Descrição
da solução

CipherTrust Data Discovery and Classification - dados técnicos

Traga agilidade e confiança para seu gerenciamento de dados

cpl.thalesgroup.com

THALES
Building a future we can all trust

Conteúdo

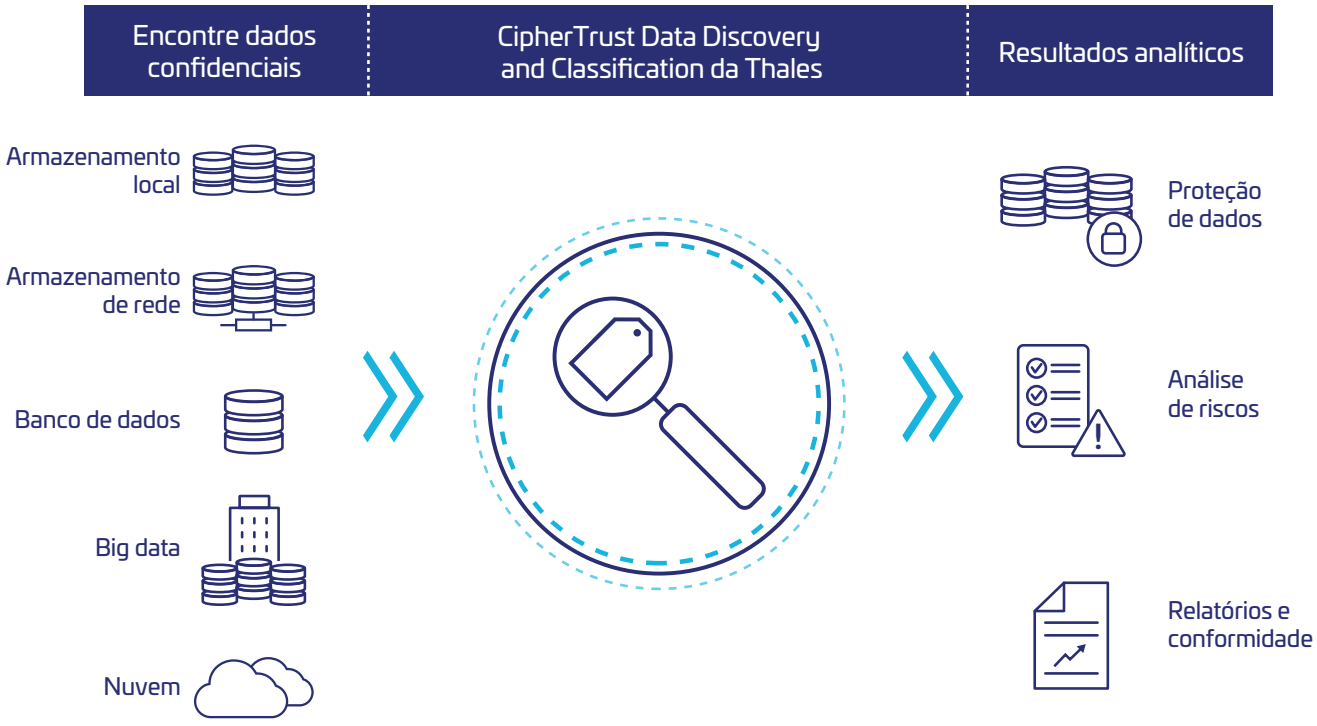
Sumário executivo

O crescimento rápido, muitas vezes exponencial, de dados ano a ano em empresas como a sua torna o gerenciamento eficaz de dados uma proposta extremamente desafiadora. A crescente mudança para o trabalho remoto eleva ainda mais o nível de exigência, com muitas áreas ou volumes de armazenamento de dados que estão fora do controle direto da sua equipe de TI.

Como parte do grupo mais amplo de sua empresa responsável pela conformidade com a privacidade e a segurança dos dados, é de suma importância garantir que nenhuma área vulnerável seja negligenciada ao implementar sua estratégia de proteção de dados. Afinal de contas, uma violação de dados inevitavelmente causará graves interrupções nos negócios, além de grandes multas incorridas pela não conformidade com o fluxo aparentemente interminável de leis e normas de privacidade de dados novas ou aprimoradas. Deixar de se preparar adequadamente definitivamente não é uma opção viável para você.

Um ponto fraco significativo frequentemente observado em implementações típicas de gerenciamento de dados é a falta de visibilidade dos tipos precisos de dados mantidos em vários servidores locais, unidades de rede e, cada vez mais, locais de armazenamento em nuvem. Muitas empresas já sofreram violações, algumas passaram por situações de quase violação e outras estão migrando grandes cargas de trabalho para a nuvem sem entender completamente a natureza fundamental dos dados em si e os riscos de exposição envolvidos, situações que você deve evitar.

Antigamente, o conhecimento da equipe era suficiente e os métodos simples de criptografia "prontos para uso" de fornecedores de banco de dados satisfaziam as necessidades, mas isso não é mais suficiente com a vasta superfície de dados que está amplamente dispersa e cresce a cada segundo. É inevitável que você precise de assistência para assumir o controle e manter sua empresa segura.



A solução CipherTrust Data Discovery and Classification da Thales é...

Uma ferramenta que é significativamente mais eficaz e eficiente do que os métodos manuais para a descoberta de dados, pois examina todos os alvos e não apenas uma amostragem dos dados. Esta ferramenta ajuda a classificar todos os seus dados, ao mesmo tempo em que oferece suporte a todos os principais sistemas operacionais, tipos de armazenamento de dados e dados estruturados e não estruturados que você provavelmente possui. Os processos e as ferramentas existentes são complementados, e não substituídos, proporcionando altos níveis de automação em sua busca por dados confidenciais, onde quer que eles estejam. Por fim, ela pode ajudar você a se tornar mais ágil e ajuda a tomar melhores decisões de gerenciamento de dados.

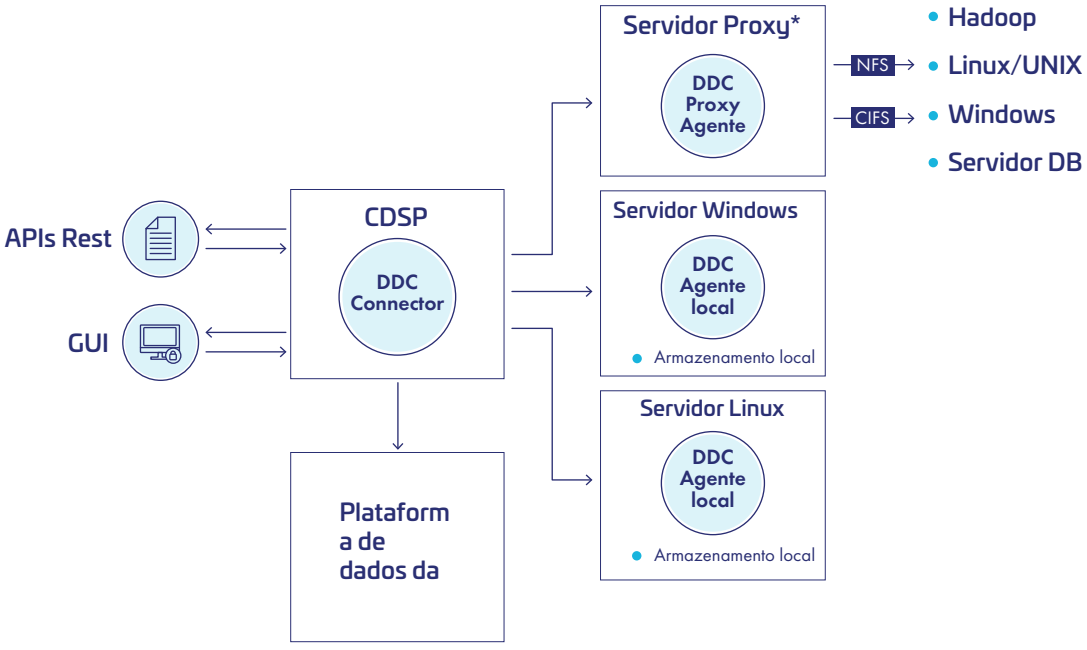
Encontra dados confidenciais que você talvez não saiba que existem em sua empresa, ajudando a eliminar ameaças à continuidade dos seus negócios e reduzir asuperficie de dados

Permite avaliar rapidamente os riscos da falta de conformidade e determinar medidas de proteção adequadas

Garante a proteção dos dados certos, como dados proprietários ou propriedade intelectual, em todos os locais de armazenamento de dados, incluindo na nuvem

O papel da CipherTrust Data Discovery and Classification (DDC)

A DDC oferece uma abordagem mais simplificada, precisa e autônoma (ou automatizada) em comparação com as pesquisas de dados confidenciais que usam métodos manuais. A DDC se destaca dos produtos da concorrência por abranger tipos adicionais de armazenamento de dados, ampliando a gama de dados estruturados e não estruturados que podem ser analisados e, ao mesmo tempo, oferecendo níveis mais altos de precisão ao encontrar dados confidenciais que outras ferramentas geralmente deixam passar.



Os elementos confidenciais encontrados pela DDC não se restringem apenas às leis e normas de privacidade de dados. A fina sintonia que usa infotipos personalizados (definidos por você) facilita a visibilidade de onde os dados confidenciais da sua organização estão presentes. Ao permitir que itens críticos (como dados financeiros internos, segredos comerciais, propriedade intelectual e planos de negócios confidenciais) sejam localizados, seus níveis atuais de proteção e os riscos associados de exposição não intencional podem ser mais bem compreendidos. A flexibilidade considerável vem da execução de várias varreduras simultaneamente, cada uma buscando diferentes tipos de informações (se desejado) para criar uma maneira mais rápida e eficiente de analisar o volume completo de dados em uma ampla variedade de locais de armazenamento. É a capacidade de criar vários perfis de classificação (personalizados quando necessário) que sustenta esses benefícios de desempenho e eficiência que nunca poderiam ser obtidos em um período de tempo comparável usando métodos manuais ou ferramentas menos capazes.

Descobrir dados é apenas uma parte da tarefa em questão, a classificação é igualmente importante, fornecendo uma compreensão aprofundada dos tipos de dados e sua pegada em sua empresa. A DDC não move nem modifica seus dados, apenas resume o que descobre durante as varreduras de maneira não intrusiva.

Você pode ver **exatamente como seus dados estão divididos** entre as categorias dados pessoais, financeiros, de saúde e de identificação nacional, e talvez se surpreenda com a existência de alguns deles. Pelo menos agora você terá uma visão exata de onde eles se encontram para gerenciar adequadamente o risco comercial.

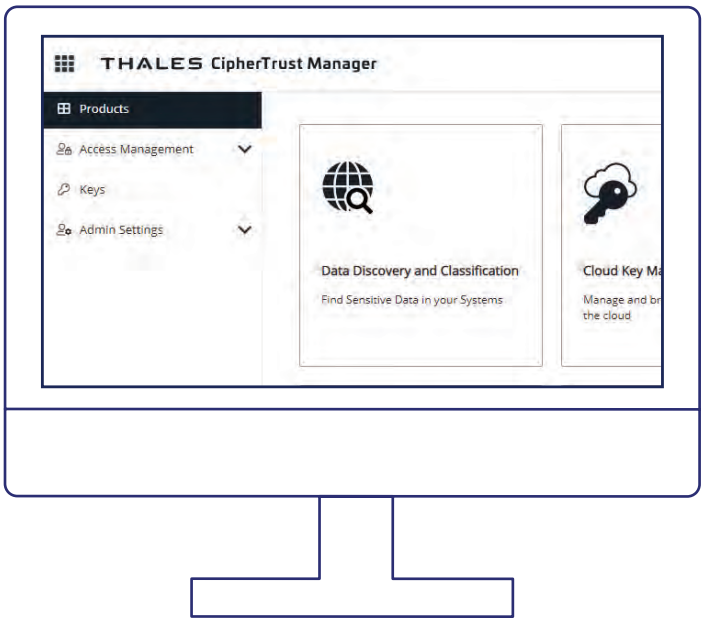
Os insights disponíveis após a realização das varreduras fornecem **orientações importantes** sobre o que você precisa fazer, especialmente em relação à proteção. Você pode escolher quantas varreduras deseja incorporar em um determinado relatório. Cada relatório melhora a visibilidade dos dados, fornecendo informações detalhadas sobre:

- Nomes dos infotipos encontrados com o número de correspondências de dados confidenciais
- O risco associado a cada um dos objetos de dados analisados durante a varredura em questão
- O status de proteção para poder ver o que está protegido e o que não está

A DDC oferece opções para executar varreduras a qualquer momento e repetidas vezes, se você quiser. A ferramenta deve ser usada regularmente para manter sua percepção atualizada, em vez de ser apenas uma atividade eventual. Como os dados estão sempre em um estado de fluxo, a DDC está pronta para transmitir a representação real mais recente do que você tem e do que pode ser necessário fazer para manter sua empresa segura.

A descoberta de segredos é um componente essencial da cibersegurança e da proteção de dados. Isso envolve a identificação de informações confidenciais, como chaves de API, senhas e números da previdência social, que podem ser expostas inadvertidamente em sistemas ou aplicativos.

É difícil ter visibilidade de segredos, pois eles estão em muitos lugares diferentes. Os desenvolvedores geralmente os espalham em repositórios de código, arquivos de configuração e dispositivos pessoais, o que torna a descoberta e o gerenciamento deles um desafio. Sistemas mais antigos, falsos positivos e o erro humano tornam a descoberta de segredos um desafio, especialmente porque os cibercriminosos estão sempre criando novas maneiras de explorar essas vulnerabilidades. 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 utiliza IA para examinar proativamente o código em busca de padrões específicos, tornando os desenvolvedores cientes deles antes que se tornem ameaças à segurança. Secrets Discovery é um recurso da CipherTrust Data Discovery and Classification da Thales e é a ferramenta de descoberta de segredos mais abrangente e confiável do mercado atual. Ele ajuda a interromper proativamente agentes criminosos antes que eles obtenham acesso não autorizado aos seus dados. Embora existam outros provedores para a descoberta de segredos, eles não sabem contar a história completa da descoberta, proteção e controle como a Thales pode. A solução da Thales é abrangente e não requer soluções de envio de peças, como acontece com muitas soluções da concorrência.



Como tudo se encaixa

A DDC é configurada usando uma interface gráfica de usuário (iniciada a partir do console CipherTrust Manager) ou por meio da API REST. Esta solução oferece um fluxo de trabalho simples e intuitivo, permitindo que você defina locais de dados para questionamentos, especifique os tipos de dados que deseja descobrir e decida quando e com que frequência deseja repetir o processo de varredura. As visualizações avançadas fornecem uma visão aprofundada das correspondências de dados confidenciais, do status de proteção associado e da avaliação de risco dos locais dos dados em questão. Os principais recursos estão resumidos nas seções abaixo, fornecendo uma visão bem definida do poder, da flexibilidade e do controle disponíveis para você.

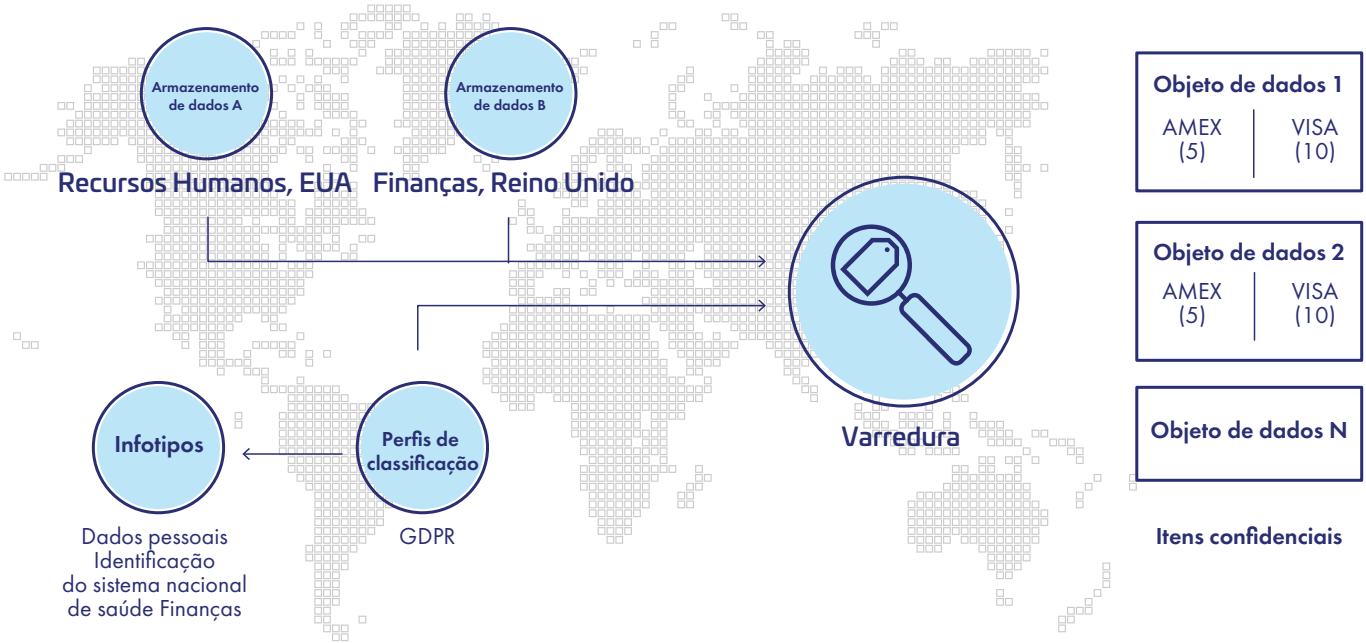
O fluxo de trabalho da DDC é fácil de seguir por meio da interface do usuário. **Três ingredientes principais** ajudam a definir seu ambiente: **armazenamentos de dados, perfis de classificação** e **infotipos**.

Normalmente, você pode adotar a seguinte sequência ao usar a DDC pela primeira vez:

Selecione e configure **armazéns de dados** de interesse – recomendamos primeiro se concentrar nos armazenamentos de dados mais frequentemente acessados e em um caminho selecionado em vez de todo o armazenamento.

Seleciona um ou mais **perfis de classificação** – cria perfis de classificação personalizados, se necessário. Durante esse processo, seleciona um ou mais **infotipos** de interesse - utiliza a capacidade de infotipo personalizado se a lista criada for insuficiente.

Configure e inicie a varredura – considere a possibilidade de selecionar apenas um armazenamento de dados para sua primeira análise, a fim de testar sua configuração.



Armazenamentos de dados

Armazenamento local	Armazenamento local SharePoint sob demanda Servidor Exchange Windows e Linux locais	Armazenamento em rede • Windows Share (CIS/SMB) • Sistema de arquivos Unix (NFS)
Armazenamento em rede	Windows share (CIS/SMB)	
Banco de dados	BM DB2 Microsoft SQL MongoDS MySQL	Oracle DB PostgreSQL SAP HANA SQL
Big data	Hadoop clusters	Teradata
Nuvem	AWS S3 Buckets Azure Blobs e Table Google Workspace (Gmail e Gdrive)	Azure Table Office 365 (Exchange, SharePoint, & OneDrive) SalesForce

Tipos de arquivos suportados

Bancos de dados	Access Dbase	SQLite MSSQL MDF e LDF	**Microsoft Office**	v5 6 95 97 2000	XP 2003 em diante Arquivos Office: Word, Excel, PowerPoint. Access, OutlooK, Other(.pub e .xps)
Imagens	BMP FAX GIF JPG	PDF (integrado) PNG TIF	**Código aberto**	Star Office /Open Office/Libre Office	
Compactados	Bzip2 Gzip (todos os tipos)	TAR ZIP (todos os tipos)	**Padrões abertos**	PDF RTF HTML	XML CSV TXT
Microsoft Backup Archive	Microsoft Binary/ KF				

Tipos de arquivos suportados

APA	Australia Privacy Amendment	**HIPAA**	Health Insurance Portability and Accountability Act
APPI	Act on Protection of Personal Information	**KVKK**	Lei turca de proteção de dados pessoais
CCPA	California Consumer Privacy Act	**LGPD**	Lei Geral de Proteção de Dados (Brasil)
GDPR	Finanças	**NYDFS**	New York State Department of Financial Services
GDPR	General Data Protection Regulation	**PCI DSS**	Payment Card Industry DataSecurity Standard
GDPR	Saúde	**SHIELD**	Privacy Shield Framework
GDPR	Identidade do sistema nacional de saúde	**UK-GDPR**	General Data Protection Regulation (UK)
GDPR	Dados pessoais		

A cobertura de dados estruturados e não estruturados fornecida pela DDC é atualizada frequentemente com novos recursos. Confira as especificações mais recentes aqui.

Os principais perfis de classificação estão integrados e alinhados com as principais leis e regulamentações de dados, tanto regionais quanto globais. É possível fazer alterações nesses perfis ou adicionar perfis totalmente novos, se necessário. Vários atalhos são fornecidos em termos de edição e cópia para que você possa criar e testar rapidamente seus próprios perfis. Há total flexibilidade na especificação de vários parâmetros, incluindo níveis de sensibilidade e infotipos.

Tipos de arquivos suportados		
Nenhum	**Público**	**Interno**
Privado	**Restrito**	

Categorização de dados confidenciais

A DDC já vem com vários infotipos, mais de 250, abrangendo a grande maioria das leis e normas regionais e globais de privacidade de dados. Quando um modelo de perfil de classificação já existente é selecionado, o subconjunto apropriado de infotipos é adicionado automaticamente. Você pode modificar ou ampliar essa lista criando seus próprios infotipos personalizados, permitindo que sejam definidas regras que descrevam precisamente como o mecanismo de varredura deve procurar as cadeias de dados em questão. O acesso total aos grupos e categorias está disponível como parte da definição, de modo que as correspondências de dados possam ser exibidas nas seções apropriadas dos resultados da varredura.

Categorias de infotipos (já no produto)		
Finanças	Cartões de crédito/débito	Informações de conta bancária
Dados pessoais	E-mails Credenciais de login Número do cartão Etnia Número da placa Número de registro Número do passaporte Data de nascimento Endereço MAC	Lista de endereços Número do telefone Sexo Religião Endereço IP Número do celular Nome Profanidade
Saúde	Informações de saúde do paciente	
Identidade do sistema nacional de saúde	Identificação pessoal	
Segredos	Descoberta de segredos	

Uso de agente para descoberta

A análise detalhada dos dados é realizada por agentes de descoberta que executam a varredura e informam os resultados ao DDC Connector para análise e processamento. Existem dois tipos de agentes: local e proxy. Normalmente, você instalaria agentes locais em locais de armazenamento de dados (para os quais você tem os direitos de acesso apropriados) para garantir que os dados nunca saiam do servidor por motivos de segurança ou desempenho. Por outro lado, os agentes proxy são usados para armazenamentos de dados em rede ou remotos, nos quais um servidor proxy separado hospeda o agente.

Tipo de agente	Prós	Contras
Local	Varredura mais rápida Os dados permanecem locais Não é preciso credencial	Tempo de implementação mais longo Gerenciamento mais complexo Suporta apenas armazenamentos de dados locais
Proxy	Implementação e dimensionamento mais rápidos Capacidade de fazer varredura de múltiplos armazenamentos de dados Suporte a vários tipos de armazenamentos de dados Nenhum recurso consumido no host de destino	Dados enviados pela rede para o agente antes da varredura Aumento da carga da rede e da super'ficie de dados O ideal é que estejam localizados na mesma LAN virtual (VLAN)

Benefícios comuns de ambos os tipos de agentes:

Um **número ilimitado** de agentes disponíveis para implementação sem custo extra, pois o licenciamento é baseado no volume de dados novos analisados

É possível executar várias subvarreduras para reduzir o tempo necessário para a varredura geral

A criptografia TLS está disponível para todas as comunicações entre armazenamentos de dados e agentes para proteger dados confidenciais contra escutas

Os dados de origem não são afetados, pois os agentes acessam apenas uma cópia temporária dos dados na memória interna durante a varredura

Os dados confidenciais não são armazenados durante o processo, pois é enviado apenas um resumo dos resultados da varredura para o DDC Connector

As varreduras **continuam** e registram resultados mesmo quando a conexão com o DDC Connector for cortada

Com seus agentes instalados, você pode começar a pensar sobre o que e como deseja fazer a varredura. Oferecemos uma grande flexibilidade na forma como as varreduras são configuradas, gerenciadas e operadas. Os parâmetros importantes configuráveis para cada varredura de forma independente incluem:

- Nome (até 64 caracteres)
- Descrição (até 250 caracteres)
- Um ou mais armazenamentos de dados (onde fazer a varredura)
- Um ou mais perfis de classificação (o que procurar)
- Operação manual ou programada (quando ativar)

Após a conclusão de uma determinada varredura, ela é adicionada a uma lista de todas as varreduras que foram realizadas. Após, utiliza-se a ferramenta de relatório para visualizar os resultados detalhados da varredura. Dependendo do que for encontrado, você poderá fazer alterações na configuração da varredura e executá-la novamente, o que é vantajoso ao trabalhar em diferentes armazenamentos de dados ou em novos tipos de normas de conformidade pela primeira vez.

Análise de resultados da varredura

Os resultados de varreduras anteriores e novas estão disponíveis para uso com a ferramenta de relatório integrada. São oferecidas três principais exibições para relatórios de varredura:

- **Varreduras**
- **Armazenamentos de dados**
- **Objeto de dados**

Antes que as informações detalhadas estejam disponíveis, é gerado um relatório que agrega os resultados de uma ou mais varreduras de sucesso. Muitas vezes, por motivos logísticos, de segurança ou de desempenho, você pode querer usar várias varreduras (cada uma procurando diferentes tipos de dados regulamentados) para analisar todo o seu espaço de dados. Com nossa abordagem flexível, você ainda pode fazer isso e ajustar cada varredura conforme necessário, usando várias iterações, antes de gerar um relatório final que possa representar o status atual de todos os seus dados. Também é fácil entender sua postura organizacional do ponto de vista de um único regulamento.

Cada guia do módulo de relatório oferece uma visão de aspectos ligeiramente diferentes dos seus dados - todas, porém, têm o objetivo comum de ajudar a identificar rapidamente quaisquer dados confidenciais em risco.

Visualização de varreduras

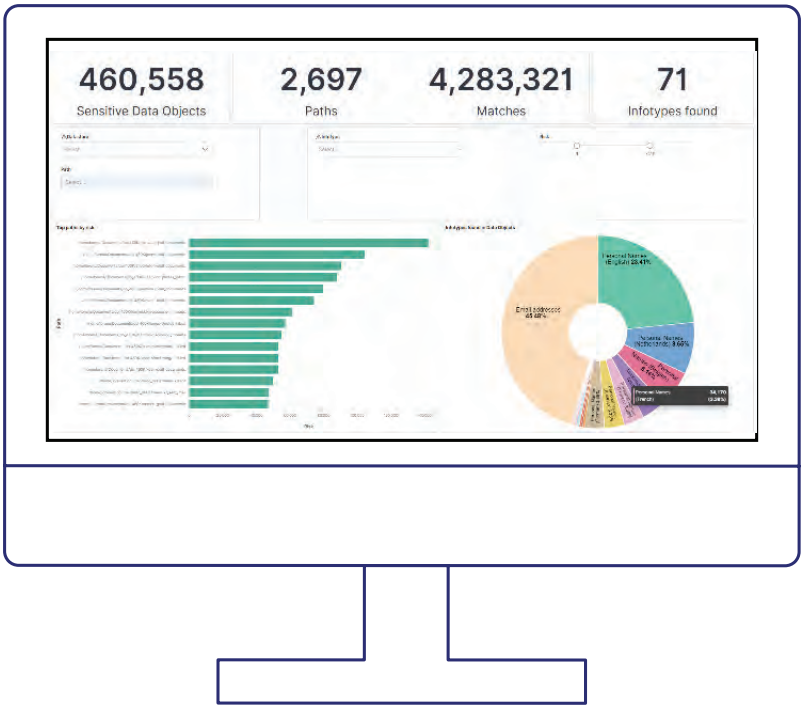
Fornece uma visão de varredura agregada de alto nível dos infotipos encontrados (divididos por porcentagem em cada categoria presente), juntamente com três outros gráficos que representam a presença de objetos de dados confidenciais em termos de distribuição de categorias, tipos de conteúdo e tipos de arquivo em questão.

Visualização dos armazenamentos de dados

Fornece uma lista dos armazenamentos de dados com detalhes que incluem risco, nível de confidencialidade, infotipos encontrados e número de objetos de dados confidenciais presentes em cada armazenamento de dados. Isso proporciona um meio rápido de avaliar em alto nível se os dados confidenciais estão ou não em risco e quais armazenamentos de dados estão envolvidos.

Visualização de objeto de dados

Fornece uma lista detalhada de todos os objetos de dados verificados que contêm dados confidenciais classificados em ordem decrescente de risco de exposição Para cada objeto de dados confidenciais em questão, é possível ver onde ele está localizado, o armazenamento de dados no qual ele reside e os nomes individuais e as correspondências de dados para todos os infotipos associados encontrados. As informações sobre o status da correção também estão presentes, o que proporciona uma visão mais profunda dos seus dados confidenciais, confirmando se uma política de criptografia está ativa ou não. Nenhum dado confidencial é armazenado como parte do processo de relatório.



Exportação de dados

Além de visualizar objetos usando a ferramenta de relatório integrada, você também pode exportar dados em um formato NDJSON para análise por uma ferramenta de relatório externa, como a da Elastic usada nas demonstrações da Thales.

Motivos da nossa escolha de tipo de arquitetura

Plataforma única e integrada

Decidimos fazer da DDC uma parte integrante da Plataforma CipherTrust Data Security da Thales CipherTrust porque, em nossa experiência, a descoberta de dados é a base de qualquer estratégia eficaz de segurança de dados. Essa abordagem de plataforma integrada permite que o CipherTrust Manager atue como o console de gerenciamento central para vários conectores, incluindo descoberta de dados, criptografia transparente e tokenização. Se já estiver usando o CTE, você estará familiarizado com o console e se beneficiará da consistência na implementação de tarefas comuns de gerenciamento, como grupos de usuários, políticas de dados, controle de acesso e login.

Correspondência precisa de padrões

A Thales realizou uma extensa pesquisa para determinar a melhor tecnologia de descoberta de dados do mercado. Após muitas pesquisas e testes de bancada, a equipe percebeu uma diferença significativa ao usar a GLASS TechnologyTM em vez da Regex. A GLASS é uma tecnologia proprietária líder de mercado da Ground Labs (um parceiro tecnológico da Thales) para definir e combinar padrões simples e complexos de dados em escala, em oposição a uma linguagem de código de desenvolvedor não criada especificamente para esse fim. Ela foi projetada desde o início com o objetivo expresso de encontrar padrões de dados em conjuntos de dados modernos em cenários de armazenamentos de dados estruturados e não estruturados.

Descoberta de alto desempenho

Um objetivo importante era fornecer um mecanismo de descoberta altamente eficiente e preciso. A maioria das soluções de descoberta de dados disponíveis atualmente usa a linguagem de expressão regular (Regex) (originada na década de 1950) para pesquisar padrões dentro de sequências de texto. Essa abordagem requer amplo conhecimento do desenvolvedor para ser implementada e a sintaxe não se baseia na gramática inglesa. O maior inimigo do Regex é o desempenho, à medida que a simultaneidade e a complexidade dos padrões aumentam, mais lento é o desempenho obtido. O padrão Regex tem limites para os padrões que pode corresponder com precisão, o que o torna longe de ser ideal no mundo moderno, onde há centenas de regulamentações de privacidade diferentes e uma ampla gama de problemas de gerenciamento de dados a serem abordados.

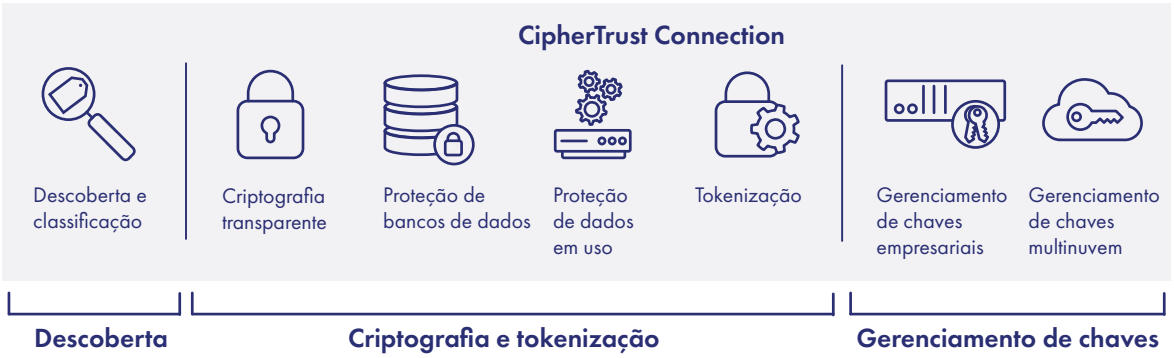
Recursos fáceis de personalização

O suporte à personalização foi outro critério importante para complementar os modelos abrangentes incluídos. Para atender às necessidades proprietárias, os padrões de dados GLASS podem ser escritos por não desenvolvedores usando uma gramática no estilo inglês para expressar como um dado ou padrão existe. A análise detalhada mostra que ele superou todas as limitações importantes do Regex para técnicas de correspondência de padrões, especialmente sua capacidade de operar em várias plataformas e ambientes de nuvem, além de ser muito econômico em termos de sobrecarga da CPU. Isso fez do GLASS um componente central ideal para ser incorporado à DDC, funcionando de forma eficiente e transparente como parte da plataforma CipherTrust na identificação e proteção de dados críticos.

Modelo de licenciamento flexível

Um modelo de consumo baseado no total de dados analisados é usado para licenciar a DDC, proporcionando um alinhamento próximo com muitos modelos de assinatura de nuvem e oferecendo um número ilimitado de agentes de descoberta sem incorrer em taxas adicionais. Isso facilita muito o acesso de todas as suas equipes aos recursos de descoberta de dados, sendo que a única decisão real a ser tomada é a capacidade geral de descoberta de dados necessária para a sua empresa. Uma nova varredura de dados antigos não é subtraída da sua franquia de uso de dados restante, apenas os novos dados analisados são contabilizados.

Plataforma CipherTrust Data Security da Thales



Segurança em primeiro lugar

Como uma empresa de segurança líder de mercado, é óbvio que criamos e implementamos soluções seguras. A DDC não é exceção, com grande ênfase em garantir que nenhum dado confidencial seja armazenado ou fique vulnerável à exposição.

- Garante que todos os dados que fluem entre seus armazenamentos de dados e agentes sejam protegidos usando criptografia robusta
- Fornece controles de acesso granulares para que você possa adaptar a solução às suas necessidades exatas

Integração com outras soluções

Plataforma CipherTrust DataSecurity

A DDC foi otimizada para ser usada como parte da plataforma CipherTrust Data Security, um conjunto integrado de produtos e soluções de segurança centrados em dados que unificam a descoberta, proteção e controle de dados em uma única plataforma. Consequentemente, você pode atender a todas as necessidades de proteção de dados usando uma única plataforma de um único provedor, neste caso a Thales. Isso lhe oferece um conjunto completo de recursos de proteção de dados, incluindo gerenciamento de chaves, controle de acesso do usuário, criptografia no nível do arquivo, criptografia na camada de aplicativos, criptografia de banco de dados, criptografia com preservação de formato, tokenização e mascaramento de dados.

CipherTrust Manager

Todos os componentes utilizam o CipherTrust Manager como console de gerenciamento, oferecendo gerenciamento central de chaves de criptografia, controle de acesso granular e configuração de políticas de segurança. Uma das principais vantagens é que nossa solução foi projetada para proteger seus dados onde quer que eles residam, no local ou na nuvem, e qualquer que seja o mecanismo de armazenamento em uso, como arquivos, bancos de dados, big data ou containers. Por fim, você acabará exigindo menos recursos dedicados às operações de segurança de dados, cumprirá suas obrigações de conformidade com mais confiança e reduzirá o risco comercial para a sua empresa.

Também é possível implementar a DDC com outras ferramentas de proteção de dados de terceiros, como as que oferecem suporte à criptografia ou tokenização de dados. Nossa solução não é intrusiva e complementa as ferramentas que você já possui, em vez de substituí-las. No entanto, o CipherTrust Manager ainda é necessário, pois fornece o único método para iniciar o recurso de descoberta de dados e

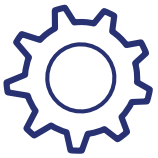
gerenciar as licenças necessárias para sua operação, juntamente com as chaves necessárias para criptografar dados confidenciais.

Alguns dos principais motivos pelos quais os clientes da Thales têm usado a DDC junto com produtos de terceiros incluem:

Muitas vezes nos perguntam... **"Qual é a diferença entre a CipherTrust Data Discovery and Classification e outras soluções de prevenção contra perda de dados (DLP)?"**

Descoberta

Proteção

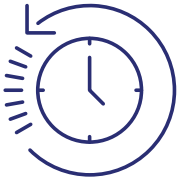


Controle

As soluções de DLP se concentram em impedir que dados confidenciais saiam do perímetro da empresa. A DDC se concentra na privacidade de dados, identificando dados confidenciais e obtendo uma compreensão clara dos dados e seus riscos. Isso permite as medidas adequadas para proteger seus dados e o cumprimento das normas de privacidade e segurança de dados.

- Nossa solução corrige erros na cobertura, já que a ferramenta de descoberta existente não pode fazer a varredura de todos os dados

Bloqueie o acesso desnecessário a dados para reduzir o risco de violações de dados



Mantenha-se atualizado com a evolução do panorama regulamentar para permanecer em

Aborda as preocupações com a transformação digital sobre segurança na nuvem para ajudar com objetivos empresariais e tecnológicos

  estruturados e não estruturados
- Busca maior precisão nas correspondências de dados para eliminar as limitações que estão enfrentando com o padrão Regex
- Suporte a uma gama mais ampla de sistemas operacionais e plataformas para questionar mais a pegada de dados

Principais conclusões

Plataforma CipherTrust Data Security

Sua estratégia de gerenciamento e proteção de dados pode ser melhorada significativamente com a solução CipherTrust Data Discovery and Classification. Junto com o CipherTrust Manager e o CipherTrust Transparent Encryption, ela proporciona visibilidade e percepção consideráveis de seus dados confidenciais, oferecendo opções de proteção rápidas e eficazes. A solução permite:

Experimente nossa avaliação gratuita de 90 dias para ver por si mesmo como nossa solução pode ajudar sua empresa agora.

Abreviações

ACL	Lista de controles de acesso
CDSP	Plataforma CipherTrust Data Security
CIFS	Common Internet File System
CM	CipherTrust Manager
CTE	CipherTrust Transparent Encryption
DB	Banco de dados
DDC	CipherTrust Data Discovery and Classification
GUI	Interface gráfica do usuário
NAS	Armazenamento conectado à rede
REST API	Aplicativo de transferência de estado representacional Interface de programação
TDP	Plataforma de dados da Thales
NAS	Armazenamento conectado à rede

Glossário

Perfil de classificação	Um perfil de classificação usa uma lista de infotipos para definir o tipo de informação confidencial a ser pesquisada durante uma varredura
Conector	Um conector é um termo genérico relacionado aos diferentes produtos ou componentes licenciáveis (que incluem DDC e CTE) que são gerenciados usando o console CipherTrust Manager
Agente CTE	Um agente CTE é um componente de software usado para criptografar dados associados a GuardPoints definidos usando políticas CTE
Correspondência de dados	Uma correspondência de dados ocorre durante uma varredura quando é encontrada uma instância qualificada de um infotipo incluído no escopo da pesquisa
Objeto de dados	Um arquivo ou tabela de banco de dados localizado em um armazenamento de dados é conhecido como objeto de dados
Armazenamento de dados	Um armazenamento de dados é a entidade onde os dados são realmente armazenados, com a DDC oferecendo suporte a vários tipos: local, rede, banco de dados, big data e nuvem
Agente DDC	Um agente DDC é um componente de software usado para verificar um armazenamento de dados em busca de tipos específicos de dados definidos por meio de infotipos associados
Descoberta	perfil de classificação
Falsos negativos	A descoberta de dados é o processo de mapeamento dos ativos de dados de uma organização, incluindo seus locais, tipos e níveis de confidencialidade
Falsos positivos	Os falsos negativos ocorrem quando o processo de descoberta não consegue identificar uma ou mais instâncias válidas de dados confidenciais
GuardPoint	Um GuardPoint especifica a lista de pastas ou caminhos a serem protegidos, o acesso a arquivos e a criptografia de arquivos no GuardPoint são controlados por políticas de segurança
Infotipo	Um infotipo é usado para categorizar dados específicos (como números de passaporte ou e-mail) a serem procurados durante uma varredura de descoberta, formando um componente integral na definição de um perfil de classificação
Política	Uma política é um conjunto de regras que regem o acesso e a criptografia de dados
Remediação	Remediação se refere ao processo de proteção (ou segurança) dos dados que foram identificados como vulneráveis como resultado de uma varredura, os métodos típicos de correção incluem criptografia, tokenização, mascaramento de dados e controle de acesso.
Conjunto de recursos	Um conjunto de recursos se refere aos arquivos ou diretórios aos quais a política se aplicará, juntamente com as regras principais associadas
Risco	Um risco é a presença de um objeto de dados confidenciais em um armazenamento de dados e está diretamente relacionado às correspondências de dados encontradas no objeto de dados ou no armazenamento de dados
Varredura	Uma varredura faz parte do processo de descoberta usado para pesquisar dados confidenciais em armazenamentos de dados usando critérios definidos em perfis de classificação

Objeto de dados confidenciais	Um objeto de dados que contém qualquer correspondência de dados é conhecido como um objeto de dados confidenciais
Nível de confidencialidade	Nível de confidencialidade é um parâmetro obrigatório (ao definir armazenamentos de dados e perfis de classificação) relacionado ao grau de vulnerabilidade potencial de um determinado objeto de dados, se exposto
Dados estruturados	Os dados estruturados são altamente organizados e facilmente compreendidos pela linguagem de máquina, exemplos incluem nomes, datas, endereços, números de cartão de crédito, informações de estoque, geolocalização e muito mais
Tag	Uma tag ajuda a agrupar dados e pode ser especificada ao criar armazenamentos de dados e perfis de classificação
Plataforma de dados da Thales	A plataforma de dados da Thales (TDP) é uma plataforma de big data baseada na tecnologia Hadoop que é usada pela DDC para várias tarefas, incluindo o armazenamento de resultados de varreduras
Dados não estruturados	Dados não estruturados são informações que não têm um modelo de dados (ou esquema) predefinido ou não são organizados de maneira predefinida, o que os torna inadequados para armazenamento em um banco de dados relacionado

THALES

Building a future we can all trust

Entre em contato conosco

Para saber as localizações de todos os escritórios e obter informações de contato, acesse cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com