proofpoint.

RESUMO DA SOLUÇÃO

Segurança de dados para GenAI

Garanta o uso seguro da inteligência artificial generativa.

Principais vantagens

- Tenha visibilidade sobre o uso não autorizado de ferramentas de GenAI
- Evite a exposição de dados confidenciais por ferramentas corporativas de GenAI e pelo desenvolvimento utilizando LLMs
- Imponha políticas de uso aceitável de GenAI na nuvem e nos endpoints
- Monitore ameaças internas com políticas dinâmicas para uso arriscado de inteligência artificial
- Treine os funcionários no uso aceitável de ferramentas de GenAI

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

A inteligência artificial generativa (GenAI) tem um potencial imenso de promover produtividade, inovação e insights de dados. Porém, sua adoção também traz desafios, particularmente em segurança de dados, privacidade e conformidade. Os usuários correm o risco de expor dados confidenciais e propriedade intelectual quando utilizam ferramentas de GenAI públicas e uma governança fraca pode resultar em acesso não autorizado a dados por ferramentas corporativas, como Microsoft 365 Copilot, e saídas de dados confidenciais categorizados indevidamente. LLMs personalizados, treinados com dados de clientes, podem divulgar informações de identificação pessoal (PII), aumentando os riscos de falta de conformidade com regulamentos como RGPD, HIPAA e CCPA. Sem uma governança forte, as organizações se vêem diante de violações de segurança e multas decorrentes da falta de conformidade com os regulamentos.

A Proofpoint assegura um uso aceitável de ferramentas e modelos de GenAI por meio de uma abordagem abrangente e centrada em pessoas que combina visibilidade, controle e educação. A solução Proofpoint Data Loss Prevention (DLP) monitora o uso de GenAI em endpoints, oferecendo insights sobre interações de usuários e identificando ferramentas não autorizadas. Para evitar perda de dados, a Proofpoint impõe políticas que bloqueiam ou editam dados confidenciais inseridos em prompts de GenAI. O Proofpoint Data Security Posture Management (DSPM) evita a exposição de dados por ferramentas de GenAI e LLMs classificando e protegendo dados confidenciais contra acesso não autorizado. Além disso, o Proofpoint ZenGuide oferece treinamento personalizado para conscientização quanto à segurança para educar os funcionários sobre práticas seguras de GenAI, promovendo com isso uma cultura de uso responsável. Ao integrar essas estratégias, a Proofpoint protege os dados confidenciais das organizações no cenário de GenAI em evolução.

Tenha visibilidade sobre o uso não autorizado de ferramentas de GenAI

A Proofpoint ajuda as organizações a compreender quem está utilizando quais ferramentas de GenAI e se dados confidenciais estão sendo vazados por essas ferramentas ou LLMs personalizados. Nosso relatório de segurança de dados sobre uso de inteligência artificial ressalta os tipos de dados confidenciais enviados para ferramentas de GenAI públicas, os usuários mais ativos, os principais sites por atividade e mais (Figura 1).

Por meio de APIs de nuvem, você pode identificar e gerar alertas sobre autorizações de aplicativos de inteligência artificial de terceiros, como OpenAI. Você também pode descobrir implantações de inteligência artificial no AWS Bedrock e no Azure OpenAI que estejam utilizando dados confidenciais.

Principais vantagens

- Evite a exposição de dados confidenciais por ferramentas corporativas de GenAI e pelo desenvolvimento utilizando LLMs

Evite a exposição de dados confidenciais por ferramentas de GenAI e LLMs

O Proofpoint DSPM descobre e classifica dados confidenciais em fluxos de trabalho de inteligência artificial, evitando exposições que possam resultar em violações. Ele também protege dados acessados pelo Microsoft Copilot aplicando rótulos do Microsoft Information Protection (MIP), os quais são utilizados para impor políticas de proteção, como controles de acesso e criptografia.

Ele protege aplicativos de inteligência artificial e LLMs personalizados em plataformas como AWS Bedrock e Azure OpenAI detectando dados confidenciais inseridos em modelos fundamentais ou personalizados e fluxos de trabalho de Retrieval-Augmented Generation (RAG).

A Proofpoint oferece APIs especializadas para segurança de LLM, viabilizando análises de confidencialidade em tempo real dos dados que fluem para dentro e para fora dos LLMs. Essas APIs oferecem governança e visibilidade plenas sobre o uso dos dados, com integração descomplicada nos fluxos de trabalho do cliente, para uma implantação efetiva.

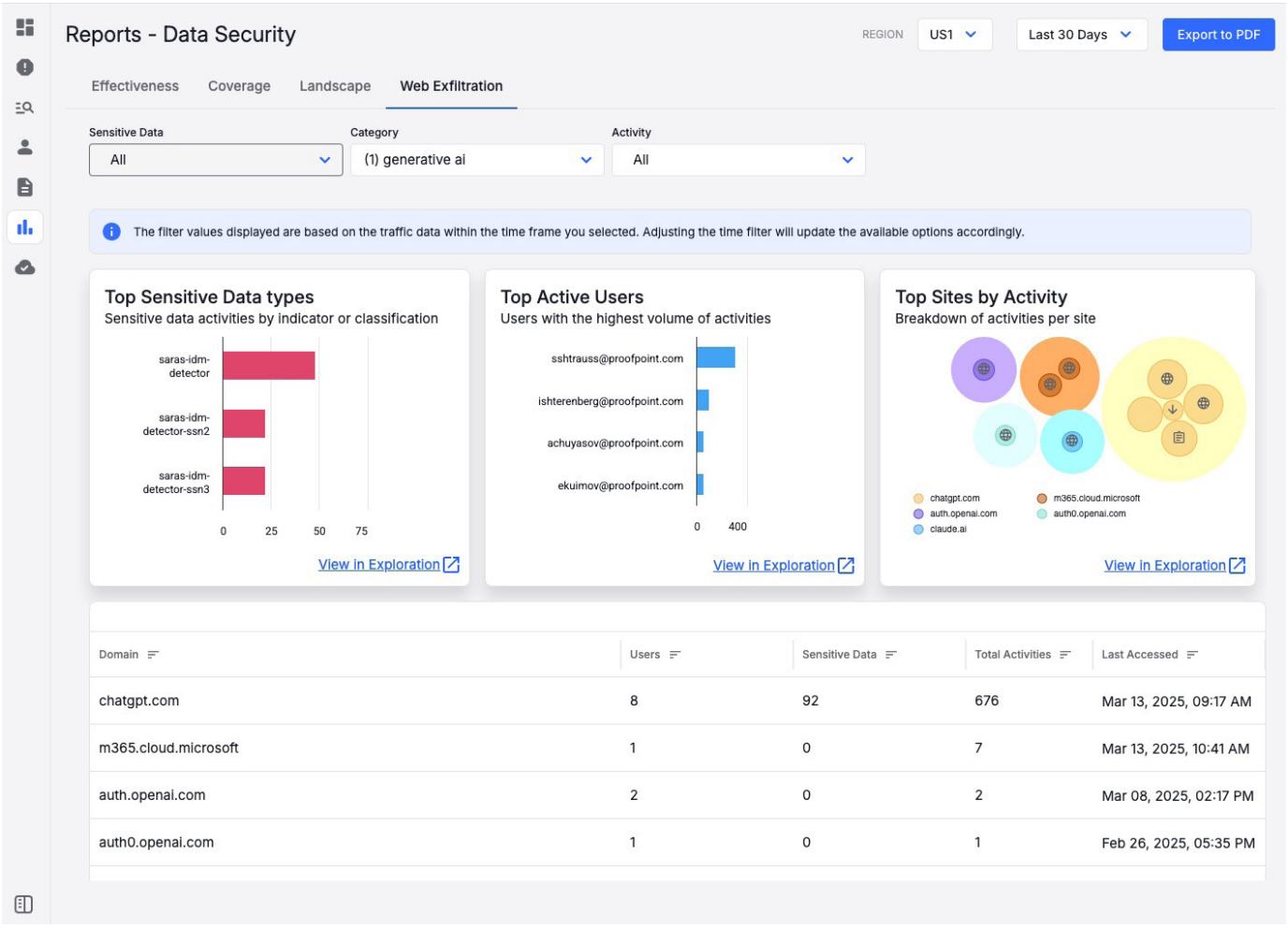

Figura 1. Relatório que destaca os maiores riscos de vazamento de dados por GenAI.

Principais vantagens

- Imponha políticas de uso aceitável de GenAI na nuvem e nos endpoints
- Monitore ameaças internas com políticas dinâmicas para uso arriscado de inteligência artificial
- Treine os funcionários no uso aceitável de ferramentas de GenAI

Defenda-se de perda de dados e ameaças internas associadas ao uso de GenAI

Nos endpoints, você pode monitorar a navegação dos usuários em sites de GenAI utilizando categorização de Web ou gerar alertas de instalações não autorizadas de aplicativos de inteligência artificial. Nossas políticas dinâmicas podem aumentar o monitoramento dos endpoints dos usuários com base em comportamentos arriscados. Você pode, por exemplo, capturar metadados e imagens de tela antes e depois dos usuários enviarem conteúdo confidencial para sites de GenAI não autorizados. Isso ajuda você a poupar tempo na investigação das interações dos usuários com ferramentas de GenAI.

Com o Proofpoint DLP, você pode impor políticas de DLP em endpoints para mais de 600 ferramentas de GenAI por usuário, grupo ou departamento e bloquear uploads via Web para plataformas de GenAI ou editar dados confidenciais inseridos em prompts. Para preservar a produtividade dos usuários, nossa solução também pode incentivar os usuários a obedecer políticas de uso de GenAI ou solicitar a eles uma justificativa de trabalho em vez de aplicar políticas de prevenção.

Com APIs de nuvem, oferecemos visibilidade sobre arquivos expostos por compartilhamento excessivo no Microsoft 365 Copilot e alertamos a sua equipe de segurança quando usuários abusam do Copilot para localizar arquivos que contêm informações confidenciais.

Por exemplo, a Proofpoint detecta quando um elemento interno arriscado utiliza o Copilot para acessar muitos arquivos que contêm dados confidenciais em um curto período de tempo. Além disso, nossa solução classifica, rotula e protege conteúdo gerado por inteligência artificial em aplicativos de nuvem. Ela também revoga ou bloqueia autorizações de aplicativos de inteligência artificial de terceiros não aprovados.

Treine os funcionários no uso aceitável de ferramentas de GenAI

A Proofpoint instrui os usuários a utilizar GenAI com segurança na sua organização. O Proofpoint ZenGuide treina os usuários com vídeos, pôsteres, módulos interativos e boletins informativos sobre manuseio seguro de dados. O Proofpoint ZenGuide permite que você aproveite insights sobre os seus usuários de alto risco e automatize uma aprendizagem adaptada conforme o risco para grupos específicos, como desenvolvedores, ou para os seus usuários mais arriscados.

Atividades de treinamento motivam comportamentos seguros por meio de avaliações, incentivos personalizados e experiências de orientação. As atividades incluem avaliações de conhecimentos, tarefas de treinamento, notificações e reconhecimento de políticas, todas desenvolvidas para aumentar a conscientização e promover um uso seguro e aceitável de ferramentas de GenAI.

Viabilização de negócios com GenAI segura

A Proofpoint oferece uma solução centrada em pessoas para desafios modernos de segurança de dados. Nós oferecemos insights sobre exposição e risco de perda de dados em ferramentas de GenAI e modelos de LLM.

Com a Proofpoint, você pode equilibrar facilmente a produtividade dos usuários com a segurança dos dados adotando estratégias que deem aos usuários acesso a modelos e ferramentas de GenAI com educação, monitoramento mais rigoroso e os controles de dados certos.

proofpoint.

A Proofpoint, Inc. é uma empresa líder em cibersegurança 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 →

0207-017-07-01 03/25