cyberhaven

Prevenção de perda de dados reinventada

As limitações da DLP tradicional

As ferramentas tradicionais de prevenção de perda de dados não protegem dados importantes, bloqueiam a atividade normal e usam tecnologia desatualizada que torna a vida dolorosa para administradores e usuários finais. Questionamos todas as suposições e construímos uma solução DLP baseada em nuvem desde o início para proteger os dados de uma maneira melhor.

Depende muito da inspeção de conteúdo

Confiando inteiramente na análise de conteúdo, as ferramentas DLP não identificam com precisão dados importantes. Também geram alertas falsos positivos que desperdiçam o tempo dos analistas.

Cria uma experiência ruim para os usuários finais

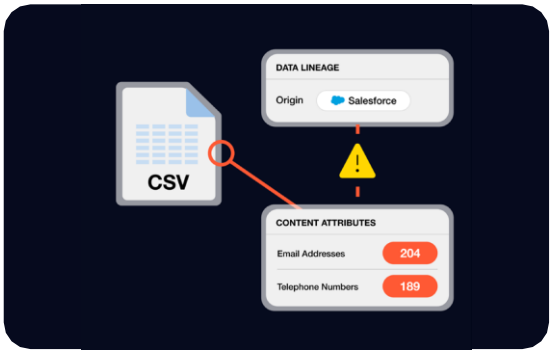
Como os falsos positivos impedem que os usuários façam seu trabalho, os recursos de prevenção das ferramentas DLP geralmente não são ativados. Sua tecnologia desatualizada também torna os computadores mais lentos e quebra o aplicativo na nuvem.

É demorado para implantar e gerenciar

As equipas de segurança precisam investir muito tempo e recursos ajustando as políticas de conteúdo DLP para reduzir os falsos positivos. Ferramentas DLP mais antigas também exigem software e bancos de dados locais.

Cyberhaven redefine prevenção de perda de dados

Identificamos dados importantes que as ferramentas DLP tradicionais não conseguem e protegemos esses dados em todos os canais de exfiltração com um produto e uma política.



Encontre, siga e proteja dados que escapam à análise de conteúdo

Dados importantes geralmente não contêm nenhum padrão de conteúdo reconhecível e, às vezes, nenhum texto. A linhagem de dados nos ajuda a identificar o que outras ferramentas perdem, incluindo:

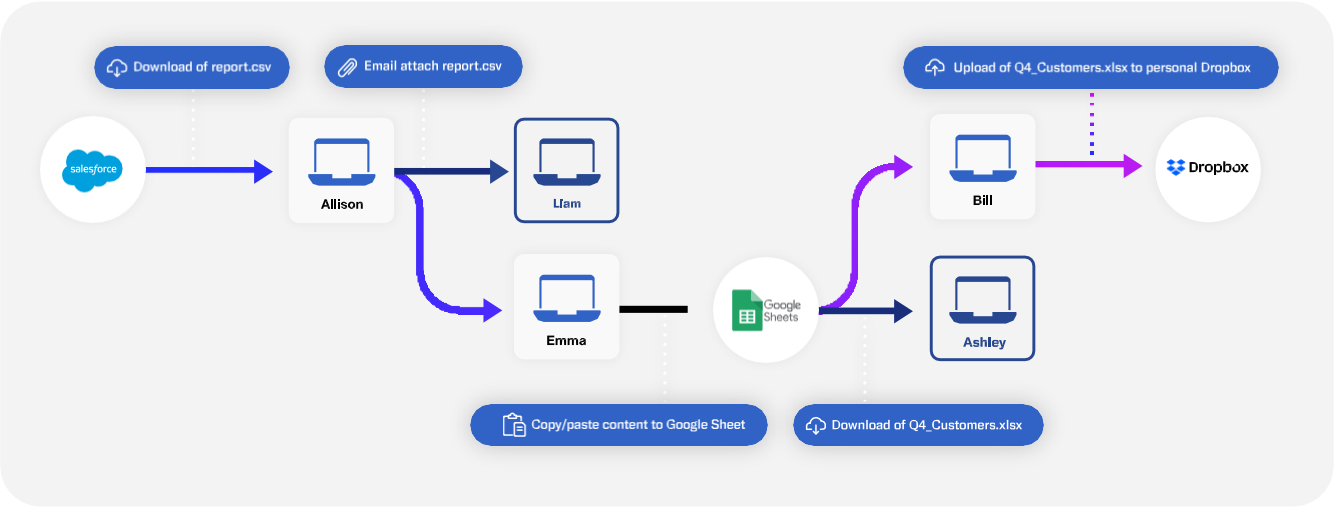
Análise de Conteúdos e dados

Combinamos análise de conteúdo com linhagem de dados – onde os dados se originaram, onde foram e quem os tratou – para identificar melhor quais dados são importantes e o que não são. Nossa abordagem minimiza falsos positivos criados por padrões de conteúdo comuns, como números de telefone e e-mails.

- **Client data**
- **Source code**
- **Product designs**
- **Financials**
- **Recorded meetings**
- **Employee HR data**
- **Architectural plans**
- **And more...**

A magia por trás de Cyberhaven é a linhagem de dados

A linhagem de dados é uma tecnologia que só está disponível na Cyberhaven. Ele rastreia dados desde sua origem e onde quer que vá, fornecendo o contexto que usamos para identificar quais dados são importantes.



Origem

Quer se trate da base de dados de clientes em Snowflake ou do design de produto em Figma, diferentes tipos de dados têm origem em locais diferentes.

Como foi tratado

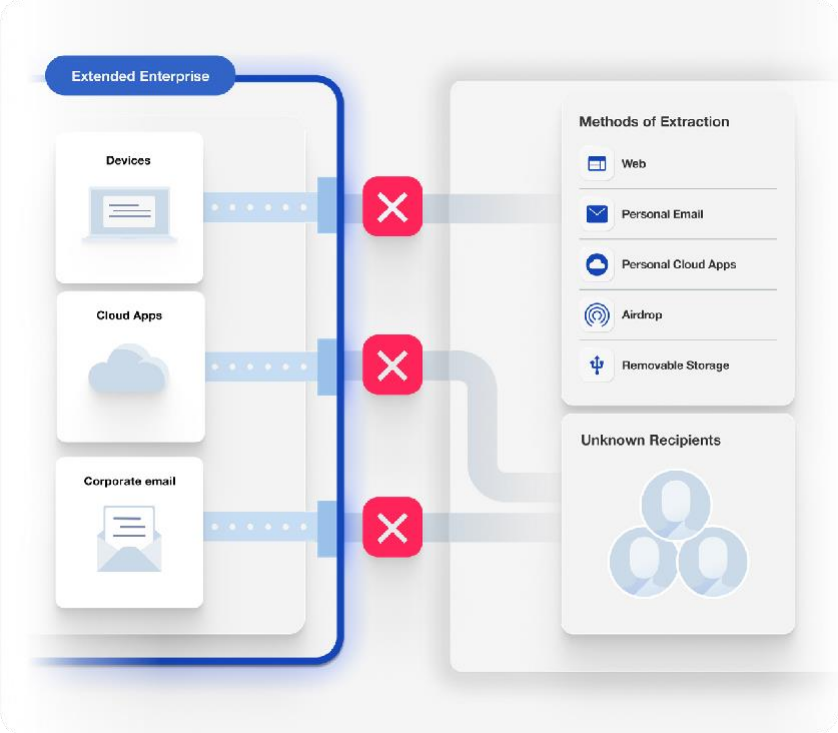
Os dados são movidos de maneiras reconhecíveis, passando pelo site de reunião do conselho no SharePoint ou pela conta de carta de oferta do funcionário no DocuSign.

Quem interagiu

Diferentes funcionários produzem trabalhos diferentes, desde pesquisadores que desenvolvem fórmulas de medicamentos até designers que trabalham em novos produtos.

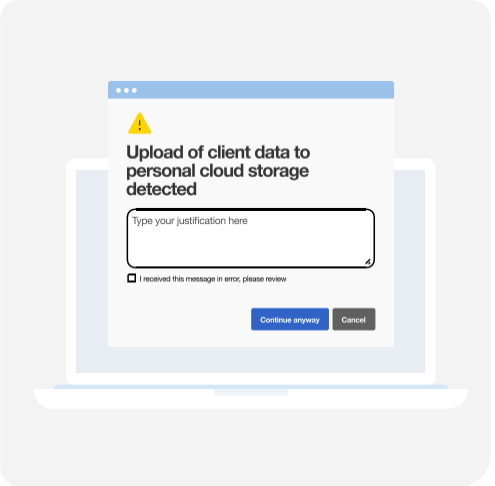
Um produto e uma política que protege todos os canais de exfiltração

O Cyberhaven impede que os dados em sua empresa estendida saiam de seu controle com uma única estrutura de política que se aplica onde quer que seus dados vão.



Ação em tempo real para proteger os dados e educar os usuários sobre o comportamento certo

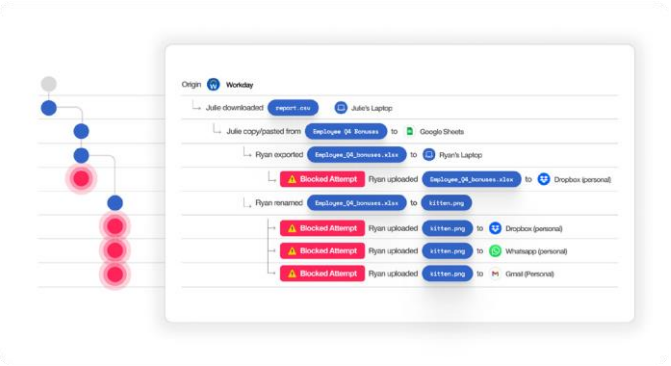
Quando os dados correm o risco de serem exfiltrados, tome medidas instantaneamente e apresente uma mensagem ao usuário educando-o sobre a política da empresa e o comportamento aceitável. Uma base de funcionários instruída leva a 80% menos incidentes e reduz o risco para os dados ao longo do tempo.



- **Bloquear a exfiltração de dados confidenciais**
- **Educar os utilizadores**
- **Permitir substituição com justificação**

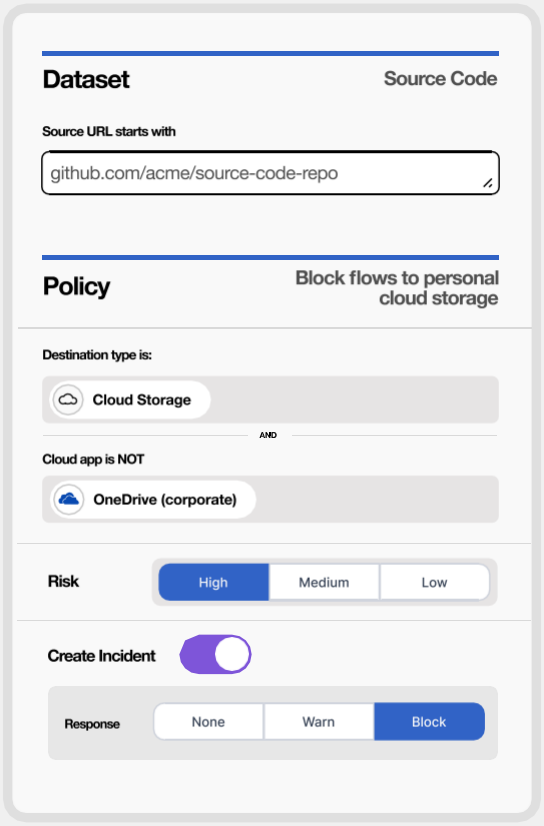
Investigue incidentes com uma imagem completa dos eventos antes da tentativa de exfiltração

O Cyberhaven fornece uma visão de resposta a incidentes, rastreando cada etapa e ação relacionada a um dado que levou a um incidente, incluindo quem lidou com ele e como ele se moveu em toda a organização para que os analistas possam investigar e resolver incidentes mais rapidamente.



Implementar políticas que sejam fáceis de criar e manter

Cyberhaven data lineage makes it possible to define incredibly simple policies and get better results with fewer false positives than policies based on content analysis alone.



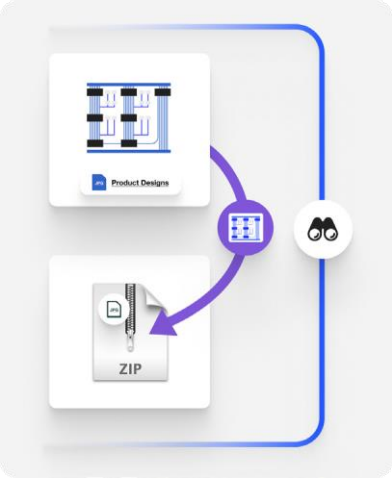
Defina políticas usando um editor de políticas visual intuitivo

A linhagem de dados Cyberhaven torna possível definir políticas incrivelmente simples e obter melhores resultados com menos falsos positivos do que políticas baseadas apenas na análise de conteúdo.

Teste políticas em dados históricos para visualizar e iterar rapidament

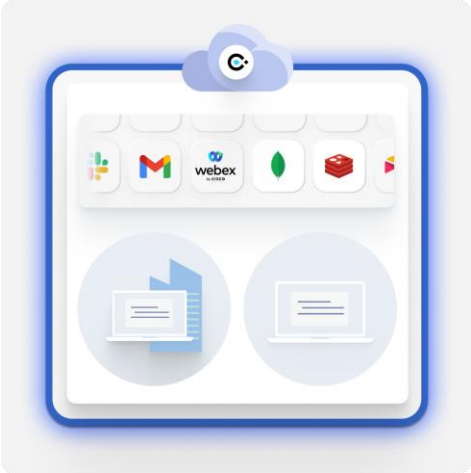
A Cyberhaven mantém um registro completo de cada ação do usuário para cada parte dos dados. Ao editar uma política, você pode ver como ela se aplicaria aos dados históricos para fazer rapidamente quaisquer ajustes sem implantá-la na produção e esperar semanas pelos resultados.

Proteja dados obscurecidos por criptografia e compactação



O Cyberhaven rastreia que tipo de dados foram criptografados ou compactados, portanto, mesmo depois que os dados em si não podem ser digitalizados, você pode rastreá-los e protegê-los da exfiltração.

DLP moderna fornecida a partir da nuvem



O serviço da Cyberhaven é fornecido a partir da nuvem, portanto, não há bancos de dados ou servidores de aplicativos para gerenciar.

Tudo o resto que espera de uma solução DLP

Quando nos propusemos a redefinir o DLP, incluímos os recursos padrão que você espera.

Modelos de políticas prontos para uso

Comece rapidamente com dezenas de políticas prontas para uso para casos de uso comuns e requisitos específicos do setor.

Identificadores de conteúdo padrão e personalizados

Inclui identificadores de conteúdo para padrões PII, PCI e PHI comuns, listas de palavras-chave padrão ou crie seu próprio identificador com RegEx personalizado.

Reconhece rótulos de classificação de terceiros

Reconhece rótulos que produtos de classificação , como o Microsoft AIP, aplicam a arquivos e oferece suporte a rótulos em políticas do Cyberhaven.

Reconhecimento ótico de caracteres (OCR)

Extrai conteúdo de texto em arquivos de imagem e PDFs e oferece suporte ao uso desses dados em políticas baseadas em conteúdo.

Destaque da partida

Os incidentes para políticas baseadas em conteúdo incluem um trecho destacado mostrando o que acionou a política. Essas correspondências são armazenadas na nuvem do cliente.

Captura de tela

Opcionalmente, registre a tela do usuário nos segundos que antecedem um incidente. As capturas de tela são armazenadas na nuvem do cliente.

Integração de diretórios de usuários

Integra-se com serviços de diretório locais e baseados em nuvem para oferecer suporte a políticas granulares baseadas em grupos de usuários e departamentos.

Relatórios e análises

Inclui painéis prontos para uso e um mecanismo de relatórios totalmente personalizável para análises avançadas.

Integração SIEM e APIs

Integra-se nativamente a ferramentas SIEM, como o Splunk, e expõe incidentes por meio de uma API para que você possa adicioná-los a qualquer ferramenta de segurança de terceiros.

Controle de acesso baseado em OLE

Inclui funções padrão prontas para uso ou cria suas próprias funções personalizadas com qualquer combinação de permissões.

Go beyond DLP

Cyberhaven is more than a modern DLP solution, it's a new approach to protecting data from insider threats and accidental exposure we call Data Detection and Response.

The best way to understand the magic of Cyberhaven is to see a live demo.

Contact us at sales@cyberhaven.com to learn more