cyberhaven

Gestão proativa de riscos internos

Até agora, os produtos de risco interno adotaram uma abordagem passiva - alertam-no para ameaças, mas não as detêm, e muitos dos seus alertas são falsos positivos. O Cyberhaven combina consciência de dados e sinais comportamentais para detetar e deter ameaças internas e proteger dados importantes.

Os limites da gestão tradicional do risco de iniciados

Analisa apenas o comportamento, não os dados que estão sendo manipulados

As ferramentas de IRM examinam o comportamento, mas não podem conectá-lo a quais dados estão a ser manipulados ou eventos ao longo do tempo. Eles ativam alertas para coisas que não são arriscadas enquanto perdem muitas ameaças internas reais.

Não é possível intervir e impedir que os dados saiam

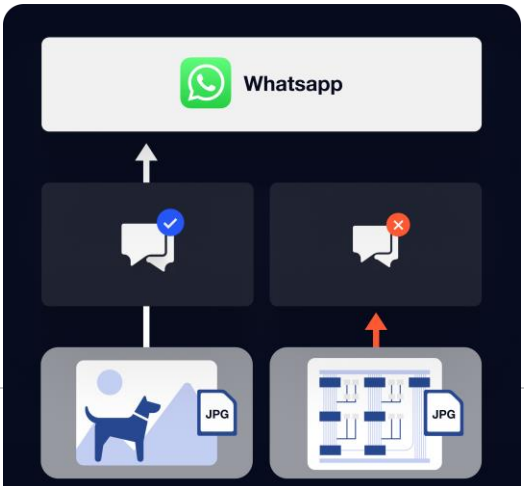
Quando as ferramentas de IRM detetam um utilizador a manipular dados incorretamente, elas apenas enviam um alerta. Eles são projetados para ingerir logs de eventos e analisá-los, mas não têm espaço para agir quando os dados estão em risco.

Envia alertas sem contexto para investigar

Para entender a intenção do usuário, os analistas de segurança que investigam um incidente potencial geralmente precisam procurar detalhes adicionais além do que um alerta de uma ferramenta de IRM lhes fornece.

Cyberhaven redefine gestão de risco interno

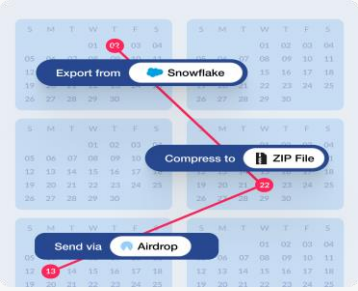
Não nos limitamos a detetar com precisão ameaças internas. A Cyberhaven intervém no momento em que os dados estão em risco para protegê-los, então damos aos analistas de segurança tudo o que eles precisam para investigar rapidamente.



Combine análise comportamental com análise de dados para detetar ameaças com precisão

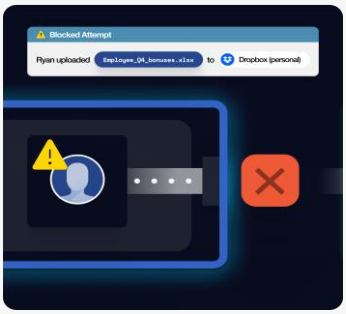
A Cyberhaven distingue precisamente entre um funcionário que executa uma ação com dados corporativos importantes e dados pessoais/sem importância. Esta dimensão adicional torna-nos mais sensíveis a ameaças internas reais, ao mesmo tempo que nos permite ignorar muitos comportamentos do dia-a-dia que não são arriscados.

Identifique ameaças que se desdobram ao longo de semanas ou meses, não apenas horas



Cyberhaven armazena um registro de eventos indefinidamente e podemos correlacionar eventos que ocorrem com semanas ou meses de intervalo, que é quantas ameaças acontecem no mundo real.

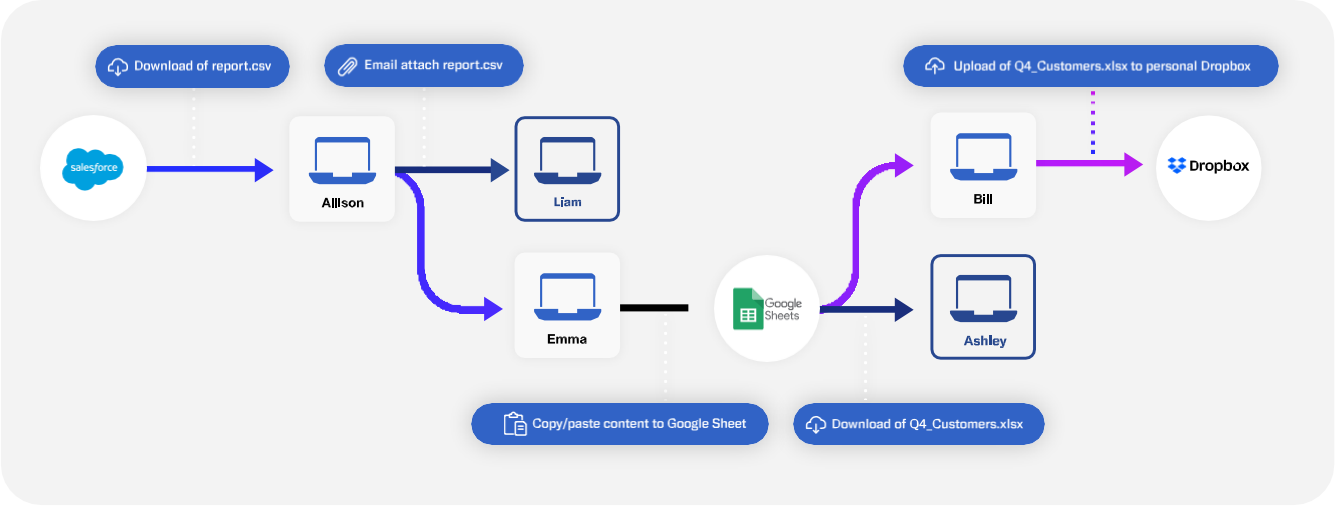
Não apenas detete com precisão as ameaças internas, detenha-as



O Cyberhaven foi criado para tomar medidas imediatas quando há uma ameaça interna em andamento para impedir que alguém pegue dados importantes. Bloqueamos a exfiltração de dados em todos os canais, incluindo nuvem, e-mail, sites, dispositivos de armazenamento removíveis, Apple AirDrop e muito mais.

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

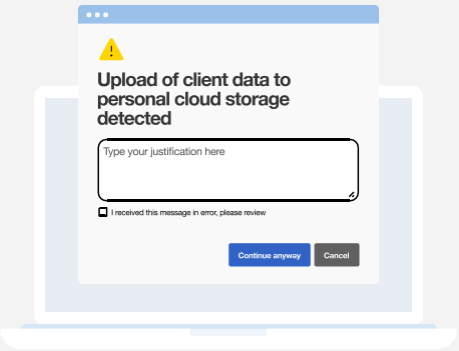
Os dados são movidos de maneiras reconhecíveis, passando pelo site de reunião do conselho no SharePoint ou pela conta de carta de oferta do funcionário no DocuSign.

Quem interagiu com ele

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

Educar os usuários sobre o comportamento apropriado no momento usando pop-ups em tempo real

A melhor segurança começa com uma força de trabalho instruída. Quando um funcionário faz algo arriscado, podemos mostrar uma mensagem pop-up treinando-o no momento, o que é mais eficaz do que notificações por e-mail.



Coletar eventos de nível forense sem acesso físico a um dispositivo

Capturamos remotamente todas as ações do usuário relacionadas a cada dado e as armazenamos com segurança em nossa nuvem para que você possa realizar um investigação pós-incidente sem necessidade de posse física de um dispositivo.

Dê aos analistas o contexto necessário para entender rapidamente a intenção do usuário

O Cyberhaven fornece uma visão de resposta a incidentes rastreando cada etapa e ação relacionada a um dado que leva a um incidente, ajudando a análise a entender rapidamente se o comportamento é devido a descuido ou parte de um padrão de comportamento malicioso.

Tudo o mais que você espera de uma solução de IRM

Quando nos propusemos a redefinir o IRM, incluímos os recursos padrão esperados.

Colete o comportamento do usuário em todas as plataformas

Coleta o comportamento do usuário na nuvem, dispositivos, mensagens, e-mail, aplicativos e muito mais e correlaciona eventos relacionados entre plataformas.

Sinalizar alterações de nome de arquivo ou extensão

Sinaliza quando um usuário altera a extensão ou o nome de um arquivo que contém dados confidenciais e pode bloquear a exfiltração subsequente.

Controlar alterações nas permissões de compartilhamento

Rastreia permissões de compartilhamento para usuários individuais e também links que podem ser acessados por qualquer pessoa na organização ou qualquer pessoa com o link.

Listas de observação de usuários e correção elevada

Adicione usuários a listas de observação e aplique ações de resposta elevadas, como bloquear o upload para destinos não aprovados sem permitir que o usuário final substitua.

Distinga instâncias de aplicativos pessoais e corporativos

Distinga entre a instância corporativa de um aplicativo de nuvem aprovado e uma instância pessoal do mesmo aplicativo.

Integração de diretórios de usuários

Integra-se com serviços de diretório locais e baseados em nuvem para obter detalhes do usuário, como departamento, gerente e data de partida.

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.

Captura de arquivos forenses

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.

Relatórios e análises

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

Controle de acesso baseado em função

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

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.

O Cyberhaven é mais do que uma solução moderna de gerenciamento de risco interno, é uma nova abordagem para proteger os dados contra ameaças internas e exposição acidental que chamamos de Deteção e Resposta de Dados.

Vá além do IRM com o Cyberhaven

Contacte-nos em sales@cyberhaven.com para saber mais.