proofpoint.

Guia de compras de soluções de prevenção de perda de dados

Este guia de compras destaca as capacidades mais importantes para uma solução moderna de proteção de informações. Ele resume o que a Proofpoint aprendeu criando programas bem-sucedidos de prevenção de perda de dados (DLP) para organizações de todos os portes, no mundo todo e em todos os mercados verticais. Seu objetivo é ser um guia de referência útil para leitores que estão começando sua jornada de DLP ou que estão atualizando seus sistemas de DLP existentes.

Comece com segurança centrada em pessoas

Para defender dados contra ameaças únicas e comuns, você precisa de uma plataforma compatível com um modelo de segurança centrado em pessoas. O que é um modelo de segurança centrado em pessoas? Essencialmente, ele proporciona visibilidade total sobre como os usuários interagem com dados confidenciais e rastreia qualquer comportamento arriscado. Isso assegura que você obtenha um contexto importante sobre suas intenções quando dados forem perdidos ou roubados ou quando eles fizerem algo que pareça suspeito.

Com uma solução que segue uma abordagem centrada em pessoas, é possível ver rapidamente o seu risco de perda de dados no e-mail, em endpoints e em aplicativos de nuvem, como Microsoft 365, Google Workspace, Salesforce e outros. Esses insights asseguram que você possa agir rapidamente e seguir os passos apropriados para evitar quaisquer incidentes de perda de dados.

Elementos-chave de uma solução de DLP moderna

Para gerenciar a perda de dados e evitar ameaças internas, você precisa ser capaz de detectar, analisar, prevenir e responder aos incidentes. Só é possível reduzir os seus riscos fazendo tudo isso de forma coordenada.

Monitorar

Para proteger dados, você não pode se concentrar apenas no conteúdo. Você precisa de visibilidade sobre o que os usuários estão fazendo com os dados. Ao monitorar a atividade de dados de todos os usuários em endpoints, e-mail, nuvem e Web, você tem uma visão holística e insights contextualizados.

85%

das organizações sofreram um ou mais incidentes de perda de dados em 2023

50%

dos adultos economicamente ativos que mudaram de emprego nos últimos dois anos admitiram ter levado consigo dados da empresa

Detectar

Você precisa de uma solução que possa detectar, o mais imediatamente possível, quando um usuário executa uma ação arriscada ou quando dados são potencialmente expostos — mesmo que não chegue ao nível de um incidente com todas as suas implicações. As capacidades de detecção precisam atingir o equilíbrio ideal no que se refere a alertas, os quais devem ser tanto imediatos quanto decisivos. Não deve haver excesso de alertas, a ponto de causar fadiga.

Analisar

Com uma boa análise, você pode analisar tendências comportamentais dos usuários e caçar as ameaças. Contudo, isso só é possível quando uma solução de DLP combina atividades de usuários de múltiplos canais. Isso assegura que você capture qualquer comportamento de usuário arriscado. Embora isso possa ser feito automaticamente, é fundamental que analistas possam se aprofundar nos próprios dados para terem êxito.

Responder

É importante investigar e responder aos incidentes com rapidez e eficiência. Por quanto mais tempo uma ameaça interna persistir, mais danos ela pode causar à sua reputação e à sua lucratividade. Uma solução moderna de DLP pode impor políticas e remediar ameaças automaticamente. A automação mantém seguros os seus dados mais valiosos e aumenta a eficiência da sua equipe de segurança.

Prevenir

Prevenção é a capacidade de impedir que um usuário viole as suas políticas de segurança, acidental ou intencionalmente. Isso é feito por meio de treinamento dos usuários, lembretes em tempo real e bloqueio de atividades dos usuários, quando necessário.

3 principais casos de uso

As organizações perdem dados de três maneiras principais. Todas são causadas por pessoas. Uma plataforma de proteção de informações centrada em pessoas precisa lidar com:

- Usuários descuidados, displicentes no manuseio de dados confidenciais
- Usuários descuidados que expõem dados confidenciais ao utilizar aplicativos de inteligência artificial generativa (GenAI)
- Elementos internos maliciosos, cuja intenção é causar danos

1. Usuários descuidados e erros comuns

Usuários descuidados são a principal causa de perda de dados, segundo o relatório Data Loss Landscape de 2024 de Proofpoint. Esses usuários não desejam vazar dados. Eles só querem fazer seu trabalho com o máximo de eficiência. Porém, seus erros podem ter consequências graves, como interrupção de negócios, danos à marca, enfraquecimento perante a concorrência, multas e violações de regulamentos e ações judiciais.

US$3,5 bi é o gasto total projetado com DLP até 2025.[1]

77 DIAS para resolver ameaças internas.[2]

85% das organizações são visadas por ataques de nuvem.[3]

56% dos incidentes estão relacionados a descuido por parte do usuário.[4]

Veja a seguir algumas das maneiras pelas quais esses usuários geram risco:

- Envio de e-mails para pessoas erradas, com ou sem anexos
- Visitação de sites de phishing
- Instalação de software não autorizado
- Compartilhamento público de arquivos e dados confidenciais
- Envio de informações de identificação pessoal (PII) para uma conta de e-mail pessoal
- Armazenamento de dados corporativos confidenciais em dispositivos pessoais

Proteção contra comportamento descuidado

Um sistema eficaz de proteção de informações centrado em pessoas bloqueia as atividades arriscadas. Ele também oferece instruções aos usuários descuidados para ajudá-los a compreender o que há de errado em seus comportamentos para que eles possam mudá-los.

O que procurar:

- **Classificação.** Certifique-se de que e-mails, dados e conteúdos sejam monitorados consistentemente, tanto manualmente quanto por inteligência artificial (AI) para identificar e classificar os usuários arriscados. Quando um usuário é classificado como de alto risco, o sistema atribui uma pontuação de risco para proteger devidamente os dados.
- **Detecção.** O sistema deve monitorar e-mails, documentos e dados, avaliando riscos de conformidade constantemente. Enquanto o conteúdo está em movimento entre canais — sejam endpoints, e-mail, nuvem ou Web — ele deve ser examinado para assegurar que essa movimentação ou compartilhamento não viole as políticas da sua organização. Caso uma violação seja detectada no e-mail, o sistema deve permitir que equipes de segurança bloqueiem o e-mail ou o rastreie para investigação adicional.
- **Prevenção.** Os usuários devem ser impedidos de vazar dados confidenciais por canais e dispositivos. Isso inclui e-mails mal direcionados (com ou sem anexos), unidades USB, uploads na Web, sincronização na nuvem e impressão. Se os usuários cometerem um erro, eles devem receber imediatamente uma mensagem de advertência contextualizada que os permita remediar e evitar o incidente de perda de dados em tempo real, sem a participação de um administrador. Conforme o caso, os usuários podem explicar porque precisam de acesso aos dados. Com isso, a equipe de segurança é notificada, podendo permitir ou negar a solicitação.

1 The Radicati Group. “Data loss prevention (DLP) market value revenue forecast worldwide from 2019 to 2025” (Previsão global de receitas em valor de mercado, de 2019 a 2025). Maio de 2022.
2 Ponemon Institute. “2022 Cost of Insider Threats Global Report” (Relatório global sobre o custo das ameaças internas de 2022). Fevereiro de 2022.
3 Assaf Friedman e Itir Clarke (Proofpoint) “How Attackers Use Compromised Accounts to Create and Distribute OAuth Apps” (Como atacantes utilizam contas comprometidas para criar e distribuir aplicativos OAuth). Maio de 2021.
4 Ponemon Institute. “2022 Cost of Insider Threats Global Report” (Relatório global sobre o custo das ameaças internas de 2022). Fevereiro de 2022.

2. Usuários descuidados e aplicativos de GenAI

Os usuários podem conseguir um grande aumento de produtividade quando utilizam o ChatGPT e outras ferramentas de inteligência artificial generativa (GenAI). Porém, dados confidenciais são frequentemente vazados dessa forma. Para evitar a perda de dados sem prejudicar a produtividade, você precisa de medidas robustas de proteção de dados. O problema é que não se pode impor políticas de uso aceitável de GenAI quando não se compreende o conteúdo e a maneira como os funcionários interagem com ele.

Proteção contra comportamento descuidado com GenAI

Medidas robustas de proteção de dados são importantes para proteger dados confidenciais contra vazamento por ferramentas de GenAI. Você não pode simplesmente bloquear totalmente o acesso a ferramentas de GenAI. É importante encontrar maneiras de dar acesso aos usuários porque essas ferramentas aumentam a produtividade e promovem inovação.

Se você quer que os funcionários utilizem ferramentas de GenAI sem colocar em risco a segurança dos dados, é preciso adotar uma abordagem centrada em pessoas no que se refere à perda de dados. Uma solução que utiliza essa abordagem permite e bloqueia cirurgicamente o uso de ferramentas de GenAI por parte dos funcionários com base em seu comportamento e em suas interações com o conteúdo, mesmo que os dados tenham sido manipulados ou tenham passado por vários canais.

O que procurar:

- **Identificação de conteúdo confidencial.** Quando um sistema consegue identificar qual conteúdo é importante e deve ser protegido, ele pode evitar a perda de dados com muito mais eficiência. Procure métodos avançados de identificação e classificação de conteúdo, como reconhecimento ótico de caracteres, correspondência de dados exata e correspondência de documentos indexados.
- **Monitoramento de usuários.** Deve haver visibilidade sobre quem está utilizando ferramentas de GenAI no seu ambiente e como as estão utilizando. O sistema deve ser capaz de detectar, bloquear e alertar sobre vários tipos de ações do usuário. Isso inclui o upload de arquivos de código-fonte e a colagem de propriedade intelectual corporativa.
- **Gerenciamento de risco proativo.** Ao criar e salvar investigações personalizadas, as suas equipes podem pesquisar regularmente vazamentos de dados e outras atividades arriscadas associadas a ferramentas de GenAI.

3: Usuários maliciosos

Usuários maliciosos são perigosos porque estão na posição ideal para capturar dados confidenciais. E funcionários demissionários são um dos tipos mais arriscados de elementos internos. Ao longo de um período de nove meses em 2023, funcionários demissionários causaram 87% dos vazamentos de arquivos anômalos entre os locatários de nuvem que utilizaram a plataforma Proofpoint Information Protection. Tais usuários costumam achar que têm o direito de levar informações consigo ao deixar a empresa devido ao tempo que dedicaram aos seus projetos.

O que torna os elementos internos tão ameaçadores é que eles podem esperar pacientemente pela oportunidade certa e usar seu acesso privilegiado para encontrar dados valiosos e pontos fracos na segurança. Além disso, as empresas frequentemente pioram sua própria situação ao permitir que os funcionários acessem e armazenem dados em seus dispositivos pessoais. Isso facilita ainda mais que os funcionários roubem dados confidenciais.

Um sistema centrado em pessoas monitora alguns usuários mais rigorosamente que outros. Ele também aplica controles de segurança mais rígidos aos usuários mais arriscados.

Proteção contra usuários maliciosos

Um sistema centrado em pessoas monitora alguns usuários mais rigorosamente que outros. Ele também aplica controles de segurança mais rígidos aos usuários mais arriscados. Além disso, ele bloqueia proativamente ações maliciosas com base em fatores de risco, como quando um funcionário pede demissão ou é despedido.

O que procurar:

- **Visibilidade.** Visibilidade sobre endpoint, e-mail, nuvem e Web proporciona uma visão holística e oferece insights contextualizados sobre o que o usuário está fazendo. Deve-se coletar telemetria sobre as interações dos usuários com dados e sistemas — como quando eles renomeiam um arquivo confidencial ou fazem upload de tal arquivo para um site não autorizado ou uma pasta de sincronização na nuvem. Se um usuário instala ou executa aplicativos não autorizados, essas atividades também devem ser monitoradas. E a equipe de segurança deve poder monitorar, em tempo real, qualquer um que dispare um alerta.
- **Investigações.** Você quer uma biblioteca abrangente de ameaças com alertas sobre os casos de uso mais comuns (descumprimento de expediente, vazamento de dados e desvio de controles de segurança). Isso assegura que você esteja operacional rapidamente. Os alertas para a equipe de segurança devem incluir metadados detalhados e imagens de tela das atividades dos usuários. E uma cronologia de eventos contextualizada ajuda os investigadores a compreender o “quem, o quê, quando e onde” da atividade do usuário.
- **Arquitetura moderna.** A vantagem de uma plataforma nativa em nuvem é que ela pode ser dimensionada para centenas de milhares de usuários. Quando ela inclui recursos como controles de acesso baseados em atributos, mascaramento e anonimização de dados e suporte para data centers multirregionais, é possível cumprir requisitos de residência e privacidade de dados. Além disso, um sistema moderno estende o seu sistema de segurança. A razão disso é que ele facilita a integração com uma variedade de ferramentas, inclusive:
  - Coordenação de segurança, automação e resposta (SOAR)
  - Gerenciamento de eventos e informações de segurança(SIEM)
  - Resposta a incidentes
  - Sistemas de gerenciamento de tíquetes

Capacidades exigidas

Agora que você sabe como sistemas de DLP modernos e centrados em pessoas podem ajudar a protegê-lo, vejamos mais atentamente as capacidades exatas de que você necessita. Elas se enquadram em três categorias:

- Detecção e prevenção do risco de perda de dados
- Análise e resposta
- Implantação e implementação

Detecção e prevenção do risco de perda de dados

Quando as equipes de segurança têm insights sobre o comportamento dos usuários e sobre conteúdos confidenciais, elas podem responder ao risco dos dados de maneira apropriada e com mais precisão.

NECESSIDADE DO CLIENTE	CAPACIDADES EXIGIDAS
Detecção de conteúdo confidencial	Detecção e análise de dados confidenciais em e-mail, endpoint, nuvem e Web
	Capacidade incorporada de classificar dados confidenciais com base no contexto corporativo
	Classificação de dados complementada por inteligência artificial com grandes modelos de linguagem (LLM)
	Métodos avançados de identificação, inclusive: • Reconhecimento ótico de caracteres (OCR) • Correspondência de dados exata (EDM) • Correspondência de documentos indexados (IDM)
	Políticas predefinidas para detectar dados confidenciais, como: • PII • PCI, SOX, GLBA e termos da SEC sobre negociação com base em informações privilegiadas • PHI, HIPAA, ICD-9, ICD-11 e código nacional de drogas • RGPD, UK-DPA, EU-DEPD, PIPEDA
	Capacidade de definir políticas para ler e aplicar rótulos de confidencialidade do Microsoft Information Protection (MIP) para identificar dados críticos da empresa

NECESSIDADE DO CLIENTE	CAPACIDADES EXIGIDAS
Monitoramento do comportamento dos usuários	Uma abordagem centrada em pessoas que permite aos analistas responder rapidamente ao oferecer insights sobre: • Intenção do usuário • Padrões de acesso a dados • Padrões de acesso a aplicativos
	Capacidade de monitorar interações do usuário com dados na nuvem e em endpoints gerenciados e não gerenciados, como: • Renomeação de arquivos • Alteração em extensões de arquivos • Upload e download na Web • Cópia para USB • Sincronização de compartilhamentos na nuvem • Abertura de documentos • Atividade de arquivo anômala
	Monitoramento de uso de sites e aplicativos, como: • Upload, colagem ou digitação de conteúdo em sites de GenAI • Download e instalação de ferramentas de hackeamento e backup de dados
	Monitoramento do comportamento dos seus elementos internos mais arriscados para compreender suas intenções e mitigar o risco, como ao manipular o Registro do Windows para remover controles
	Monitoramento proativo de usuários arriscados ao capturar telas somente quando um alerta for gerado, para preservar a privacidade
	Capacidade de instruir os usuários e pedir justificativa para acesso a dados confidenciais em vez de bloquear e prejudicar a produtividade (e-mail, endpoint, nuvem e Web)
Prevenção de perda de dados	Treinamento para conscientização quanto à segurança que ajuda a mudar o comportamento dos usuários quando estes aprendem a evitar riscos de cibersegurança e protegem dados confidenciais
	Prevenção de vazamento de dados confidenciais de endpoints gerenciados, como: • Cópia de arquivos para um dispositivo USB não autorizado • Upload de arquivos para uma pasta pessoal na nuvem • Impressão de documentos confidenciais • Colagem de conteúdo confidencial da área de transferência • Compartilhamentos de rede
	Remediação automática do compartilhamento indiscriminado de arquivos em aplicativos de nuvem e redução automática de permissões de compartilhamento de arquivos
	Viabilização de acesso seguro de dispositivos não gerenciados a arquivos confidenciais em aplicativos de nuvem aprovados pelo departamento de TI
	Detecção e prevenção automáticas de e-mails enviados para pessoas erradas, com ou sem anexo
	Detecção e prevenção automáticas de e-mails enviados para pessoas certas, mas com o arquivo errado anexado
	Prevenção de compartilhamento de dados confidenciais ainda não predefinidos para contas de e-mail pessoais e outras contas não autorizadas

Análise e resposta

É importante para as equipes de segurança resolver incidentes rapidamente entre diversos canais. Também é desejável limitar a exposição dos dados para resguardar a privacidade.

NECESSIDADE DO CLIENTE	CAPACIDADES EXIGIDAS
Resolução de incidentes em vários canais	Um console multicanal unificado para e-mail, endpoint e nuvem, utilizado para: • Triagem de alertas • Investigações • Investigações personalizadas • Resposta
	Análise multicanal que mostra: • Atividades dos usuários ao longo do tempo • Atividades de arquivo ao longo do tempo, conforme eles são criados, modificados e compartilhados
	Capacidades proativas de investigação que proporcionam visibilidade em tempo real sobre comportamentos de usuários arriscados
	Integração com o SIEM da sua organização, permitindo triagem de fluxos de trabalho com as ferramentas existentes
	Capacidade de detectar e responder automaticamente a riscos de perda de dados associados a usuários comprometidos por meio de: • Encerramento de sessões • Redefinição de senhas • Remediação do risco • Identificação do impacto
Privacidade	Controles de acesso flexíveis que garantem que os analistas só vejam os dados de que precisam
	Informação de identificação de usuário anonimizada e mascaramento de conteúdo confidencial para proteger os dados e eliminar a parcialidade dos analistas

Implantação e implementação

Após escolher a melhor solução de DLP para a sua organização, você terá de implantá-la. A chave para uma implantação descomplicada é escolher os parceiros certos para ajudá-lo na sua jornada de DLP.

NECESSIDADE DO CLIENTE	CAPACIDADES EXIGIDAS
Implantação	Uma solução nativa em nuvem que pode ser implantada rapidamente
	Uma solução altamente expansível que pode ser estendida facilmente para centenas de milhares de usuários por locatário
	Uma solução de fácil manutenção que requer o mínimo de atenção e cuidado, na qual as atualizações são comunicadas com clareza e a assistência do fornecedor está disponível conforme a necessidade
	Administração e política centralizadas que cumprem requisitos de residência de dados em múltiplas regiões
	Uma plataforma flexível que se integra com o seu ecossistema de segurança, incluindo soluções como: • Microsoft • Okta e Sailpoint • CrowdStrike • Splunk e Service Now • Zscaler e Citrix ShareFile
	Um agente de endpoint leve em modo de usuário que: • Aumenta a visibilidade sobre possíveis ameaças internas • Melhora a produtividade dos usuários • Elimina problemas de estabilidade • Não conflita com outras soluções
Implementação	Serviços profissionais que podem ajudar você a implantar a solução rapidamente com uma equipe de especialistas experientes e a ajustar o seu sistema conforme as suas necessidades. A implementação de uma solução de DLP exige muitas etapas, como: • Coleta de requisitos • Projeto • Personalização da solução • Testes e ajustes • Treinamento de administradores e usuários • Documentação
DLP gerenciada	Para organizações de qualquer porte, deve-se considerar o uso de uma oferta de DLP gerenciada. Uma oferta de serviços gerenciados inclui especialistas experientes que vão projetar, implantar e cogerenciar o seu programa, garantindo a continuidade da equipe

SAIBA MAIS

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

1207-013-07-01 7/24