR) e tecnologias de impressão digital. Essa combinação reduz falsos positivos e melhora a proteção em todos os canais.

A classificação personalizada autônoma (ACC) da Proofpoint utiliza grandes modelos de linguagem (LLMs) para aprender sobre o conteúdo confidencial de cada organização. Isso é feito sem ajustes manuais. As equipes podem encontrar e proteger dados proprietários rapidamente. Exemplos incluem código-fonte, modelos financeiros, documentos de engenharia e registros de clientes. Isso simplifica a criação de políticas e acelera a realização de valor.

Mecanismos compartilhados de detecção à base de IA oferecem uma proteção consistente em todos os canais de DLP da empresa. As organizações podem detectar e classificar informações de identificação pessoal (PII), informações protegidas de saúde (PHI), dados do setor de cartões de pagamento (PCI), credenciais, propriedade intelectual e informações confidenciais da empresa. Alertas enriquecidos por LLM adicionam contexto para que as equipes possam investigar e responder mais rapidamente.

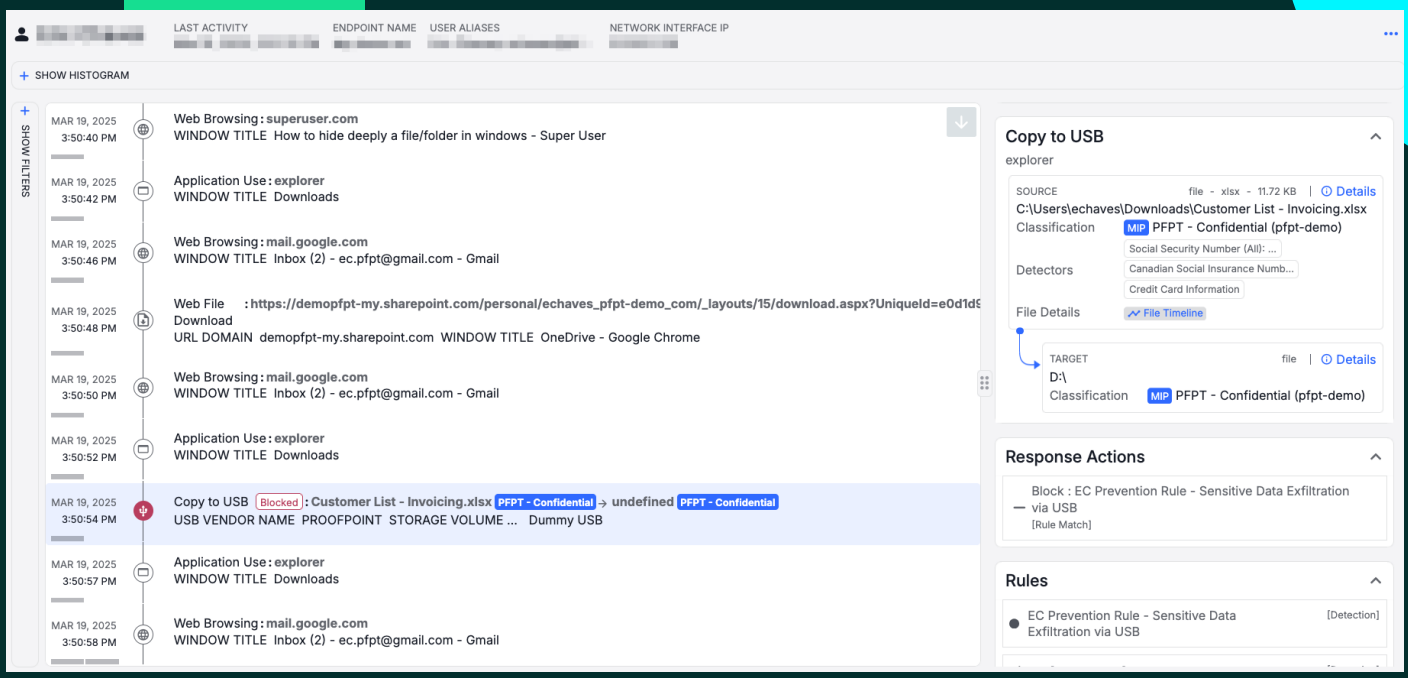

Figura 1. Este exemplo do Data Security Workbench mostra uma sequência arriscada de ações do usuário. O usuário procura maneiras de ocultar um arquivo, faz o download de um arquivo confidencial do SharePoint e tenta copiá-lo para um pendrive. As ações e a cronologia sugerem uma possível evasão de política que exige uma revisão mais aprofundada.

Aplicação adaptável de políticas e remediação orientada para o usuário

A Proofpoint oferece aplicação de políticas compartilhadas em todos os canais de DLP. As equipes podem definir as políticas uma vez e aplicá-las de forma consistente.

Políticas adaptáveis ajudam as equipes a monitorar usuários de alto risco, entender intenções e automatizar respostas. Quando um alerta aparece, essas políticas coletam mais metadados e evidências visuais. Insights mais claros ajudam os analistas a investigar mais rapidamente e a reduzir o custo total de propriedade.

A Proofpoint também previne a perda de dados confidenciais em prompts de GenAI. Nossa solução orienta os usuários para um uso mais seguro da IA. Ela corrige automaticamente o compartilhamento indiscriminado de arquivos em aplicativos de nuvem. Ela também pede que os usuários justifiquem a cópia de dados confidenciais para uma pasta na nuvem ou para uma unidade de rede.

Reduza os custos operacionais e acelere a resolução de incidentes

Operações de DLP eficientes em múltiplos canais

Equipes que utilizam ferramentas de DLP legadas e isoladas frequentemente enfrentam investigações lentas, visibilidade fragmentada e violações não detectadas de políticas. A Proofpoint reúne detecção, políticas e controles de governança em todos os canais de DLP. O Data Security Workbench também centraliza a telemetria e os alertas. Isso ajuda as equipes a realizar triagem, investigação e resposta de forma mais rápida.

O console do Data Security Workbench fornece:

- Visões cronológicas das interações dos usuários com dados confidenciais (veja a figura 1)
- Configuração de DLP e gerenciamento de alertas unificados (veja a figura 2)
- Investigações vinculadas em e-mail, nuvem, endpoints e aplicativos de IA
- Rastreamento da linhagem dos arquivos à medida que os arquivos são criados, modificados e compartilhados
- Caça a ameaças para encontrar e investigar riscos mais cedo
- Dashboards para executivos e relatórios de auditoria

Segurança de dados proativa

O Data Security Workbench permite que você pesquise e filtre riscos de dados. Você pode criar visualizações personalizadas para gerenciar esses riscos antes que eles cresçam. Você pode pesquisar tentativas de vazamento de dados e outras atividades arriscadas, como o uso de aplicativos de GenAI não aprovados. A cronologia do usuário mostra quem fez o quê, onde, quando e por quê.

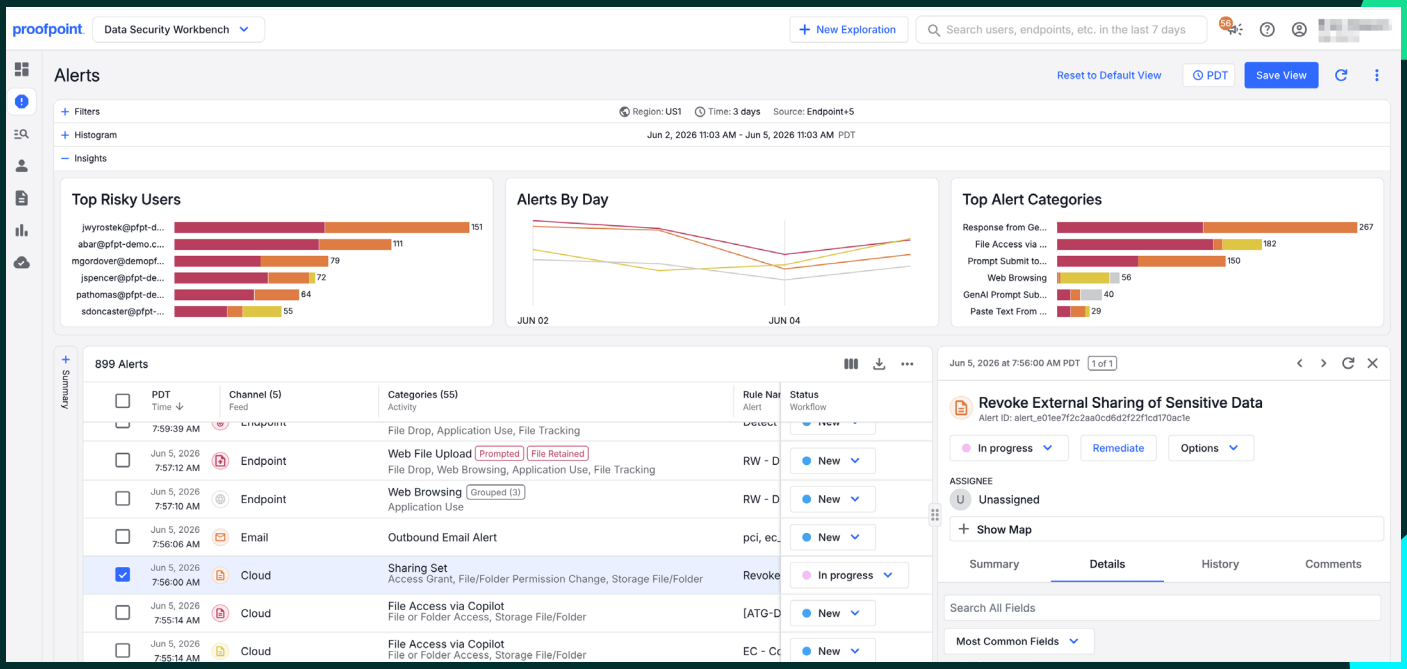

Figura 2. No Data Security Workbench, você pode criar explorações personalizadas de riscos de dados.

Viabilize a agilidade empresarial com uma arquitetura moderna

As soluções da Proofpoint são entregues como serviços, economizando tempo valioso. Elas são implementadas rapidamente, expandem-se automaticamente e facilitam a manutenção. Elas são modulares e utilizam serviços de nuvem compartilhados. Nossas soluções nativas de nuvem suportam múltiplos locatários e APIs. Elas são feitas para serem expandidas. Elas podem acomodar centenas de milhares de usuários por locatário. A plataforma da Proofpoint integra-se com parceiros como Microsoft, Okta, Splunk e ServiceNow.

Controles granulares de privacidade de dados

A Proofpoint oferece um console global nativo de nuvem e pode armazenar dados em várias regiões. Controles de acesso baseados em atributos limitam quem pode visualizar alertas e investigações por função, área ou região. O mascaramento de dados e a anonimização de usuários (veja a figura 3) ajudam a atender regras regionais de privacidade e residência de dados.

Agente de endpoint altamente estável

Nosso agente leve em modo de usuário é estável e de implantação rápida. Ele é único na forma como detecta perda de dados e possíveis ameaças internas. Você pode alterar o comportamento do agente atualizando políticas na plataforma. Diferentemente de agentes em modo de kernel, o agente da Proofpoint proporciona uma experiência de usuário confiável. Isso pode reduzir chamados de help desk e economizar tempo do administrador.

Reduza o tempo para realização de valor com nossos conhecimentos

Prevenir a perda de dados requer especialização técnica e em produto, além de sólidas qualificações em governança de dados. Os serviços Applied da Proofpoint ajudam você a obter mais valor do seu investimento, apoiar operações contínuas e amadurecer seu programa de proteção de dados.

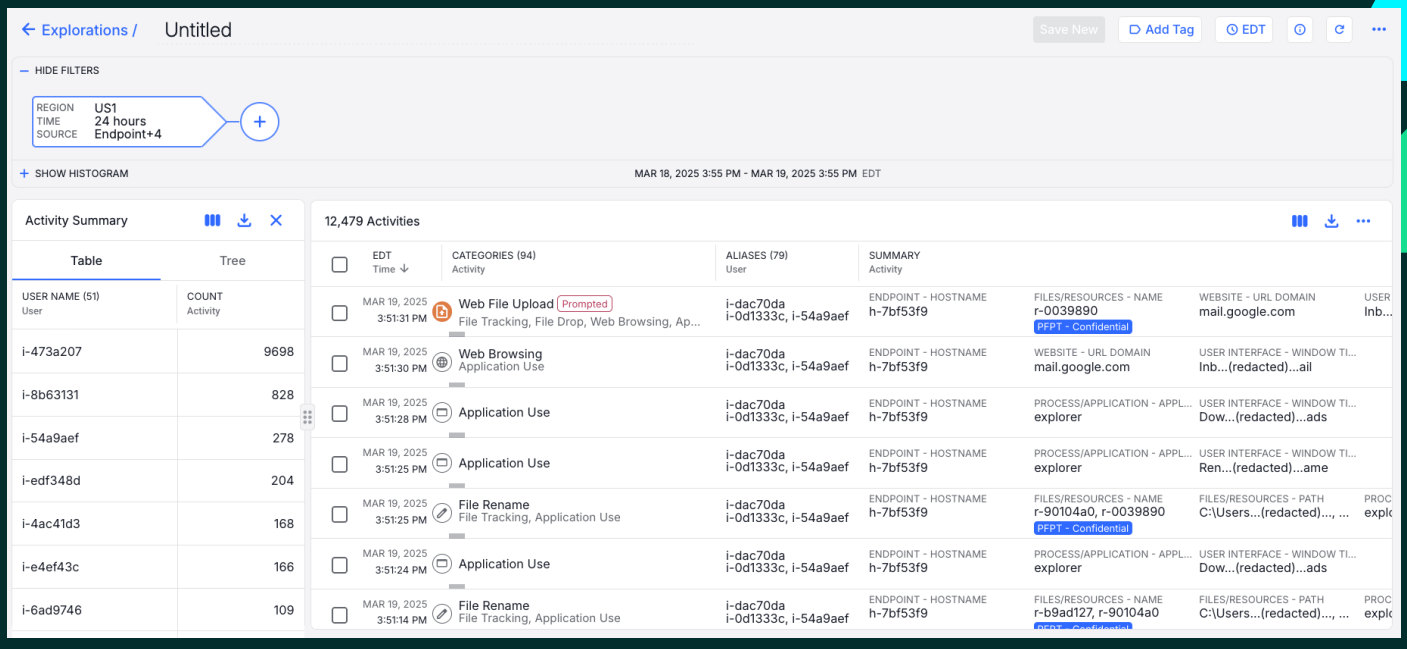

Figura 3. O console pode anonimizar detalhes do usuário durante uma investigação. Isso protege a privacidade e ajuda a reduzir o viés do analista.

Principais recursos e capacidades	DLP Transform Tier 1	DLP Transform Tier 2	Add-ons
Contexto detalhado de usuários e arquivos	✓	✓	
Caça a ameaças para detectar e investigar mais cedo	✓	✓	
Um único agente em modo de usuário para ameaças internas e DLP	✓	✓	
Detectores avançados de DLP (Regex, OCR, IDM, EDM) e classificação de MIP	✓	✓	
Classificadores de IA prontos para uso e autônomos	✓	✓	
Linhagem de dados para monitorar e detectar movimentações de arquivos	✓	✓	
Modalidades de proxy direto, reverso e API	✓	✓	
Detectores abrangentes 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 e Teams)	✓	✓	
Detecção e análise de dados confidenciais em mensagens de e-mail e anexos		✓	
Criptografia dinâmica de e-mails externos ou de comunicações internas		✓	
Impressão digital de documentos confidenciais em e-mails		✓	
Prevenção de perda de dados acidental ou intencional via e-mail à base de inteligência artificial			✓
Descoberta e classificação de repositórios de dados			✓
Detecção de risco de exposição e remediação em repositórios de dados			✓
Captura visual de ameaças internas			✓

Saiba mais

Para obter mais informações, visite **proofpoint.com/br**.

proofpoint.