Proofpoint Endpoint DLP e Proofpoint ITM

Tenha proteção centrada em pessoas contra ameaças internas e perda de dados no endpoint

Produtos

- Proofpoint Endpoint Data Loss Prevention
- Proofpoint Insider Threat Management

Principais vantagens

- Reduzir o risco de ameaças internas e perda de dados confidenciais
- Simplificar a resposta a incidentes associados a elementos internos e a violações de políticas
- Acelerar a valorização de programas de prevenção de perda de dados e de ameaças internas

A atual força de trabalho distribuída trabalha de/em qualquer lugar. Funcionários, terceirizados e contratantes têm acesso a mais dados do que nunca — estejam esses dados em seu laptop, no e-mail ou na nuvem. O risco de perda de dados, portanto, nunca esteve tão alto. Contudo, os dados não se perdem sozinhos. Pessoas perdem dados.

Os usuários que vazam dados podem ser categorizados em três tipos: descuidados, maliciosos ou comprometidos. Antes de implementar as políticas apropriadas, você precisa primeiro compreender o contexto por trás do comportamento do usuário. Isso também ajuda a determinar a melhor resposta quando ocorre um incidente associado a elementos internos.

O Proofpoint Endpoint Data Loss Prevention (DLP) e o Proofpoint Insider Threat Management (ITM) oferecem uma abordagem centrada em pessoas para o gerenciamento de ameaças internas e a prevenção de perda de dados no endpoint.

Eles ajudam as equipes de TI e de cibersegurança a:

- Identificar comportamentos arriscados de usuários e interação com dados confidenciais
- Detectar e prevenir incidentes de segurança relacionados a elementos internos e perda de dados de endpoints
- Responder mais rapidamente a incidentes causados por usuários

O Proofpoint Endpoint DLP protege usuários comuns contra perda de dados. O Proofpoint ITM inclui a mesma proteção, mas também defende contra ameaças usuários arriscados oferecendo visibilidade profunda sobre as atividades dos usuários. Ambos os produtos são parte da plataforma Information Protection and Cloud Security. Trata-se de uma plataforma abrangente, contextualizada e nativa de nuvem que oferece visibilidade e insights em vários canais. Ela ajuda você a configurar políticas, triar alertas, caçar ameaças e responder a incidentes em um console centralizado. A plataforma ajuda a evitar perda de dados e a investigar violações internas com rapidez e eficiência. Quanto mais rapidamente um incidente é resolvido, menos danos ele pode causar à sua empresa, marca e lucratividade.

Monitore tanto usuários comuns quanto arriscados

Flexibilidade com um único agente de endpoint

No ambiente competitivo de hoje em dia, você precisa ser capaz de gerenciar ameaças internas e perdas de dados em endpoints. Porém, a maioria das organizações não precisa — e nem deveria — coletar telemetria de endpoints sobre todas as atividades de todos os usuários, o tempo tempo. Em vez disso, recomendamos uma abordagem mais adaptável, com base no risco. Isso significa obter insights sobre algumas atividades de todos os seus usuários e todas as atividades dos usuários mais arriscados.

Para satisfazer essa necessidade, a Proofpoint desenvolveu um agente de endpoint leve que protege contra perda de dados e oferece visibilidade profunda sobre as atividades dos usuários. Com uma simples mudança na configuração da política, você pode ajustar a quantidade e os tipos de dados que coleta de cada usuário ou grupo de usuários. Essa abordagem adaptável ajuda a investigar e a responder a alertas com mais eficiência. E não requer que você colete quantidades absurdas de dados.

Usuários comuns são, tipicamente, usuários habituais da empresa. Considerando seu baixo risco, você pode monitorá-los com o Proofpoint Endpoint DLP para obter insights sobre atividades de dados e o contexto do usuário. Você pode, por exemplo, configurar regras para gerar alertas quando um usuário tentar vazar dados confidenciais copiando-os para uma unidade USB ou fazendo upload para uma pasta de sincronização na nuvem.

Usuários arriscados demandam mais atenção. Tais usuários podem incluir funcionários que estão saindo ou entrando na empresa, contratantes terceirizados, donos de contas privilegiadas e usuários visados, como executivos seniores. Você precisa de insights mais profundos para compreender suas motivações e intenções. Seu monitoramento deve se basear em seus comportamentos ou circunstâncias. O Proofpoint ITM coleta dados detalhados sobre as atividades desses usuários. Esses dados podem proporcionar insights contextuais sobre suas intenções antes, durante e após um evento.

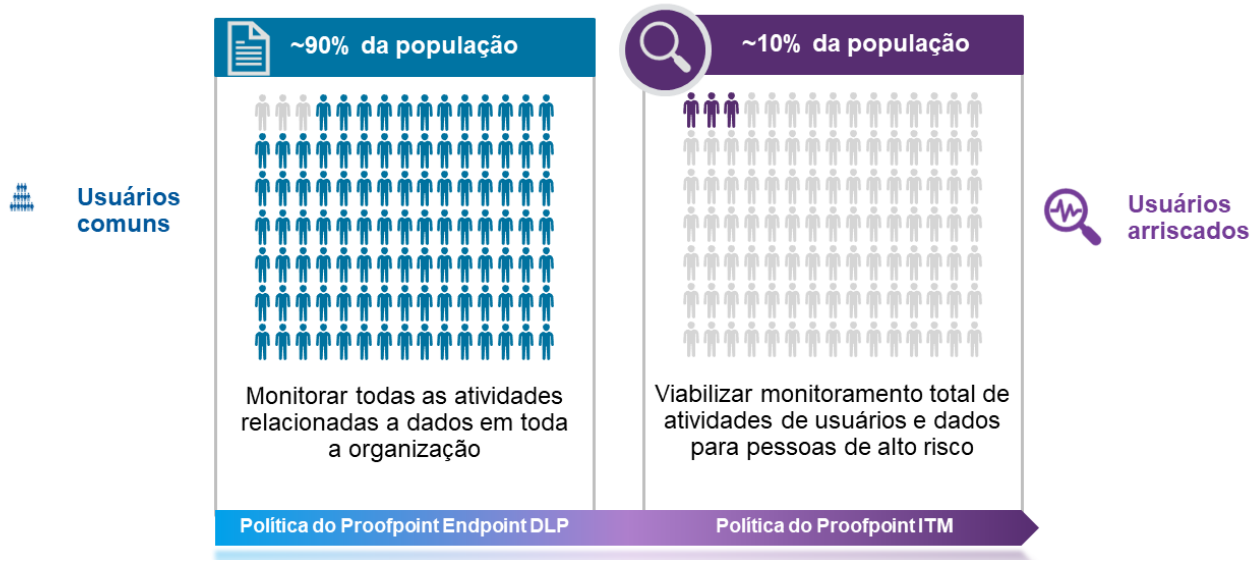

Figura 1. Um único agente leve no endpoint proporciona a flexibilidade de monitorar tanto usuários comuns quanto arriscados.

Os insights detalhados do ITM ajudam a responder “o quem, o quê, o onde e o quando” de atividades arriscadas. Com contexto e insights, você pode discernir melhor a intenção do usuário quando ocorrem perdas de dados e comportamentos contrários à política.

Listas de observação de usuários

Listas de observação inteligentes ajudam você a organizar e a priorizar usuários por tolerância ao risco, com base em seus perfis. Essas listas de observação podem se basear em critérios como o grau de sigilo do cargo do usuário ou dos dados que ele acessa. Elas também podem se basear na vulnerabilidade do usuário a phishing e outras ameaças de engenharia social. Os critérios também podem se basear na localização do usuário, em mudanças na sua situação empregatícia e em outros fatores de recursos humanos e jurídicos.

Ofereça visibilidade e contexto sobre atividades de usuários e dados

Visibilidade sobre usuários comuns e arriscados

Tanto o Proofpoint Endpoint DLP quanto o Proofpoint ITM oferecem visibilidade sobre como os usuários interagem com dados. No entanto, eles diferem nos tipos e na quantidade de dados que coletam.

O Proofpoint Endpoint DLP coleta telemetria sobre interações do usuário com dados no endpoint. Isso inclui observar quando os usuários manipulam tipos de arquivos, como ao alterar a extensão do arquivo ou renomear arquivos que contêm dados confidenciais. Isso também inclui observar quando eles tentam mover dados confidenciais, como ao fazer upload para um site não autorizado ou copiar para uma pasta de sincronização na nuvem.

O Proofpoint ITM oferece uma visão mais completa de atividades baseadas em endpoints para que você possa monitorar usuários arriscados. Além de capturar as interações de dados que o Proofpoint Endpoint DLP captura, ele também oferece visibilidade sobre o uso de aplicativos, capturas de tela de atividades em endpoints e outros comportamentos arriscados. Tais comportamentos podem incluir instalação e execução de ferramentas não autorizadas ou realização de atividades de administração de segurança. Os insights detalhados do ITM ajudam a responder “o quem, o quê, o onde e o quando” de atividades arriscadas. Com contexto e insights, você pode discernir melhor a intenção do usuário quando ocorrem perdas de dados ou comportamentos contrários à política.

A abordagem centrada em pessoas da Proofpoint proporciona uma visibilidade mais granular sobre a interação dos seus usuários com dados confidenciais, em comparação com a de ferramentas de DLP tradicionais. As ferramentas tradicionais de DLP não oferecem visibilidade sobre movimentação de dados, a não ser que uma ação provoque um alerta. Elas também não correlacionam usuários a ações. Devido a essas omissões, é possível que passem despercebidas atividades de dados aparentemente benignas que, no contexto, sejam parte de um comportamento de risco mais amplo.

Varredura de conteúdo e classificação de dados

Você pode identificar dados confidenciais em movimento, quando eles estão sob maior risco. Isso é possibilitado por meio de varredura do conteúdo em movimento e leitura de rótulos de classificação de dados, como os do Microsoft Information Protection.

Ao aproveitar os 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, você talvez não possa contar com a classificação de dados para identificar dados regulamentados e de clientes. Porém, você pode aproveitar os detectores de conteúdo do Proofpoint Cloud App Security Broker (CASB) e do Proofpoint Email DLP, que são comprovados e os melhores do mercado. O Proofpoint Intelligent Classification and Protection (anteriormente chamado Dathena) permite descobrir e classificar dados automaticamente, em tempo real, com inteligência artificial.

Você pode configurar regras de varredura de conteúdo para detectar e evitar comportamentos arriscados. Um alerta será gerado quando o comportamento estiver em desacordo com a política, proporcionando insights decisivos em tempo real. Atividades de usuários arriscados acionam a varredura de conteúdo. Essas atividades podem incluir uploads ou downloads na Web, cópia para unidades USB, compartilhamento ou sincronismo na nuvem e abertura de documentos.

Detecte em tempo real comportamentos de usuários arriscados e interação com dados

Mecanismo de regras flexíveis

Você pode criar regras e gatilhos do zero, conforme as especificidades do seu ambiente. Ou pode adaptar nossos cenários de ameaças predefinidos. Você pode modificar cenários por grupos de usuários, aplicativos e data/hora, bem como por confidencialidade dos dados, rótulos de classificação, origens e destinos, tipos e canais de movimentação. Para oferecer consistência e ajudá-lo a poupar tempo, as regras que você configurar para o ITM podem ser aplicadas a outros canais, como e-mail, nuvem e Web, através do coordenador de política unificada da plataforma.

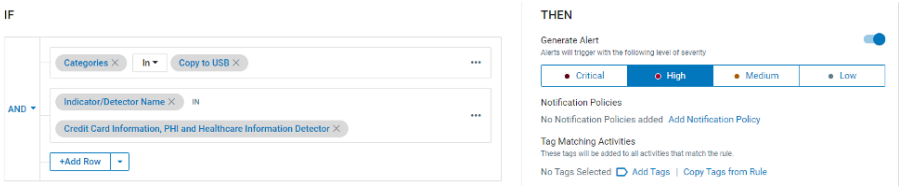

Figura 2. Configure alertas com declarações condicionais simples.

Biblioteca de alertas

O Proofpoint Endpoint DLP e o Proofpoint ITM incluem bibliotecas de alertas prontas. Estas permitem uma configuração fácil e uma valorização rápida. Tanto o Endpoint DLP quanto o Proofpoint ITM podem alertá-lo quanto a interações no endpoint e movimentações de dados arriscadas. O Proofpoint ITM também pode alertar quanto a uma variedade maior de comportamentos arriscados de ameaça interna.

Biblioteca de alertas do Endpoint DLP e do ITM

ATIVIDADE DE DADOS	ATIVIDADE DE USUÁRIO (SOMENTE ITM)
Alertas relacionados a interação e vazamento de dados, inclusive (mais de 40 alertas): • Upload de arquivos para a Web • Cópia de arquivos para dispositivos USB • Cópia de arquivos para sincronização local na nuvem • Impressão de arquivos • Atividades em arquivos (renomear, mover, excluir) • Rastreamento de arquivos (de Web para USB, de Web para Web etc.) • Download de arquivos da Web • Arquivos enviados como anexos de e-mail • Arquivos transferidos por download de e-mail/ endpoint	Alertas relacionados a toda sorte de atividades de usuário no endpoint (mais de 100 alertas): • Ocultação de informações • Acesso não autorizado • Desvio de controles de segurança • Comportamento descuidado • Criação de uma porta dos fundos • Violação de copyright • Ferramentas de comunicação não autorizadas • Tarefa administrativa não autorizada • Atividades de administrador de banco de dados não autorizado (DBA) • Preparação de um ataque • Sabotagem de TI • Elevação de privilégios • Roubo de identidade • Atividades de GIT suspeitas • Uso inaceitável

Os usuários frequentemente desconhecem que seus comportamentos são arriscados. Mas você pode ativar notificações para educá-los.

Evite vazamentos não autorizados de dados pelo endpoint

Detectar atividades de dados e usuários arriscados nem sempre é suficiente. Você também precisa bloquear ativamente os vazamentos de dados em tempo real. Com nossa plataforma, você pode impedir que os usuários interajam com dados confidenciais em desacordo com a política.

Essas interações incluem os seguintes tipos:

- Transferência de e para dispositivos USB
- Sincronização de arquivos com pastas na nuvem
- Upload para sites não autorizados
- Impressão de arquivos

Personalize a 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 em varredura de conteúdo. Você pode estender os recursos de DLP ao e-mail, à nuvem e a aplicativos Web com o restante de nossa plataforma Information Protection and Cloud Security.

Instrua os usuários sobre comportamentos arriscados

Os usuários frequentemente desconhecem que seus comportamentos são arriscados. Mas você pode ativar notificações para educá-los. Por exemplo, quando algum usuário tentar mover arquivos confidenciais, ele será notificado de que essa ação viola a política corporativa. E, em seguida, será solicitado a se justificar. Um link para a política da empresa pode ser acrescentado à notificação. Notificar os funcionários sobre seu comportamento ajuda a mantê-los produtivos, além de reforçar os controles de segurança. As notificações podem ser personalizadas com base no risco, no cargo e na localização do usuário.

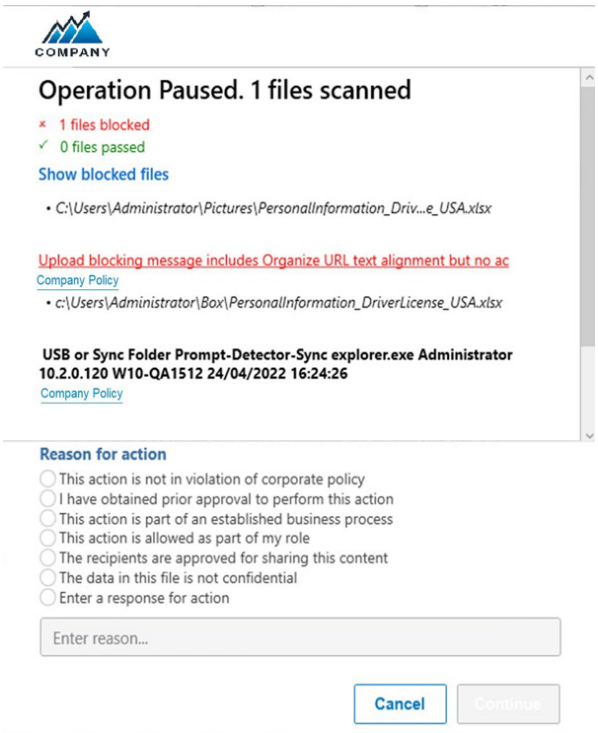

Figura 3. Notifique os usuários finais sobre comportamentos arriscados e peça que eles se justifiquem.

Acelere as investigações e a resposta aos incidentes

Console unificado

O Proofpoint Endpoint DLP e o Proofpoint ITM fazem uso da plataforma Information Protection and Cloud Security. Isso ajuda você a simplificar investigações e respostas a incidentes relacionados a elementos internos. A plataforma coleta telemetria de endpoints, e-mail e nuvem para proporcionar visibilidade sobre múltiplos canais em um único lugar. Seu console unificado oferece visualizações intuitivas para ajudar você a monitorar atividades, correlacionar alertas, gerenciar investigações, caçar ameaças e coordenar a resposta a incidentes.

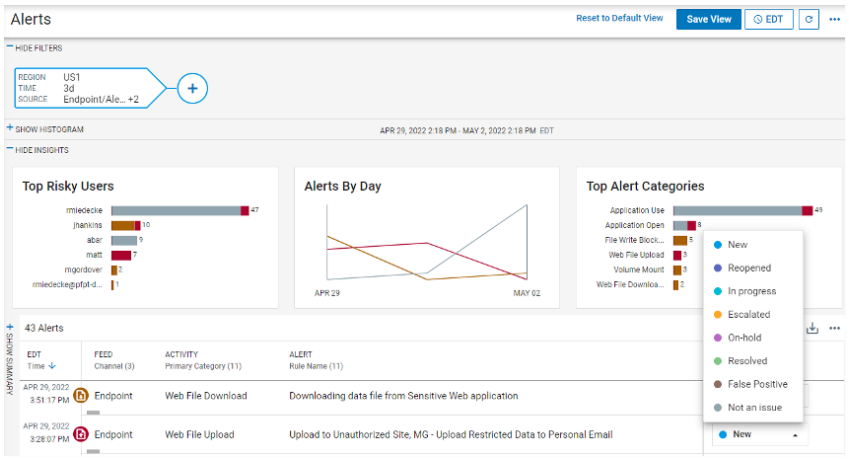

Figura 4. Visualize todos os eventos e alertas em um console unificado.

Caça a ameças por meio de apontar e clicar

Nossos recursos poderosos de pesquisa e filtragem ajudam você a caçar ameaças proativamente, com explorações de dados personalizadas. Você pode pesquisar atividades e comportamentos arriscados que se apliquem à sua organização ou em resposta a novos riscos. Como nossas capacidades de detecção, você pode adaptar um dos modelos prontos de exploração de ameaças ou criar o seu próprio modelo.

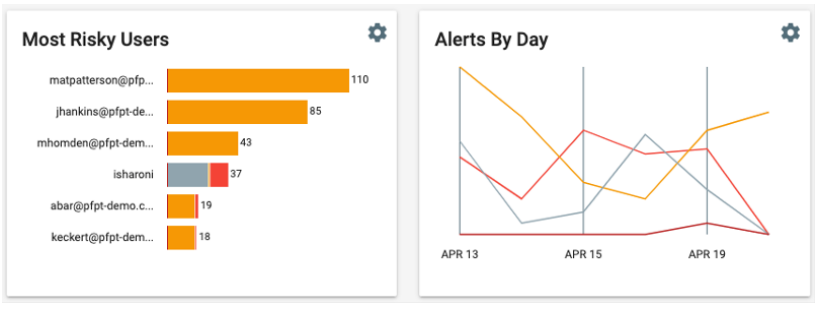

Figura 5. Procure comportamentos potencialmente arriscados ou fora do comum.

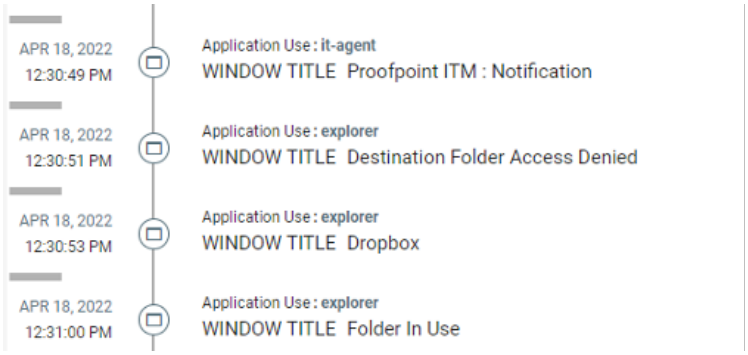

Figura 6. Uma cronologia fácil de visualizar oferece um histórico da interação do usuário com os dados.

Triagem de alertas

Nem sempre é fácil investigar e resolver alertas de segurança causados por elementos internos. Pode ser um processo longo e oneroso. Frequentemente envolve departamentos não técnicos, como os de recursos humanos, de conformidade e jurídico, bem como gerentes de linha de negócios.

Com o Endpoint DLP e o Proofpoint ITM, você pode se aprofundar em cada alerta. Eles permitem que você veja os metadados e obtenha insights contextualizados com visualizações cronológicas. As equipes de segurança podem ver rapidamente quais eventos devem ser mais investigados e quais podem ser encerrados imediatamente. Tags podem ser utilizadas para agrupar e classificar alertas. Isso facilita a coordenação.

Recursos básicos de fluxo de trabalho e compartilhamento de informações simplificam a colaboração entre cargos diversos. Você pode exportar registros de atividades arriscadas de múltiplos eventos em formatos de arquivo comuns, como PDF. Com o Proofpoint ITM, os arquivos PDF exportados pela plataforma incluem evidências na forma de imagens de tela 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 investigações forenses.

Captura de tela de usuários arriscados

Uma imagem vale por mil palavras. O Proofpoint ITM pode capturar imagens de tela das atividades dos usuários. Ter evidências claras e irrefutáveis de comportamentos maliciosos ou descuidados pode ajudar gerentes e departamentos de recursos humanos e jurídicos a tomar decisões informadas.

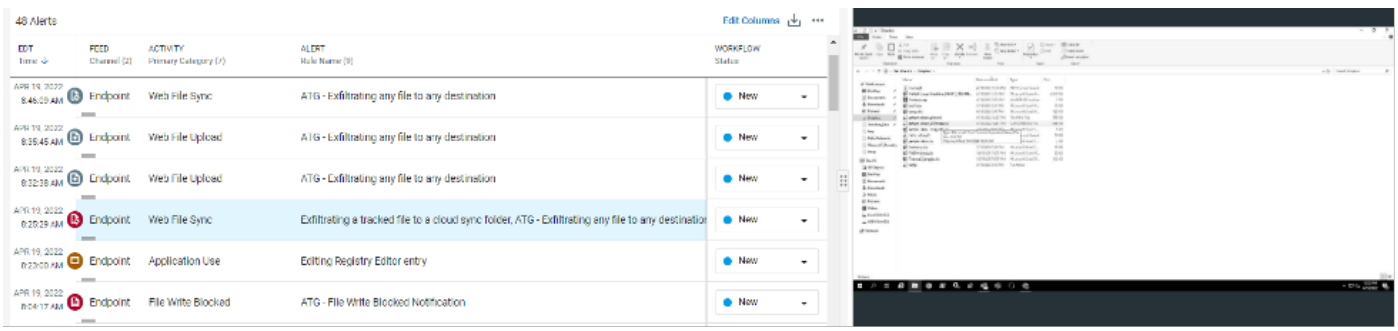

Figura 7. Visualização cronológica de atividades de usuário com capturas de tela do endpoint do usuário.

Fácil de integrar em ambientes de segurança complexos

A plataforma Information Protection and Cloud Security é impulsionada por microsserviços. Webhooks em nossa plataforma tornam fácil para as suas ferramentas de SIEM e SOAR assimilar os alertas do Endpoint DLP e do ITM. Isso ajuda você a identificar e a triar incidentes rapidamente.

Quando se tem uma infraestrutura de segurança complexa, pode ser necessário manter uma única fonte da verdade entre todos os sistemas. Nós facilitamos isso com exportações automáticas de dados do Endpoint DLP e do Proofpoint ITM para o seu armazenamento do AWS S3 próprio, operado por você.

Satisfaça necessidades de privacidade e conformidade

Gerencie a residência e o armazenamento dos dados

Nós oferecemos suporte para data centers multirregionais na plataforma Information Protection and Cloud Security. Isso pode ajudar você a cumprir requisitos de privacidade e residência de dados. Temos atualmente data centers nos Estados Unidos, na Europa, na Austrália e no Japão.

Você pode controlar o armazenamento de dados de endpoints por agrupamento de endpoints. Cada agrupamento, ou "realm", pode ser mapeado para armazenamento em um data center específico. Isso permite aos clientes separar geograficamente os dados. Por exemplo, dados de endpoints dos EUA podem ser gerenciados por um realm dos EUA, sendo enviados para um data center dos EUA.

Cuide da privacidade com controles de acesso baseados em atributos

Você precisa de flexibilidade e controle sobre o acesso aos dados para atender requisitos de privacidade. Com o Endpoint DLP e o Proofpoint ITM, você pode gerenciar o acesso facilmente para assegurar que os analistas de segurança vejam somente os dados relevantes. Você pode, por exemplo, criar políticas granulares e atribuir o acesso de maneira que um analista de segurança baseado na Europa só possa ver dados europeus, e não dados dos Estados Unidos ou da região da Ásia-Pacífico. Você tem a flexibilidade de dar a um analista acesso somente aos dados de um usuário específico ou limitar o tempo durante o qual ele terá acesso a esses dados.

Obtenha visibilidade e contexto sobre múltiplos canais

O Proofpoint Endpoint DLP e o Proofpoint ITM aproveitam plenamente a plataforma Information Protection and Cloud Security. Eles adotam uma abordagem centrada em pessoas ao lidar com conteúdo, comportamentos e ameaças para evitar perda de dados e investigar ameaças. Por meio de um console unificado, você pode obter visibilidade e insights contextualizados sobre múltiplos canais, inclusive endpoints, nuvem, e-mail e Web.

Em um único console, você pode configurar políticas, caçar ameaças e investigar e responder a alertas, seja qual for o canal. Não é necessário alternar de uma ferramenta para outra para realizar cada atividade. Você também pode se aprofundar nos metadados dos alertas. Isso o ajuda a compreender o que aconteceu antes, durante e após um evento. A solução nativa em nuvem também pode ser distribuída rapidamente, o que contribui para uma valorização rápida.

Trabalhe com mais eficiência, poupe um tempo valioso e minimize interrupções dos negócios associadas a perda de dados e ameaças internas com a visibilidade e o contexto proporcionados pela plataforma Information Protection and Cloud Security.

SAIBA MAIS

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