Folha de dados

Principais motivos para usar a plataforma CipherTrust Data Discovery and Classification da Thales

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Estar em conformidade com a evolução constante das leis e normas de privacidade de dados é um grande desafio. Saber onde residem todos os seus dados confidenciais é uma tarefa contínua, cara e que consome tempo quando se depende exclusivamente de métodos manuais. Minimizar os riscos decorrentes da inevitável dispersão de dados, que se não for controlada, pode se tornar não gerenciável.

A notícia boa é que já há ajuda disponível através da plataforma CipherTrust Data Discovery and Classification com IA, que oferece benefícios consideráveis, incluindo:

- **Segurança aprimorada.** Descobre erros de conformidade para ajudar a reduzir riscos
- **Mais eficiência.** Protegendo seus dados com maior risco em tempo hábil
- **Escalabilidade inerente.** Permite adicionar mais locais às suas varreduras sob demanda à medida que a sua pegada de dados cresce.

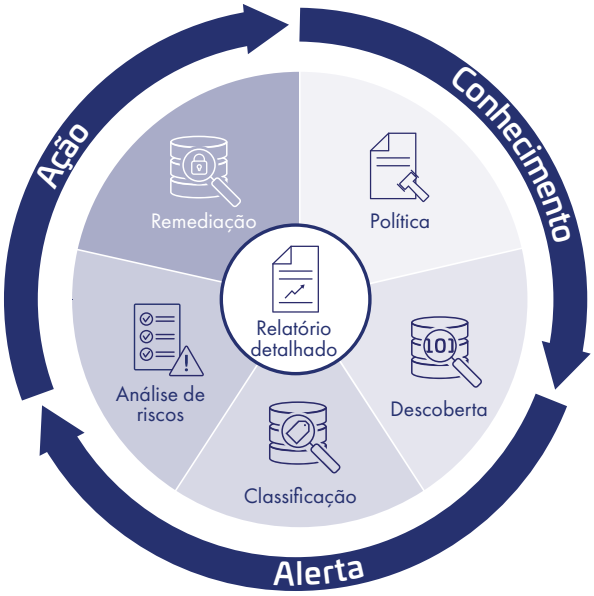
A CipherTrust Data Discovery and Classification ajuda sua empresa a obter visibilidade completa dos seus dados confidenciais com descoberta, classificação e análise de risco de dados eficiente em armazenamentos de dados heterogêneos. Conheça os principais motivos por que é preciso considerar a implementação da CipherTrust Data Discovery and Classification agora.

Segurança aprimorada

Descobre erros de conformidade

Para evitar o risco empresarial significativo da não conformidade com as diversas leis e normas de privacidade de dados, você deve conhecer seus dados confidenciais e saber onde eles residem Com modelos predefinidos para diversas leis de dados, incluindo CCPA, GDPR, HIPPA e PCI DSS, você pode configurar rapidamente varreduras abrangentes usando a CipherTrust Data Discovery and Classification para identificar todos os dados confidenciais em seus repositórios de dados, onde quer que eles residam. A maioria dos erros de conformidade encontrada pode ser corrigida imediatamente usando métodos de proteção de dados como o CipherTrust Transparent Encryption.

Evidencia riscos de segurança



Conhecer os tipos precisos de dados confidenciais em sua infraestrutura e os níveis de risco associados a eles pode ajudar a fornecer o insight aprofundado que você precisa para aplicar camadas adicionais de proteção. A CipherTrust Data Discovery and Classification permite atribuir níveis de confidencialidade específicos para os dados (nenhum, público, interno, privado e restrito) quando você estiver definindo seus armazenamentos de dados e seus perfis de classificação para diferentes tipos de conjuntos de dados sujeitos a conformidade regulamentar, leis de privacidade ou apenas requisitos empresariais internos. Depois de executar as varreduras, as informações podem ser classificadas por níveis de risco, definidos por você, para ajudar a destacar possíveis riscos de segurança, como quando nenhum controle de acesso ou criptografia é aplicado. Você pode tomar as medidas de correção adequadas, sabendo que está eliminando os riscos de segurança da sua empresa.

Identificação de configurações incorretas de políticas

É amplamente reconhecido como boa prática de segurança limitar o acesso a dados, especialmente a dados confidenciais, os quais realmente precisam de controle de acesso. No entanto, uma investigação completa pode levar tempo se for conduzida de forma manual e de acordo com a necessidade, e pode não fornecer todas as evidências de que você precisa em relação aos erros cometidos ao configurar políticas de controle de acesso. É nesta situação que a CipherTrust Data Discovery and Classification pode intervir com suas varreduras abrangentes e relatórios. Analise facilmente os dados do relatório para ver exatamente onde o acesso a dados confidenciais precisa ser controlado com mais rigor ou onde os erros cometidos na configuração dos direitos de acesso precisam ser corrigidos.

Eliminação de dados desnecessários

É muito fácil acabar com uma proliferação descontrolada de dados, o que custa dinheiro em armazenamento e também aumenta o risco de uma violação de dados prejudicial, reter os dados realmente necessários é algo recomendado como parte dos requisitos do PCI DSS. Ao filtrar o relatório gerado por um evento de varredura da CipherTrust Data Discovery and Classification, você pode identificar informações específicas que precisam ser excluídas, arquivadas ou removidas do armazenamento de dados em questão, normalmente porque são duplicadas, obsoletas ou redundantes.

Descoberta de segredos

Quando segredos como tokens, chaves de API, senhas ou nomes de usuário são descobertos por criminosos, eles podem ser usados para invadir os sistemas de TI. A CipherTrust Data Discovery and Classification examina proativamente o código em busca de padrões específicos, tornando os desenvolvedores cientes deles antes que se tornem ameaças à segurança. A Secrets Discovery da Thales é a ferramenta de descoberta de segredos mais abrangente e confiável do mercado atual e ajuda proativamente a impedir a ação de criminosos antes que eles obtenham acesso não autorizado aos seus dados.

Mais eficiência

Com modelos predefinidos para diversas leis de dados, incluindo CCPA, GDPR, HIPPA e PCI DSS, você pode configurar rapidamente varreduras abrangentes usando a CipherTrust Data Discovery and Classification para identificar todos os dados confidenciais em seus repositórios de dados, onde quer que eles residam.

Definição dos fatores de risco

Descobrir dados confidenciais é um grande desafio, assim como saber como reagir com base no risco que a exposição acidental de dados confidenciais representa para sua empresa. Para isso, você precisa de uma base para definir o fator de risco associado a um determinado conjunto de dados. A CipherTrust Data Discovery and Classification ajuda, permitindo que você defina níveis de risco para cada armazenamento de dados e classifique o risco de acordo com os tipos de elementos dos dados mantidos em um repositório de dados. Dessa maneira, você pode executar várias varreduras e combiná-las em um único relatório para análise. Após, é possível classificar o relatório para analisar os fatores de risco e priorizar a ação de proteção adequada.

Coordenação de ações de forma centralizada

Depois que os dados confidenciais forem descobertos e classificados, é importante protegê-los de forma rápida e eficiente, aplicando controles de acesso e mecanismos de proteção de dados adequados. O CipherTrust Data Discovery and Classification é um componente da plataforma CipherTrust Data Security que oferece várias ações de proteção de dados e configurações de controle de acesso através de conectores configuráveis no painel do CipherTrust Manager. Por exemplo, o conector CipherTrust Transparent Encryption, líder de mercado, pode ser configurado para criptografar um armazenamento de dados confidenciais descoberto recentemente, ou determinadas seções de dados podem ser tokenizadas para proteger a privacidade dos dados a partir de um painel de controle.

Reduz o problema de integração

Quando você precisa descobrir os locais dos dados confidenciais que possui, proteger posteriormente os dados identificados e controlar o acesso restrito para reduzir o risco, lidar com vários produtos de diferentes fornecedores que não se integram facilmente ou exigem ferramentas de gerenciamento proprietárias é complicado. A plataforma CipherTrust Data Security oferece tudo o que você precisa em uma única plataforma, apenas um local para descobrir, proteger e controlar. Os dados confidenciais encontrados pela CipherTrust Data Discovery and Classification podem ser protegidos rapidamente (usando criptografia, tokenização ou mascaramento de dados) pelos agentes de proteção de dados CipherTrust apropriados (todos no controle centralizado do CipherTrust Manager). Diferentes grupos do CipherTrust Data Discovery and Classification podem ser atribuídos a diferentes armazenamentos de dados para ajudar a acelerar o tempo necessário para executar e analisar os dados das varreduras. Essa abordagem permite que uma empresa divida atividades complexas em partes gerenciáveis, cada uma realizada por uma equipe diferente de especialistas, ao mesmo tempo em que fornece funcionalidades entre equipes para facilitar um fluxo de solução coerente.

Escalabilidade inerente

Incorporação de fontes novas

À medida que sua pegada de dados se expande e você usa diferentes tipos de armazenamentos de dados, é preciso garantir que seus recursos de descoberta de dados possam localizar e classificar seus dados confidenciais o tempo todo, especialmente porque as normas de armazenamento de dados estão mudando. Não importa se seus dados são estruturados ou não, a CipherTrust Data Discovery and Classification permite que você adicione uma variedade de diferentes armazenamentos de dados (local, rede, banco de dados, big data e nuvem) a qualquer momento para cobrir seus locais de armazenamento mais recentes, de modo que você possa ter certeza de que suas varreduras contínuas estão examinando todos os locais em que seus dados confidenciais residem.

Expansão da capacidade de descoberta

Novos tipos de informações estão surgindo regularmente e precisam ser analisados. Por exemplo, sua pegada de dados pode estar mudando para abranger mais locais de armazenamento em nuvem. Você precisa de uma solução que seja atualizada regularmente para se manter relevante às suas necessidades em constante mudança, bem como aos avanços tecnológicos. A CipherTrust Data Discovery and Classification oferece a possibilidade de criar definições personalizadas para os dados confidenciais que você está tentando encontrar, caso eles não façam parte de uma lei de dados conhecida. Chamamos esse recurso de "InfoTypes personalizados" e ele permite que você encontre praticamente qualquer coisa. Você pode analisar dados mantidos localmente e em armazenamentos de dados em múltiplas nuvens. Uma combinação de agentes de descoberta locais e proxy está disponível para ajudar a simplificar a logística, aumentar o desempenho e dimensionar rapidamente quando necessário.

A CipherTrust Data Discovery and Classification oferece a possibilidade de criar definições personalizadas para os dados confidenciais que você está tentando encontrar, caso eles não façam parte de uma lei de dados conhecida.

Solução para necessidades proprietárias

Você pode ter dados confidenciais que não se enquadram nos modelos predefinidos e que também precisam ser localizados e corrigidos. Talvez você também tenha alguns dados confidenciais (por exemplo, propriedade intelectual) que sejam de propriedade da sua empresa e que precisem ser protegidos. A CipherTrust Data Discovery and Classification oferece a capacidade de adicionar novos perfis de classificação personalizados e editar os perfis de classificação predefinidos que desenvolvemos em seu nome para oferecer o melhor dos dois mundos. Além disso, você pode adicionar novas tags personalizadas para seus tipos de dados que não constam na lista de tags predefinida. É a solução de descoberta e classificação que todas as suas prováveis necessidades precisam agora e no futuro.

Fácil instalação

A Thales simplificou a configuração da CipherTrust Data Discovery and Classification automatizando a instalação por meio da Thales Data Platform (TDP). Um modelo para instalações locais automatiza a implementação de até cinco nodes. Para instalações na nuvem, a configuração é feita com apenas um clique do cliente, e tudo é automaticamente incorporado à nuvem.