proofpoint.

RESUMO DA SOLUÇÃO

Proofpoint Insider Threat Management

Proteja sua organização contra elementos internos arriscados

Principais vantagens

- Proteja-se contra danos financeiros e à marca causados por elementos internos descuidados, maliciosos e comprometidos
- Detecte proativamente comportamentos de risco com visibilidade granular de indicadores comportamentais
- Acelere as investigações com evidências irrefutáveis
- Colabore de forma eficaz com os departamentos de RH e jurídico, bem como outras partes interessadas
- Proteja a privacidade do usuário final e garanta objetividade durante as investigações
- Realize valor rapidamente com facilidade de implantação e um agente de endpoint leve

Este conjunto de soluções faz parte da plataforma integrada Human-Centric Security da Proofpoint, que atende as quatro principais áreas de riscos baseados em pessoas.

Forças de trabalho modernas e distribuídas operam de qualquer lugar e em qualquer parte. Funcionários, terceiros e prestadores de serviços têm acesso a mais dados do que nunca — estejam esses dados em dispositivos, em e-mails ou na nuvem. Mudanças organizacionais, como fusões e aquisições, alienações e reestruturações, causam incertezas que podem desencadear ameaças internas. Tensões geopolíticas e econômicas promovem ciberespionagem por parte de elementos internos.

Essas dinâmicas aumentam o risco de ameaças internas que podem levar a roubo de segredos comerciais e propriedade intelectual, além de fraude, espionagem e sabotagem de sistemas. Todos esses resultados podem causar danos materiais, financeiros, de reputação e estratégicos a uma organização. Para abordar efetivamente o risco interno, as equipes de segurança precisam de uma visão contextual do comportamento arriscado.

O Proofpoint Insider Threat Management (ITM) oferece visibilidade abrangente sobre elementos internos descuidados, maliciosos e comprometidos. Ele ajuda as equipes de segurança a identificar comportamentos arriscados e a investigar incidentes liderados por elementos internos de forma eficiente. O Proofpoint ITM possibilita uma abordagem centrada em pessoas, fornecendo insights granulares sobre o comportamento e as intenções do usuário. Ele permite configurar políticas, triar alertas, caçar ameaças e responder a incidentes em um console centralizado. Com evidências forenses, você pode investigar violações internas de forma rápida e eficiente. Quanto mais rapidamente um incidente é resolvido, menos danos ele pode causar à sua empresa, marca e lucratividade.

Reduza proativamente o risco de segurança

Visão abrangente do risco humano

Ameaças internas podem vir de qualquer lugar, a qualquer momento. Isso as coloca entre as maiores preocupações de cibersegurança para os CISOs do mundo todo. Ao utilizar o Proofpoint Human Risk Explorer (HRE) com Proofpoint ITM, você pode visualizar pontuações de sinais de risco correlacionados para identificar e mitigar proativamente riscos emergentes. O Proofpoint HRE proporciona uma compreensão abrangente do risco humano ao analisar várias dimensões em um único lugar. Isso inclui vulnerabilidades, comportamentos, exposição a ataques, manipulação de dados confidenciais, conscientização sobre segurança e identidade de funcionários individuais.

O Proofpoint HRE também usa insights baseados em dados para fazer recomendações. Por exemplo, se um usuário apresentar um comportamento arriscado, como o download de grandes volumes de informações confidenciais, você pode tomar medidas imediatas. Isso pode incluir a aplicação de controles de segurança mais rigorosos, a atribuição de treinamentos direcionados ou o aumento do monitoramento. Ao abordar primeiro os usuários de alto risco, você pode reduzir significativamente a probabilidade de incidentes e melhorar sua postura geral de risco.

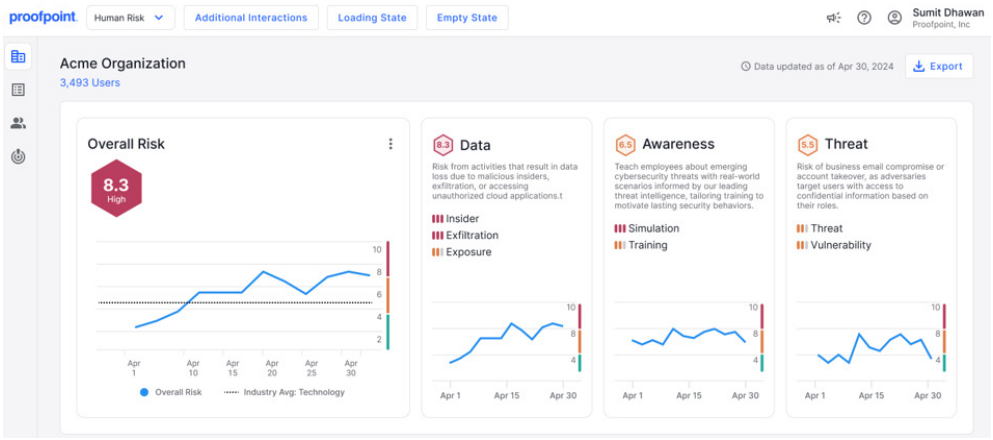

Figura 1. Com o Proofpoint Human Risk Explorer, você pode entender facilmente o risco geral da sua organização e como ele se compara com o risco do setor. Aprofundando-se, você pode obter informações sobre riscos associados a elementos internos, vazamento de dados e exposição de dados.

Abordagem adaptável com base no risco

Para mitigar o risco interno, a maioria das organizações identifica grupos de risco comum. Estes são indivíduos ou equipes cujas funções, comportamentos ou circunstâncias determinam que eles podem representar um risco maior para a integridade de sistemas e dados. Os grupos de risco comum incluem funcionários demissionários, funcionários novos, usuários com acesso privilegiado, executivos, prestadores de serviços, clicadores e outros.

Mas e quanto a usuários arriscados desconhecidos? A maioria das organizações não precisa — e talvez nem deva — coletar telemetria de endpoint sobre todas as atividades de todos os usuários o tempo todo. Em vez disso, a Proofpoint viabiliza uma abordagem adaptável e orientada por riscos. Isso significa uma mudança de políticas estáticas e manuais para políticas que se ajustam automaticamente, em tempo real, com base no comportamento do usuário.

Em uma abordagem adaptável, políticas dinâmicas ajustam o monitoramento do usuário com base em comportamentos, e não em características de risco predeterminadas. Por exemplo, considere um usuário que não faz parte de nenhum grupo de risco. Quando esse usuário começa a copiar dados confidenciais para uma unidade USB, o Proofpoint ITM gera um alerta, acionando um monitoramento elevado. A política de monitoramento elevado captura imagens de tela e metadados detalhados por um determinado período de tempo. O monitoramento ocorre apenas quando há necessidade. Isso ajuda a garantir privacidade e simplifica os alertas para os analistas de segurança. Com uma abordagem adaptável baseada em risco, você economiza tempo e aumenta a precisão da detecção.

Agente de endpoint altamente estável e flexível

Para permitir uma abordagem adaptável baseada em risco, a Proofpoint usa um único agente de endpoint leve que protege contra perda de dados e oferece insights detalhados sobre o comportamento do usuário. Você pode ajustar a quantidade e os tipos de dados coletados para cada usuário ou grupo de usuários. Isso ajuda você a detectar ameaças precocemente e a investigar e responder a alertas de forma eficiente, com menos custos de processamento e armazenamento. O agente em modo de usuário da Proofpoint não entra em conflito com outras soluções e não exige processamento intensivo, garantindo estabilidade, produtividade do usuário e desempenho.

Obtenha insights em tempo real sobre comportamentos de risco

Visibilidade granular sobre usuários de risco

Para ajudar você a detectar comportamentos de risco, a Proofpoint oferece uma visão detalhada da atividade de dados no endpoint. Isso inclui usuários tentando mover dados confidenciais, como ao fazer upload para sites não autorizados ou copiar para pastas de sincronização em nuvem.

Também inclui usuários manipulando tipos de arquivo (por exemplo, alterando extensões de arquivo) ou renomeando arquivos com dados confidenciais. Essas atividades podem indicar que os usuários estão escondendo seus rastros. Juntamente com contexto adicional, como um funcionário pedindo demissão e indo trabalhar para um concorrente, essas atividades podem indicar um usuário de alto risco que precisa ser melhor investigado.

A Proofpoint também oferece visibilidade sobre o uso de aplicativos e navegação na Web. Sinais de comportamento de risco incluem instalar e executar ferramentas não autorizadas, realizar atividades de administração de segurança, adulterar controles de segurança ou fazer download de software malicioso. A Proofpoint oferece insights detalhados para ajudá-lo a responder quem, o quê, onde e quando em relação a atividades arriscadas. Com contexto e insights, você pode discernir melhor a intenção do usuário quando ocorre um comportamento incomum.

Varredura de conteúdo e classificação de dados

Dados confidenciais são expostos quando compartilhados ou transferidos. A Proofpoint verifica dados em movimento e interpreta rótulos de classificação, como os do Microsoft Information Protection (MIP), para garantir que as políticas certas sejam aplicadas.

Ao aproveitar seus investimentos existentes em classificação de dados, você pode identificar informações empresariais confidenciais, como propriedade intelectual, sem criar fluxos de trabalho separados para equipes de segurança e usuários finais. Em alguns casos, porém, talvez não seja possível contar com a classificação de dados para identificar dados regulamentados e dados de clientes. Nessas situações, você pode aproveitar os detectores líderes de mercado da Proofpoint, incluindo correspondência exata de dados (EDM) para dados estruturados e correspondência de documentos indexados (IDM) para conteúdo não estruturado, como propriedade intelectual. Esses métodos avançados melhoram a precisão da detecção e protegem suas informações mais críticas.

Mecanismo de regras flexível e biblioteca de alertas

Com o Proofpoint ITM, você pode criar novas regras e gatilhos adaptados ao seu ambiente. Ou pode adaptar nossos cenários de ameaças predefinidos. Você pode modificar esses cenários por grupos de usuários, aplicativos e datas/horários. Você também pode modificá-los com base na confidencialidade dos dados, rótulos de classificação, fontes e destinos, canais de movimentação e tipos.

ATIVIDADE DE DADOS	ATIVIDADE COMPORTAMENTAL
Alertas relacionados a interação e vazamento de dados, incluindo: • Upload de arquivos para a Web • Cópia de arquivos para unidades USB • Cópia de arquivos para sincronização com nuvem local • Impressão de arquivos • Copiar/colar arquivos/pastas/textos • Atividades em arquivos (renomear, copiar, mover, excluir) • Rastreamento de arquivos (Web para USB, Web para Web etc.) • Download de arquivos da Web • Arquivo enviado como anexo de e-mail • Arquivo baixado de e-mail/endpoint	Alertas relacionados a comportamento, incluindo: • Ocultação de informações • Acesso não autorizado • Desvio de controles de segurança • Comportamento descuidado • Criação de uma porta dos fundos • Violação de direitos autorais • Ferramentas de comunicação não autorizadas • Tarefa administrativa não autorizada • Atividade não autorizada de administrador de banco de dados (DBA) • Preparação de um ataque • Sabotagem de TI • Elevação de privilégios • Roubo de identidade • Atividade suspeita no Git • Uso inaceitável

O Proofpoint ITM também inclui bibliotecas de alertas predefinidos. Estes permitem uma configuração fácil e uma realização de valor mais rápida. Eles podem alertá-lo sobre movimentos de dados ou interações em endpoints arriscados. A Proofpoint também pode alertá-lo sobre uma gama mais ampla de comportamentos de risco de elementos internos. A biblioteca de ameaças internas inclui mais de 150 regras baseadas nas diretrizes do Instituto CERT e em pesquisas comportamentais. Essas regras são uma maneira rápida e fácil de detectar comportamentos arriscados.

Evite o vazamento não autorizado de dados no endpoint

Detectar usuários e atividades de dados arriscados nem sempre é suficiente. Você também deve bloquear o vazamento de dados em tempo real. Com nossa solução, você pode impedir que os usuários interajam com dados confidenciais fora dos termos da política. Isso inclui transferir dados de/para dispositivos USB, sincronizar arquivos com pastas na nuvem, fazer upload para a Web, copiar e colar, imprimir, bem como copiar para dispositivos móveis, cartões SD, compartilhamentos de rede etc. Você também pode impedir que os usuários enviem dados confidenciais por meio de sites de IA generativa (GenAI).

Você pode personalizar sua prevenção com base em usuários, grupos de usuários, grupos de endpoints, nomes de processos, dispositivo USB, número de série do dispositivo USB, fornecedor do dispositivo USB, rótulos de classificação de dados, URL de origem e correspondência de varredura de conteúdo.

Simplifique e acelere as investigações

Console unificado

A Proofpoint ajuda você a simplificar investigações e respostas relacionadas a elementos internos. Para visibilidade multicanal, você pode reunir telemetria de endpoints, e-mail e nuvem em um só lugar. Esse console unificado, conhecido como Data Security Workbench, oferece visualizações claras para ajudá-lo a monitorar atividades, correlacionar alertas, gerenciar investigações, caçar ameaças e coordenar a resposta a incidentes. Essa visão centralizada é uma solução ferramental simplificada que reduz seus custos operacionais.

Os poderosos recursos de pesquisa e filtragem da Proofpoint ajudam você a procurar proativamente por riscos internos com explorações de dados personalizadas. Você pode procurar comportamentos e atividades arriscados que se apliquem à sua organização ou em resposta a riscos novos. Você pode acelerar as investigações com pesquisa assistida por IA usando prompts em linguagem natural. Assim como nossas capacidades de detecção, você pode adaptar um dos modelos predefinidos de exploração de ameaças ou criar o seu próprio.

Triagem de alertas

Nem sempre é fácil investigar e resolver alertas de segurança originados por elementos internos. O processo pode ser longo e oneroso. Além de frequentemente envolver outros departamentos não técnicos, como de RH, de conformidade e jurídico, bem como gerentes de linha de negócios.

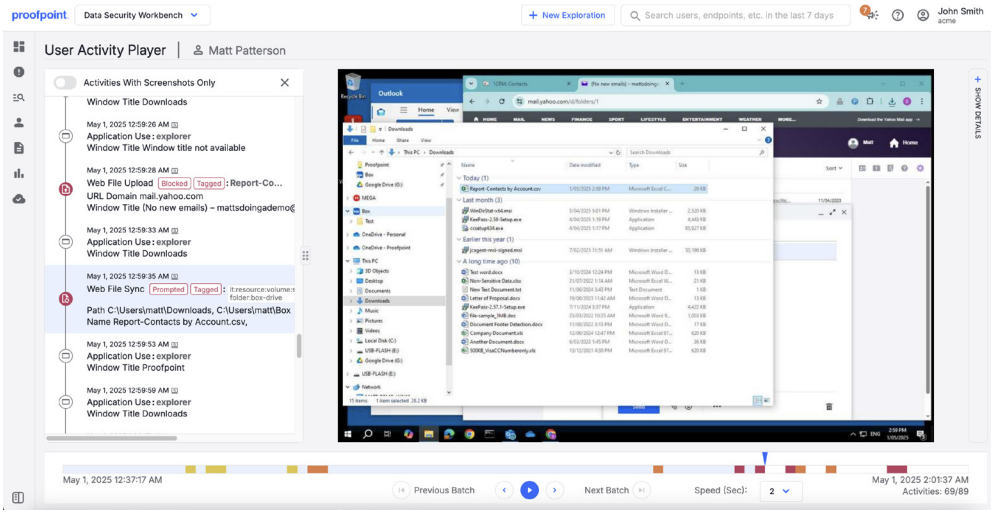

Figura 2. No Data Security Workbench, você pode ver o que aconteceu antes, durante e depois de um incidente interno em uma visão cronológica. Você pode visualizar facilmente capturas de tela para obter contexto adicional e evidências forenses.

Com a Proofpoint, você pode mergulhar profundamente em cada alerta. Você pode ver metadados e insights contextualizados com visualizações cronológicas. As equipes de segurança podem ver quais eventos precisam investigar mais a fundo e quais podem encerrar imediatamente. Insights contextualizados antes, durante e depois de um incidente liderado por elementos internos fornecem contexto sobre as intenções do usuário. Compreender se o usuário é descuidado, malicioso ou comprometido é fundamental para decidir quais serão os próximos passos.

Recursos de fluxo de trabalho e compartilhamento de informações otimizam a colaboração entre equipes multidisciplinares. Você pode exportar registros de atividades arriscadas de múltiplos eventos em formatos de arquivo comuns, como PDF. Essas exportações incluem capturas de tela como evidência e o contexto relacionado. Isso pode ajudar equipes não técnicas, como as de recursos humanos e do departamento jurídico, a interpretar facilmente os dados para análise forense e a tomar decisões informadas.

Captura de tela para evidências de análise forense

Uma imagem vale por mil palavras. O Proofpoint pode capturar imagens de tela da atividade do usuário. Evidências claras e irrefutáveis de comportamento malicioso ou descuidado podem ajudar gerentes e departamentos de RH e jurídico a tomar decisões informadas.

Quando se tem uma infraestrutura de segurança complexa, pode ser necessário manter uma única fonte da verdade entre todos os sistemas. Isso pode envolver a retenção de capturas de tela, trechos ou arquivos para fins investigativos no seu próprio armazenamento. A Proofpoint facilita isso com exportações automáticas de dados para o seu armazenamento próprio e operado no AWS S3, Microsoft Azure e Google Cloud Platform.

Equilibre os controles de privacidade e segurança

Um programa de gerenciamento de risco interno bem-sucedido equilibra a privacidade do usuário e a segurança dos dados em conformidade com regulamentações de privacidade de dados. A Proofpoint adota uma abordagem de privacidade desde a concepção, incorporando a privacidade ao design do produto. Isso ajuda você a proteger os direitos dos funcionários, a cumprir leis de privacidade e a evitar vieses durante as investigações.

Residência de dados e armazenamento

O Proofpoint oferece suporte a data centers em várias regiões. Isso pode ajudar você a cumprir requisitos de privacidade e residência de dados. Atualmente, temos data centers nos Estados Unidos, Canadá, Europa, Emirados Árabes Unidos, Austrália e Japão.

Você pode controlar o armazenamento de dados de endpoint usando agrupamentos de endpoints. Cada agrupamento, ou “realm”, pode ser mapeado para um data center para armazenamento. Isso permite que os clientes separem os dados geograficamente com facilidade.

Controles de acesso baseados em atributos

Você precisa de flexibilidade e controle sobre o acesso aos dados para atender requisitos de privacidade. Com a Proofpoint, você pode assegurar que os analistas de segurança vejam apenas os dados de que precisam. Por exemplo, você pode conceder a um analista acesso apenas aos dados de um usuário específico ou limitar por quanto tempo ele terá acesso.

Anonimização e mascaramento de dados

A anonimização de informações pessoais garante a privacidade do usuário e elimina vieses durante as investigações. A Proofpoint anonimiza os dados coletados dos usuários e não armazena nomes completos nem identificações funcionais dos usuários que causam alertas. Em vez disso, os analistas investigam alertas com base em identificadores exclusivos e anonimizados. Quando a identidade de um usuário precisa ser conhecida, o analista de segurança pode solicitar a desanonimização, que um administrador pode conceder.

O mascaramento de dados também mantém os dados privados. Você pode mascarar dados confidenciais, como informações protegidas de saúde (PHI) e informações de identificação pessoal (PII). Isso torna os dados não identificáveis na interface do usuário. Apenas as pessoas que precisam acessar os dados podem vê-los na íntegra.

Viabilize a agilidade empresarial com uma abordagem moderna

Expanda rapidamente e com facilidade

A Proofpoint é uma solução nativa de nuvem que se dimensiona e se adapta facilmente às necessidades em constante mudança da sua empresa. Ela pode acomodar centenas de milhares de usuários por locatário. Além disso, a solução é implantada rapidamente e é de fácil manutenção. Isso garante uma realização de valor rápida. A Proofpoint também se integra facilmente ao seu ecossistema existente com uma abordagem baseada em API. Webhooks facilitam a assimilação de alertas pelas suas ferramentas de gerenciamento de informações e eventos de segurança (SIEM) e de coordenação, automação e resposta de segurança (SOAR). Isso ajuda você a identificar e a triar incidentes rapidamente.

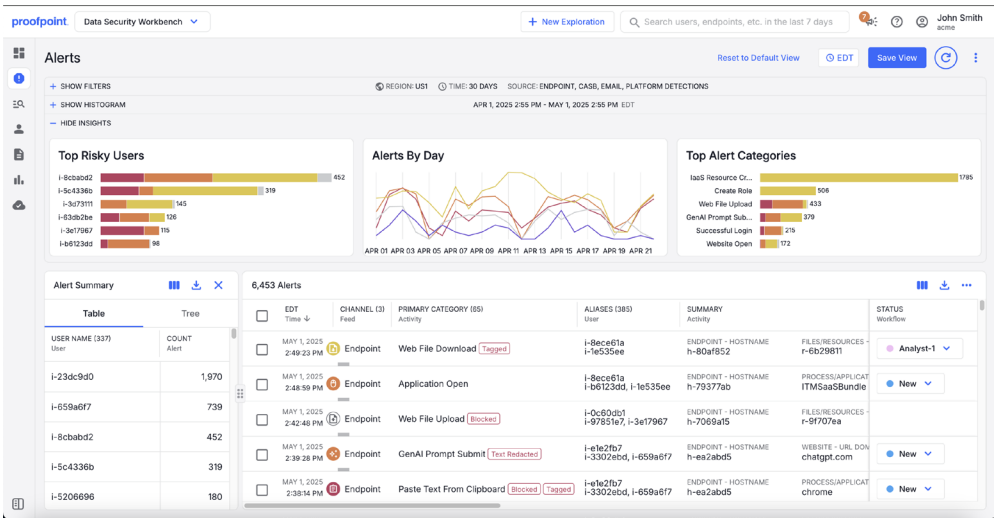

Figura 3. A anonimização protege a identidade do usuário, ajudando a assegurar a privacidade enquanto elimina vieses durante as investigações.

Viabilize mudanças no âmbito de toda a empresa

Mudanças organizacionais podem gerar dúvida e incerteza. Isso cria um ambiente ideal para ameaças internas. Fusões e aquisições, demissões iminentes ou novas tecnologias, como a IA generativa, podem ser gatilhos para que um risco interno se torne uma ameaça interna. As equipes de risco interno precisam de visibilidade e controles para dar suporte às mudanças quando estas ocorrem. A Proofpoint possibilita isso com uma abordagem adaptável baseada em risco, que oferece detecção e prevenção proativas.

Desenvolva e amadureça o seu programa

Um programa eficaz de risco interno é uma combinação de pessoas, processos e tecnologia. A Proofpoint pode ser sua parceira confiável na jornada rumo a um programa bem-sucedido de gerenciamento de risco interno. Nossos serviços Premium oferecem as qualificações necessárias para otimizar seu programa, alavancar seus investimentos em tecnologia e assegurar a adesão e o envolvimento das partes interessadas. Serviços Advisory oferecem aconselhamento estratégico e assistência contínua enquanto você desenvolve e aprimora seu programa. Serviços Applied ajudam você a otimizar seu investimento em tecnologia, dar suporte às suas operações contínuas e amadurecer seu programa de risco interno.

proofpoint.

DESCUBRA A PLATAFORMA PROOFPOINT →