Folha de dados

CipherTrust Data Discovery and Classification - perguntas frequentes

cpl.thalesgroup.com

THALES
Building a future we can all trust

Conteúdo

3 Fatores comerciais e de mercado
3 O que é a CipherTrust Data Discovery and Classification (DDC)?
3 Quais problemas/casos de uso do cliente a DDC aborda?
3 Quais são os setores que usam e precisam da CipherTrust Data Discovery and Classification?
3 Como a solução ajuda a proteger dados e cumpre a conformidade?

4 Conceitos básicos
4 O que é descoberta de dados?
4 O que é classificação de dados?
4 O que é remediação de dados?
4 Como a DDC se compara às soluções de prevenção contra perda de dados (DLP)?

4 Informações sobre a implementação da solução
4 Quais são as opções de implementação?
4 Quais são os prós e os contras das implementações baseadas em agente e sem agente?
5 Onde são executadas as varreduras de descoberta?
5 É necessário um agente para cada armazenamento de dados?
5 Como um agente é selecionado para varredura?
5 É possível fazer a varredura de um caminho ou tabela específica em um armazenamento de dados?
5 Quais fatores devem ser considerados para decidir quantos agentes são necessários?
5 O cliente pode definir seus próprios tipos de dados?
6 Quais países a solução abrange?
7 A DDC oferece suporte para plataformas de nuvem pública?
7 Como uma empresa pode ver os resultados de uma varredura?
7 O que significam as pontuações de risco e como elas são usadas?
7 Quais modelos de conformidade estão incluídos na solução?
7 Quais idiomas a solução usa?
7 Uma única varredura pode fazer a análise de vários regulamentos?
7 Uma varredura consegue descobrir segredos?
7 Como é possível fazer a varredura de dados semiestruturados?
7 O mecanismo de varredura ignora determinados arquivos?
7 Qual é o desempenho da varredura?
8 O que a CipherTrust DDC faz para reduzir falsos positivos e falsos negativos?

8 Segurança
8 Onde a solução armazena as informações que utiliza durante a operação?
8 Como a DDC se comunica de forma segura com os armazenamentos de dados?

8 Preços e licenciamento
8 Quais são os preços e tipos da DDC?
8 Como um cliente pode monitorar os dados que consumiu?
9 Como é calculada a capacidade restante da franquia de dados?
9 O que acontece no final do período da licença, mesmo quando uma capacidade não utilizada está disponível?
9 Quais recursos são fornecidos na renovação da licença da DDC?

THALES
Building a future we can all trust

Fatores comerciais e de mercado

O que é a CipherTrust Data Discovery and Classification (DDC)?

A solução CipherTrust Data Discovery and Classification oferece visibilidade completa da localização de dados confidenciais em toda a empresa, para que você possa descobrir e corrigir erros de conformidade. A DDC faz a varredura de armazenamentos de dados estruturados e não estruturados em busca de entidades nomeadas em diferentes formatos e idiomas para ajudar a encontrar qualquer tipo de dado confidencial, em qualquer idioma e em qualquer lugar da empresa. Depois de identificar os problemas de segurança, você pode corrigi-los rapidamente usando uma das soluções de criptografia líderes de mercado da plataforma CipherTrust.

Quais problemas/casos de uso do cliente a solução aborda?

Conformidade com as normas de segurança e privacidade: As empresas precisam proteger as informações de identificação pessoal (PII) contra vazamentos de dados e uso indevido para cumprir os requisitos das regulamentações de privacidade, como o Regulamento Geral de Proteção de Dados (GDPR), a Lei de Privacidade do Consumidor da Califórnia (CCPA), a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) e a Lei Geral de Proteção de Dados do Brasil (LGPD). A CipherTrust DDC oferece visibilidade completa da localização de dados confidenciais, aumentando a capacidade da empresa de adotar controles de segurança de dados adequados e medidas para proteger dados pessoais confidenciais contra perda e acesso não autorizado.

Mais visibilidade dos dados: as empresas precisam de maior visibilidade dos dados para dar suporte a uma melhor tomada de decisão para análise e correção de riscos, bem como para relatórios e conformidade. De acordo com o relatório sobre ameaças a dados da Thales de 2024, 70% das empresas conseguem classificar apenas 50% ou menos de seus dados. A CipherTrust DDC verifica automaticamente seus armazenamentos de dados em ambientes locais, híbridos e multinuvem para ajudar a proteger e gerenciar seus dados confidenciais.

Menos riscos de exposição durante a migração para a nuvem: os principais programas de mudança, como a transformação digital, envolvem a transferência de grandes quantidades de dados confidenciais de um ambiente para outro. A dispersão descontrolada de dados em plataformas de nuvem aumenta o potencial de um evento de violação de dados, bem como a violação das normas de privacidade. À medida que os ambientes de TI se tornam mais complexos, fica mais difícil descobrir dados confidenciais e supervisionar ou gerenciar o acesso às fontes de dados. A CipherTrust DDC oferece visibilidade de exatamente quais informações estão armazenadas para que você possa planejar uma estratégia eficaz de transformação para proteger os dados em cada etapa do processo.

Descoberta de segredos: as tendências modernas de desenvolvimento, como conteinerização, DevOps e automação, contribuíram para um aumento maciço no uso de segredos (credenciais, certificados e chaves) para autenticação. Os segredos podem ser vulneráveis a ciberataques quando não são gerenciados com segurança. A plataforma CipherTrust Data Security oferece um fluxo de trabalho simplificado para lidar com esse risco. A DDC descobre automaticamente mais de 30 tipos diferentes de segredos, incluindo chaves AES, segredos de autenticação e chaves SSH. Uma vez descobertos os segredos expostos, as equipes de segurança podem tomar medidas para remediar o risco e melhorar a postura de segurança usando o CipherTrust Secrets Management.

Quais são os setores que usam e precisam da CipherTrust Data Discovery and Classification?

Os setores altamente regulamentados, como financeiro, de seguros, saúde, manufatura, varejo e governo, representam o mercado-alvo dessa solução. Na verdade, qualquer setor que precise estar em conformidade com as normas de privacidade, especialmente se estiver passando por uma transformação digital, compartilhando dados confidenciais com um ecossistema de parceiros comerciais ou fornecedores, ou rastreando dados confidenciais em terminais, é cliente-alvo da CipherTrust Data Discovery and Classification.

Como a solução ajuda a proteger dados e cumpre a conformidade?

A CipherTrust Data Discovery and Classification localiza com eficiência dados confidenciais em uma empresa usando um fluxo de trabalho simplificado que automatiza a descoberta, classificação e proteção, elimina pontos cegos de segurança e fornece uma visão clara dos dados confidenciais e seus riscos. A solução vem com um conjunto abrangente de modelos incorporados para a descoberta rápida de dados regulamentados. Como resultado, as empresas podem descobrir e corrigir erros de proteção de dados, priorizar seus esforços de correção e responder proativamente a um número cada vez maior de normas de privacidade e segurança de dados de maneira mais fácil.

Conceitos básicos

O que é descoberta de dados?

A descoberta de dados é o processo de encontrar dados confidenciais ou regulamentados, estruturados e não estruturados armazenados em diferentes armazenamentos de dados, por exemplo, nuvem, servidores de arquivos, bancos de dados, big data, dispositivos, backups, instantâneos etc. A descoberta de dados é útil para encontrar dados confidenciais que os clientes precisam proteger para cumprir várias regulamentações. Dado o volume e a variabilidade dos dados e dos armazenamentos de dados, isso pode ser um desafio para qualquer empresa.

O que é classificação de dados?

A classificação de dados é o processo de categorização de dados com base em critérios predefinidos, por exemplo, modelos incorporados para normas de privacidade de dados ou perfis personalizados criados por uma empresa. A classificação de dados ajuda a determinar os níveis adequados de segurança necessários para os dados confidenciais. A CipherTrust Data Discovery and Classification oferece quatro níveis de classificação por padrão. Esses níveis de classificação são incorporados com as descrições a seguir. Se uma empresa quiser adicionar mais níveis ou alterar a definição de qualquer nível, ela poderá editar os níveis de classificação.

- Dados restritos: são dados altamente confidenciais, por exemplo, dados pessoais de clientes, segredos comerciais etc., que exigem a melhor segurança de dados possível. A divulgação desses dados pode acarretar graves consequências financeiras e jurídicas para uma empresa. As empresas devem priorizar a proteção desse tipo de dados.
- Dados privados: a divulgação desses dados pode causar sérios danos a uma empresa. Embora esses dados sejam menos confidenciais do que os restritos, eles exigem um alto nível de proteção.
- Dados internos: são dados de confidencialidade baixa, por exemplo, rascunho de um documento de planejamento. A exposição desses dados pode não causar muitos problemas para uma empresa. Uma consideração importante é que os dados geralmente não se destinam à divulgação pública.
- Dados públicos: são os dados menos confidenciais sem necessidade específica de segurança, por exemplo, comunicados à imprensa e material de marketing que são publicados em domínio público em sites. Esses dados podem ser compartilhados livremente com entidades externas.

O que é remediação de dados?

A remediação de dados é o processo de mitigação dos riscos da exposição de dados para que os dados confidenciais permaneçam protegidos contra acesso e uso não autorizados. Isso pode ser feito usando uma ou uma combinação de técnicas de proteção de dados, como criptografia de dados, tokenização, controles de identidade e acesso e outros métodos.

Como a DDC se compara às soluções de prevenção contra perda de dados (DLP)?

As soluções de DLP se concentram em impedir que dados confidenciais saiam do perímetro da empresa. A CipherTrust Data Discovery and Classification se concentra na privacidade e proteção de dados, identificando dados confidenciais e obtendo uma compreensão clara dos dados e seus riscos. Isso permite que as empresas tomem as medidas adequadas para proteger seus dados e cumpram as normas de privacidade e segurança de dados.

Informações sobre a implementação da solução

Quais são as opções de implementação?

A solução é implementada no local por meio da instalação de um agente no host ou remotamente por meio de um agente proxy.

Tipo de agente	Valor	Recomendação
Com agente	• As informações não precisam ser transmitidas pela rede para serem analisadas. • Varredura mais rápida • Não é preciso credenciais para varredura	Varredura de armazenamento de dados que permite que um agente seja instalado localmente. Por exemplo, armazenamento local e memória local no servidor ou na estação de trabalho com agentes instalados
Sem agente	• Implementação mais rápida, pois os agentes não precisam ser instalados diretamente nos hosts de destino • Realiza a varredura de vários alvos • Realiza a varredura de qualquer tipo de alvo • Não consome recursos no host de destino	Varredura de armazenamentos de dados que só podem ser acessados remotamente. Por exemplo, sistemas de banco de dados, servidores de e-mail, armazenamentos em nuvem e locais de armazenamento em rede

Quais são os prós e os contras das implementações baseadas em agente e sem agente?

Abaixo estão as recomendações para implementações baseadas em agente e sem agente:

Ambas as abordagens compartilham os seguintes prós:

Onde são executadas as varreduras de descoberta?

As varreduras de descoberta são executadas localmente, próximo ao local dos dados.

É necessário um agente para cada armazenamento de dados?

Não. Se você tiver vários armazenamentos de dados no mesmo host, poderá usar um agente para verificar todos os destinos. Os agentes proxy também podem examinar vários armazenamentos de dados.

Como um agente é selecionado para varredura?

A seleção do agente para a varredura de um armazenamento de dados é feita automaticamente pela CipherTrust Data Discovery and Classification. O status desse processo é mostrado na página de resumo dos armazenamentos de dados. A seleção do agente é feita durante o processo de criação do armazenamento de dados e o cliente pode selecionar um agente específico usando o recurso de etiqueta e o número de agentes para analisar o local de destino. Dependendo do tipo de armazenamento de dados, esse recurso pode estar disponível ou não; por exemplo, os repositórios locais não têm nenhum desses recursos, pois só podem ser verificados usando o agente local.

É possível fazer a varredura de um caminho ou tabela específica em um armazenamento de dados?

Sim, isso pode ser configurado durante a criação da varredura. Uma vez selecionado o armazenamento de dados a ser varrido, o cliente pode selecionar um alvo específico para a varredura, por exemplo, uma tabela em um banco de dados ou um caminho específico em um armazenamento local.

Quais fatores devem ser considerados para decidir quantos agentes são necessários?

A CipherTrust Data Discovery and Classification pode descobrir um ou mais armazenamentos de dados (servidores de arquivos, bancos de dados, repositórios de rede, big data etc.) em uma única varredura. Embora seja difícil generalizar, aqui estão algumas considerações:

- A quantidade de dados a serem analisados em cada armazenamento de dados. Por exemplo, um cliente pode usar vários agentes para examinar um armazenamento de dados do Hadoop, cada agente examinando um caminho diferente.
- A frequência e o número total de varreduras a serem executadas.

O cliente pode definir seus próprios tipos de dados?

Sim. O cliente pode definir seus próprios tipos de dados com base em padrões e expressões regulares.

Quais países a solução abrange?

A versão atual da solução abrange tipos de dados de países em várias regiões que podem ser usados em varreduras.

Região	Países	
África	• Gâmbia • África do Sul	
Ásia	• Hong Kong • Japão • Malásia • China • Singapura	• Coreia do Sul • Sri Lanka • Taiwan • Tailândia
Europa	• Áustria • Bélgica • Bulgária • Croácia • Chipre • República Tcheca • Dinamarca • Finlândia • França • Alemanha • Grécia • Hungria • Islândia • Irlanda • Itália • Letônia	• Luxemburgo • Macedônia • Malta • Holanda • Noruega • Polônia • Portugal • Romênia • Sérvia • Eslováquia • Eslovênia • Espanha • Suécia • Suíça • Turquia • Reino Unido • Iugoslávia (antiga)
Oriente Médio	• Irã • Israel • Arábia Saudita • Emirados Árabes Unidos	
América do Norte	• Canadá • México • Estados Unidos	
Oceania	• Austrália • Nova Zelândia	
América do Sul	• Brasil • Chile	

A DDC oferece suporte para plataformas de nuvem pública?

Sim.

Como uma empresa pode ver os resultados de uma varredura?

A CipherTrust Data Discovery and Classification permite que as empresas obtenham uma compreensão clara de seus dados confidenciais, locais, riscos e status de proteção a partir de um painel centralizado. Os usuários poderão acessar relatórios detalhados para auditorias e mitigação de riscos, tudo a partir de um painel centralizado.

O que significam as pontuações de risco e como elas são usadas?

As pontuações de risco permitem que as empresas identifiquem a confidencialidade dos objetos de dados, como arquivos e bancos de dados, agregando vários parâmetros, como nível de proteção, número de elementos encontrados, localização, quantidade de dados confidenciais etc. Com as pontuações de risco, as empresas podem identificar as fontes de maior risco e tomar medidas para proteger os dados confidenciais. No futuro, as pontuações de risco fornecerão informações adicionais, como a pontuação média de risco, para que as empresas possam comparar o risco apresentado por cada dado.

Quais modelos de conformidade estão incluídos na solução?

Alguns exemplos: APPI, CCPA, GDPR, HIPAA, NDB, PCI DSS, LGPD, UK-GDPR e SHIELD.

Quais idiomas a solução usa?

A CipherTrust DDC pode analisar qualquer caractere baseado em Unicode, ou seja, quase todos os idiomas. Do ponto de vista da GUI, o CipherTrust DDC suporta apenas o inglês, mas há planos para adicionar mais idiomas no futuro.

Uma única varredura pode fazer a análise de vários regulamentos?

Sim, o cliente pode selecionar quantos regulamentos desejar ao fazer a varredura de dados confidenciais.

Uma varredura consegue descobrir segredos ?

Sim, a CipherTrust Data Discovery and Classification analisa e detecta automaticamente códigos que revelam informações confidenciais que podem ser liberadas por engano por desenvolvedores.

Como é possível fazer a varredura de dados semiestruturados?

A CipherTrust DDC analisa dados semiestruturados e dados não estruturados.

O mecanismo de varredura ignora determinados arquivos?

É muito comum que alguns mecanismos de varredura ignorem determinados arquivos quando o tipo de arquivo é desconhecido. A CipherTrust DDC não ignora esses arquivos, mas os examina como arquivos não estruturados. A CipherTrust DDC ignorará os arquivos se, devido a um erro de acesso, não for possível ler o conteúdo. Esses arquivos serão considerados como objetos de dados inacessíveis nos relatórios.

Armazenamento de dados	Tamanho do conjunto de dados	Duração total (seg.)	Desempenho (GB/hora)
Armazenamento local Linux	Pequeno (917 MB)	340 ~5,6 min.	9,5
	Grande (1,04 TB)	88759 ~24,66 hs	39,5
MySQL	Pequeno (540 MB)	208,67 ~3,5 min.	9
	Médio (9 GB)	2784 ~ 46,4 min.	11,3

Qual é o desempenho da varredura?

O desempenho da varredura depende de diferentes aspectos dela, como o número de infotipos na descoberta, o tamanho e o número de arquivos/tabelas, a RAM atribuída aos agentes envolvidos e o número de agentes atribuídos para varrer os armazenamentos de dados.

Veja aqui:

O que a CipherTrust DDC faz para reduzir falsos positivos e falsos negativos?

É importante entender que nenhuma solução pode eliminar o potencial de falsos positivos. A CipherTrust DDC usa GLASS, uma tecnologia proprietária criada na era moderna para superar as limitações de expressão regular. Foi projetada especialmente para isso Utiliza recursos das CPUs modernas e oferece descoberta de alto desempenho. É um recurso poderoso para necessidades complexas e pode ser dimensionado para um nível de petabytes de dados.

Como resultado, a solução CipherTrust DDC contém um mecanismo que supera muitas das limitações funcionais herdadas das expressões regulares (regex) para localizar dados, o que leva a uma maior precisão, entre outras coisas. Em última análise, os infotipos incorporados são igualmente importantes em termos de como os dados são correspondidos e, usando o GLASS, o cliente pode facilmente desenvolver seus padrões e adicionar critérios de validação adicionais onde armazenam dados que são exclusivos para ele, mas que se cruzam com infotipos comuns. Além disso, os infotipos incorporados podem ser configurados com alta ou baixa precisão. Alta precisão significa que a CipherTrust DDC validará o contexto da correspondência, procurando por palavras-chave específicas relacionadas à correspondência. A análise do contexto será feita com base no formato existente e na validação do algoritmo. A baixa precisão evita a verificação do contexto. Portanto, se um cliente quiser reduzir o número de falsos negativos, ele deve considerar o uso de baixa precisão e considerar que isso pode levar a mais falsos positivos. Caso queira reduzir o número de falsos positivos, o cliente pode usar a seleção de alta precisão, mas sabendo que algumas correspondências podem ser perdidas.

Como parte dos mais de 250 infotipos que acompanham a solução CipherTrust DDC e a capacidade de desenvolvê-los conforme descrito acima, é possível atender a muitos cenários específicos do cliente ou superar quaisquer preocupações levantadas usando a criação de infotipo personalizado. Além disso, considere que, com o recurso de infotipo personalizado, também é possível definir as palavras-chave a serem usadas para um determinado caso de uso.

Segurança

Onde a solução armazena as informações que utiliza durante a operação?

A solução não coleta nem armazena dados confidenciais, mas coleta os resultados e o tipo de informação que uma empresa gerencia. Essas informações são armazenadas de forma segura na plataforma de dados da Thales, que é um banco de dados Hadoop local, criptografado e hospedado pelo cliente. A Thales fornece uma implementação de referência para o cliente usar como parte do contrato de licença.

Como a DDC se comunica de forma segura com os armazenamentos de dados?

A CipherTrust Data Discovery and Classification se comunica com os armazenamentos de dados por meio de agentes. Os agentes podem ser instalados local ou remotamente nos armazenamentos de dados. Os agentes se conectam às fontes de dados usando protocolos nativos, por exemplo, NFS para compartilhamento Unix, SMB para compartilhamento Windows, HDFS para Hadoop etc. Cada protocolo tem sua própria maneira de proteger dados. Por exemplo:

- bancos de dados: autenticação de usuário e senha com SSL/TLS.
- o NFS pode ser protegido por meio de acesso ao host e configuração de permissões de arquivo.
- o SMB usa autenticação de usuário, senha e domínio.
- o Hadoop usa um protocolo proprietário.

O cliente é responsável por:

- usar TLS ou texto simples
- proteger os servidores onde os agentes são implantados

Preços e licenciamento

Quais são os preços e tipos da DDC?

A CipherTrust Data Discovery and Classification faz parte da plataforma CipherTrust Data Security. O preço é baseado na quantidade de dados analisados por uma empresa. Uma empresa pode analisar um ou todos os seus armazenamentos de dados até o limite da quantidade de dados definido pela licença. A CipherTrust Data Discovery and Classification usa a permissão de dados como forma de licenciamento, fornecendo prazos para licença de 1 a 3 anos. Quando o período especificado expirar ou quando toda a franquia de dados for utilizada antes da expiração do período especificado, independentemente do que ocorrer primeiro, o acesso à solução será interrompido. Se o cliente quiser continuar a usar o sistema, precisará adquirir um plano adicional.

Como um cliente pode monitorar os dados que consumiu?

O cliente pode monitorar seu consumo de dados nas configurações do painel de controle do CipherTrust Manager. Ele exibe a quantidade total de dados adquiridos, o total usado até o momento e a quantidade restante disponível para digitalizar novos dados. Caso a quantidade de dados consumida seja maior do que o total disponível, uma mensagem de aviso será exibida.

Como é calculada a capacidade restante da franquia de dados?

O modelo de licença de quantidade de dados é baseado na quantidade máxima agregada de dados já analisados para cada armazenamento de dados descoberto até o momento (o cálculo é feito por caminho*). Portanto, um dado alterado não será considerado como consumo adicional de dados, a menos que a quantidade total de dados analisada aumente, em comparação com a quantidade máxima já verificada nesse caminho para o armazenamento de dados.

Por exemplo, se em um arquivo de 4 MB, apenas um byte foi alterado, já que o tamanho geral do arquivo não está aumentando, não será consumida uma quantidade adicional de dados. Observe que, mesmo que o tamanho de um determinado arquivo aumente, mas haja outros arquivos cujo tamanho diminua para compensar o aumento da quantidade de dados em arquivos individuais, a quantidade geral de dados que está sendo verificada ainda é a mesma ou menor do que a quantidade máxima de dados já verificados e, portanto, a franquia de consumo de dados não será afetada.

Ao considerar os bancos de dados, o modelo de consumo de franquia de dados baseia-se na quantidade máxima agregada de dados já verificados em cada uma das fontes/armazenamentos de dados exclusivos que foram verificados até o momento. Por exemplo, se em um banco de dados Oracle com 500 GB de dados houver um registro atualizado, a nova varredura do banco de dados não terá impacto sobre a franquia de consumo de dados. Somente quando o tamanho do banco de dados aumenta, a franquia de consumo de dados é afetada.

*caminho configurado na varredura, que pode ser um diretório, arquivo ou tabela.

O que acontece no final do período da licença, mesmo quando uma capacidade não utilizada está disponível?

Após o esgotamento do período da licença, o cliente não poderá usar a funcionalidade da DDC. No entanto, a capacidade de visualizar relatórios de varredura antigos ainda estará disponível. Mas novas varreduras não serão possíveis sem uma licença válida em uso.

Quais recursos são fornecidos na renovação da licença DDC?

Após a renovação, a capacidade de consumo de dados permanece a mesma e, mesmo que o cliente não tenha consumido toda a franquia de dados no ano anterior, isso não será acrescentado à nova franquia, pois o período de validade terminou. Também é importante levar em conta que o consumo de dados do ano anterior ainda é consumido no servidor após a inserção da nova licença, já que se supõe que as varreduras anteriores e o armazenamento de dados ainda estarão sendo analisados.

Exemplo:

- Licença 1: 15 TB com prazo de 1 ano

Após a conclusão do primeiro ano, o cliente consumiu apenas 10 TB de 15 TB e renovou a licença:

- Licença 2: 15 TB com prazo de 1 ano

Após a inserção da licença 2, a quantidade total de dados será de 15 TB e o consumo de dados permanecerá em 10 TB, não sendo redefinido.

A única maneira de redefinir a licença é fazer uma nova instalação, mas isso significa perder todos os dados do ano anterior.

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

Folha de dados

CipherTrust Data Discovery and Classification - perguntas frequentes

cpl.thalesgroup.com

THALES
Building a future we can all trust

Conteúdo

3 Fatores comerciais e de mercado

3 O que é a CipherTrust Data Discovery and Classification (DDC)?

3 Quais problemas/casos de uso do cliente a DDC aborda?

3 Quais são os setores que usam e precisam da CipherTrust Data Discovery and Classification?

3 Como a solução ajuda a proteger dados e cumpre a conformidade?

4 Conceitos básicos

4 O que é descoberta de dados?

4 O que é classificação de dados?

4 O que é remediação de dados?

4 Como a DDC se compara às soluções de prevenção contra perda de dados (DLP)?

4 Informações sobre a implementação da solução

4 Quais são as opções de implementação?

4 Quais são os prós e os contras das implementações baseadas em agente e sem agente?

5 Onde são executadas as varreduras de descoberta?

5 É necessário um agente para cada armazenamento de dados?

5 Como um agente é selecionado para varredura?

5 É possível fazer a varredura de um caminho ou tabela específica em um armazenamento de dados?

5 Quais fatores devem ser considerados para decidir quantos agentes são necessários?

5 O cliente pode definir seus próprios tipos de dados?

6 Quais países a solução abrange?

7 A DDC oferece suporte para plataformas de nuvem pública?

7 Como uma empresa pode ver os resultados de uma varredura?

7 O que significam as pontuações de risco e como elas são usadas?

7 Quais modelos de conformidade estão incluídos na solução?

7 Quais idiomas a solução usa?

7 Uma única varredura pode fazer a análise de vários regulamentos?

7 Uma varredura consegue descobrir segredos?

7 Como é possível fazer a varredura de dados semiestruturados?

7 O mecanismo de varredura ignora determinados arquivos?

7 Qual é o desempenho da varredura?

8 O que a CipherTrust DDC faz para reduzir falsos positivos e falsos negativos?

8 Segurança

8 Onde a solução armazena as informações que utiliza durante a operação?

8 Como a DDC se comunica de forma segura com os armazenamentos de dados?

9 Preços e licenciamento

9 Quais são os preços e tipos da DDC?

9 Como um cliente pode monitorar os dados que consumiu?

9 Como é calculada a capacidade restante da franquia de dados?

9 O que acontece no final do período da licença, mesmo quando uma capacidade não utilizada está disponível?

9 Quais recursos são fornecidos na renovação da licença da DDC?

THALES
Building a future we can all trust

Fatores comerciais e de mercado

O que é a CipherTrust Data Discovery and Classification (DDC)?

A solução CipherTrust Data Discovery and Classification oferece visibilidade completa da localização de dados confidenciais em toda a empresa, para que você possa descobrir e corrigir erros de conformidade. A DDC faz a varredura de armazenamentos de dados estruturados e não estruturados em busca de entidades nomeadas em diferentes formatos e idiomas para ajudar a encontrar qualquer tipo de dado confidencial, em qualquer idioma e em qualquer lugar da empresa. Depois de identificar os problemas de segurança, você pode corrigi-los rapidamente usando uma das soluções de criptografia líderes de mercado da plataforma CipherTrust.

Quais problemas/casos de uso do cliente a solução aborda?

Conformidade com as normas de segurança e privacidade: As empresas precisam proteger as informações de identificação pessoal (PII) contra vazamentos de dados e uso indevido para cumprir os requisitos das regulamentações de privacidade, como o Regulamento Geral de Proteção de Dados (GDPR), a Lei de Privacidade do Consumidor da Califórnia (CCPA), a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) e a Lei Geral de Proteção de Dados do Brasil (LGPD). A CipherTrust DDC oferece visibilidade completa da localização de dados confidenciais, aumentando a capacidade da empresa de adotar controles de segurança de dados adequados e medidas para proteger dados pessoais confidenciais contra perda e acesso não autorizado.

Mais visibilidade dos dados: as empresas precisam de maior visibilidade dos dados para dar suporte a uma melhor tomada de decisão para análise e correção de riscos, bem como para relatórios e conformidade. De acordo com o relatório sobre ameaças a dados da Thales de 2024, 70% das empresas conseguem classificar apenas 50% ou menos de seus dados. A CipherTrust DDC verifica automaticamente seus armazenamentos de dados em ambientes locais, híbridos e multinuvem para ajudar a proteger e gerenciar seus dados confidenciais.

Menos riscos de exposição durante a migração para a nuvem: os principais programas de mudança, como a transformação digital, envolvem a transferência de grandes quantidades de dados confidenciais de um ambiente para outro. A dispersão descontrolada de dados em plataformas de nuvem aumenta o potencial de um evento de violação de dados, bem como a violação das normas de privacidade. À medida que os ambientes de TI se tornam mais complexos, fica mais difícil descobrir dados confidenciais e supervisionar ou gerenciar o acesso às fontes de dados. A CipherTrust DDC oferece visibilidade de exatamente quais informações estão armazenadas para que você possa planejar uma estratégia eficaz de transformação para proteger os dados em cada etapa do processo.

Descoberta de segredos: as tendências modernas de desenvolvimento, como conteinerização, DevOps e automação, contribuíram para um aumento maciço no uso de segredos (credenciais, certificados e chaves) para autenticação. Os segredos podem ser vulneráveis a ciberataques quando não são gerenciados com segurança. A plataforma CipherTrust Data Security oferece um fluxo de trabalho simplificado para lidar com esse risco. A DDC descobre automaticamente mais de 30 tipos diferentes de segredos, incluindo chaves AES, segredos de autenticação e chaves SSH. Uma vez descobertos os segredos expostos, as equipes de segurança podem tomar medidas para remediar o risco e melhorar a postura de segurança usando o CipherTrust Secrets Management.

Quais são os setores que usam e precisam da CipherTrust Data Discovery and Classification?

Os setores altamente regulamentados, como financeiro, de seguros, saúde, manufatura, varejo e governo, representam o mercado-alvo dessa solução. Na verdade, qualquer setor que precise estar em conformidade com as normas de privacidade, especialmente se estiver passando por uma transformação digital, compartilhando dados confidenciais com um ecossistema de parceiros comerciais ou fornecedores, ou rastreando dados confidenciais em terminais, é cliente-alvo da CipherTrust Data Discovery and Classification.

Como a solução ajuda a proteger dados e cumpre a conformidade?

A CipherTrust Data Discovery and Classification localiza com eficiência dados confidenciais em uma empresa usando um fluxo de trabalho simplificado que automatiza a descoberta, classificação e proteção, elimina pontos cegos de segurança e fornece uma visão clara dos dados confidenciais e seus riscos. A solução vem com um conjunto abrangente de modelos incorporados para a descoberta rápida de dados regulamentados. Como resultado, as empresas podem descobrir e corrigir erros de proteção de dados, priorizar seus esforços de correção e responder proativamente a um número cada vez maior de normas de privacidade e segurança de dados de maneira mais fácil.

Conceitos básicos

O que é descoberta de dados?

A descoberta de dados é o processo de encontrar dados confidenciais ou regulamentados, estruturados e não estruturados armazenados em diferentes armazenamentos de dados, por exemplo, nuvem, servidores de arquivos, bancos de dados, big data, dispositivos, backups, instantâneos etc. A descoberta de dados é útil para encontrar dados confidenciais que os clientes precisam proteger para cumprir várias regulamentações. Dado o volume e a variabilidade dos dados e dos armazenamentos de dados, isso pode ser um desafio para qualquer empresa.

O que é classificação de dados?

A classificação de dados é o processo de categorização de dados com base em critérios predefinidos, por exemplo, modelos incorporados para normas de privacidade de dados ou perfis personalizados criados por uma empresa. A classificação de dados ajuda a determinar os níveis adequados de segurança necessários para os dados confidenciais. A CipherTrust Data Discovery and Classification oferece quatro níveis de classificação por padrão. Esses níveis de classificação são incorporados com as descrições a seguir. Se uma empresa quiser adicionar mais níveis ou alterar a definição de qualquer nível, ela poderá editar os níveis de classificação.

- Dados restritos: são dados altamente confidenciais, por exemplo, dados pessoais de clientes, segredos comerciais etc., que exigem a melhor segurança de dados possível. A divulgação desses dados pode acarretar graves consequências financeiras e jurídicas para uma empresa. As empresas devem priorizar a proteção desse tipo de dados.
- Dados privados: a divulgação desses dados pode causar sérios danos a uma empresa. Embora esses dados sejam menos confidenciais do que os restritos, eles exigem um alto nível de proteção.
- Dados internos: são dados de confidencialidade baixa, por exemplo, rascunho de um documento de planejamento. A exposição desses dados pode não causar muitos problemas para uma empresa. Uma consideração importante é que os dados geralmente não se destinam à divulgação pública.
- Dados públicos: são os dados menos confidenciais sem necessidade específica de segurança, por exemplo, comunicados à imprensa e material de marketing que são publicados em domínio público em sites. Esses dados podem ser compartilhados livremente com entidades externas.

O que é remediação de dados?

A remediação de dados é o processo de mitigação dos riscos da exposição de dados para que os dados confidenciais permaneçam protegidos contra acesso e uso não autorizados. Isso pode ser feito usando uma ou uma combinação de técnicas de proteção de dados, como criptografia de dados, tokenização, controles de identidade e acesso e outros métodos.

Como a DDC se compara às soluções de prevenção contra perda de dados (DLP)?

As soluções de DLP se concentram em impedir que dados confidenciais saiam do perímetro da empresa. A CipherTrust Data Discovery and Classification se concentra na privacidade e proteção de dados, identificando dados confidenciais e obtendo uma compreensão clara dos dados e seus riscos. Isso permite que as empresas tomem as medidas adequadas para proteger seus dados e cumpram as normas de privacidade e segurança de dados.

Tipo de agente	Valor	Recomendação
Com agente	• As informações não precisam ser transmitidas pela rede para serem analisadas. • Varredura mais rápida • Não é preciso credenciais para varredura	Varredura de armazenamento de dados que permite que um agente seja instalado localmente. Por exemplo, armazenamento local e memória local no servidor ou na estação de trabalho com agentes instalados
Sem agente	• Implementação mais rápida, pois os agentes não precisam ser instalados diretamente nos hosts de destino • Realiza a varredura de vários alvos • Realiza a varredura de qualquer tipo de alvo • Não consome recursos no host de destino	Varredura de armazenamentos de dados que só podem ser acessados remotamente. Por exemplo, sistemas de banco de dados, servidores de e-mail, armazenamentos em nuvem e locais de armazenamento em rede

Informações sobre a implementação da solução

Quais são as opções de implementação?

A solução é implementada no local por meio da instalação de um agente no host ou remotamente por meio de um agente proxy.

Quais são os prós e os contras das implementações baseadas em agente e sem agente?

Abaixo estão as recomendações para implementações baseadas em agente e sem agente:

Ambas as abordagens compartilham os seguintes prós:

Onde são executadas as varreduras de descoberta?

As varreduras de descoberta são executadas localmente, próximo ao local dos dados.

É necessário um agente para cada armazenamento de dados?

Não. Se você tiver vários armazenamentos de dados no mesmo host, poderá usar um agente para verificar todos os destinos. Os agentes proxy também podem examinar vários armazenamentos de dados.

Como um agente é selecionado para varredura?

A seleção do agente para a varredura de um armazenamento de dados é feita automaticamente pela CipherTrust Data Discovery and Classification. O status desse processo é mostrado na página de resumo dos armazenamentos de dados. A seleção do agente é feita durante o processo de criação do armazenamento de dados e o cliente pode selecionar um agente específico usando o recurso de etiqueta e o número de agentes para analisar o local de destino. Dependendo do tipo de armazenamento de dados, esse recurso pode estar disponível ou não; por exemplo, os repositórios locais não têm nenhum desses recursos, pois só podem ser verificados usando o agente local.

É possível fazer a varredura de um caminho ou tabela específica em um armazenamento de dados?

Sim, isso pode ser configurado durante a criação da varredura. Uma vez selecionado o armazenamento de dados a ser varrido, o cliente pode selecionar um alvo específico para a varredura, por exemplo, uma tabela em um banco de dados ou um caminho específico em um armazenamento local.

Quais fatores devem ser considerados para decidir quantos agentes são necessários?

A CipherTrust Data Discovery and Classification pode descobrir um ou mais armazenamentos de dados (servidores de arquivos, bancos de dados, repositórios de rede, big data etc.) em uma única varredura. Embora seja difícil generalizar, aqui estão algumas considerações:

- A quantidade de dados a serem analisados em cada armazenamento de dados. Por exemplo, um cliente pode usar vários agentes para examinar um armazenamento de dados do Hadoop, cada agente examinando um caminho diferente.
- A frequência e o número total de varreduras a serem executadas.

Região	Países	
África	• Gâmbia • África do Sul	
Ásia	• Hong Kong • Japão • Malásia • China • Singapura	• Coreia do Sul • Sri Lanka • Taiwan • Tailândia
Europa	• Áustria • Bélgica • Bulgária • Croácia • Chipre • República Tcheca • Dinamarca • Finlândia • França • Alemanha • Grécia • Hungria • Islândia • Irlanda • Itália • Letônia	• Luxemburgo • Macedônia • Malta • Holanda • Noruega • Polônia • Portugal • Romênia • Sérvia • Eslováquia • Eslovênia • Espanha • Suécia • Suíça • Turquia • Reino Unido • Iugoslávia (antiga)
Oriente Médio	• Irã • Israel • Arábia Saudita • Emirados Árabes Unidos	
América do Norte	• Canadá • México • Estados Unidos	
Oceania	• Austrália • Nova Zelândia	
América do Sul	• Brasil • Chile	

O cliente pode definir seus próprios tipos de dados?

Sim. O cliente pode definir seus próprios tipos de dados com base em padrões e expressões regulares.

Quais países a solução abrange?

A versão atual da solução abrange tipos de dados de países em várias regiões que podem ser usados em varreduras.

A DDC oferece suporte para plataformas de nuvem pública?

Sim.

Como uma empresa pode ver os resultados de uma varredura?

A CipherTrust Data Discovery and Classification permite que as empresas obtenham uma compreensão clara de seus dados confidenciais, locais, riscos e status de proteção a partir de um painel centralizado. Os usuários poderão acessar relatórios detalhados para auditorias e mitigação de riscos, tudo a partir de um painel centralizado.

O que significam as pontuações de risco e como elas são usadas?

As pontuações de risco permitem que as empresas identifiquem a confidencialidade dos objetos de dados, como arquivos e bancos de dados, agregando vários parâmetros, como nível de proteção, número de elementos encontrados, localização, quantidade de dados confidenciais etc. Com as pontuações de risco, as empresas podem identificar as fontes de maior risco e tomar medidas para proteger os dados confidenciais. No futuro, as pontuações de risco fornecerão informações adicionais, como a pontuação média de risco, para que as empresas possam comparar o risco apresentado por cada dado.

Quais modelos de conformidade estão incluídos na solução?

Alguns exemplos: APPI, CCPA, GDPR, HIPAA, NDB, PCI DSS, LGPD, UK-GDPR e SHIELD.

Quais idiomas a solução usa?

A CipherTrust DDC pode analisar qualquer caractere baseado em Unicode, ou seja, quase todos os idiomas. Do ponto de vista da GUI, o CipherTrust DDC suporta apenas o inglês, mas há planos para adicionar mais idiomas no futuro.

Uma única varredura pode fazer a análise de vários regulamentos?

Sim, o cliente pode selecionar quantos regulamentos desejar ao fazer a varredura de dados confidenciais.

Uma varredura consegue descobrir segredos ?

Sim, a CipherTrust Data Discovery and Classification analisa e detecta automaticamente códigos que revelam informações confidenciais que podem ser liberadas por engano por desenvolvedores.

Como é possível fazer a varredura de dados semiestruturados?

A CipherTrust DDC analisa dados semiestruturados e dados não estruturados.

O mecanismo de varredura ignora determinados arquivos?

É muito comum que alguns mecanismos de varredura ignorem determinados arquivos quando o tipo de arquivo é desconhecido. A CipherTrust DDC não ignora esses arquivos, mas os examina como arquivos não estruturados. A CipherTrust DDC ignorará os arquivos se, devido a um erro de acesso, não for possível ler o conteúdo. Esses arquivos serão considerados como objetos de dados inacessíveis nos relatórios.

Qual é o desempenho da varredura?

O desempenho da varredura depende de diferentes aspectos dela, como o número de infotipos na descoberta, o tamanho e o número de arquivos/tabelas, a RAM atribuída aos agentes envolvidos e o número de agentes atribuídos para varrer os armazenamentos de dados.

Veja aqui:

Armazenamento de dados	Tamanho do conjunto de dados	Duração total (seg.)	Desempenho (GB/hora)
Armazenamento local Linux	Pequeno (917 MB)	340 ~5,6 min.	9,5
	Grande (1,04 TB)	88759 ~24,66 hs	39,5
MySQL	Pequeno (540 MB)	208,67 ~3,5 min.	9
	Médio (9 GB)	2784 ~ 46,4 min.	11,3

O que a CipherTrust DDC faz para reduzir falsos positivos e falsos negativos?

É importante entender que nenhuma solução pode eliminar o potencial de falsos positivos. A CipherTrust DDC usa GLASS, uma tecnologia proprietária criada na era moderna para superar as limitações de expressão regular. Foi projetada especialmente para isso Utiliza recursos das CPUs modernas e oferece descoberta de alto desempenho. É um recurso poderoso para necessidades complexas e pode ser dimensionado para um nível de petabytes de dados.

Como resultado, a solução CipherTrust DDC contém um mecanismo que supera muitas das limitações funcionais herdadas das expressões regulares (regex) para localizar dados, o que leva a uma maior precisão, entre outras coisas. Em última análise, os infotipos incorporados são igualmente importantes em termos de como os dados são correspondidos e, usando o GLASS, o cliente pode facilmente desenvolver seus padrões e adicionar critérios de validação adicionais onde armazenam dados que são exclusivos para ele, mas que se cruzam com infotipos comuns. Além disso, os infotipos incorporados podem ser configurados com alta ou baixa precisão. Alta precisão significa que a CipherTrust DDC validará o contexto da correspondência, procurando por palavras-chave específicas relacionadas à correspondência. A análise do contexto será feita com base no formato existente e na validação do algoritmo. A baixa precisão evita a verificação do contexto. Portanto, se um cliente quiser reduzir o número de falsos negativos, ele deve considerar o uso de baixa precisão e considerar que isso pode levar a mais falsos positivos. Caso queira reduzir o número de falsos positivos, o cliente pode usar a seleção de alta precisão, mas sabendo que algumas correspondências podem ser perdidas.

Como parte dos mais de 250 infotipos que acompanham a solução CipherTrust DDC e a capacidade de desenvolvê-los conforme descrito acima, é possível atender a muitos cenários específicos do cliente ou superar quaisquer preocupações levantadas usando a criação de infotipo personalizado. Além disso, considere que, com o recurso de infotipo personalizado, também é possível definir as palavras-chave a serem usadas para um determinado caso de uso.

Segurança

Onde a solução armazena as informações que utiliza durante a operação?

A solução não coleta nem armazena dados confidenciais, mas coleta os resultados e o tipo de informação que uma empresa gerencia. Essas informações são armazenadas de forma segura na plataforma de dados da Thales, que é um banco de dados Hadoop local, criptografado e hospedado pelo cliente. A Thales fornece uma implementação de referência para o cliente usar como parte do contrato de licença.

Como a DDC se comunica de forma segura com os armazenamentos de dados?

A CipherTrust Data Discovery and Classification se comunica com os armazenamentos de dados por meio de agentes. Os agentes podem ser instalados local ou remotamente nos armazenamentos de dados. Os agentes se conectam às fontes de dados usando protocolos nativos, por exemplo, NFS para compartilhamento Unix, SMB para compartilhamento Windows, HDFS para Hadoop etc. Cada protocolo tem sua própria maneira de proteger dados. Por exemplo:

- bancos de dados: autenticação de usuário e senha com SSL/TLS.
- o NFS pode ser protegido por meio de acesso ao host e configuração de permissões de arquivo.
- o SMB usa autenticação de usuário, senha e domínio.
- o Hadoop usa um protocolo proprietário.

O cliente é responsável por:

- usar TLS ou texto simples
- proteger os servidores onde os agentes são implantados

Preços e licenciamento

Quais são os preços e tipos da DDC?

A CipherTrust Data Discovery and Classification faz parte da plataforma CipherTrust Data Security. O preço é baseado na quantidade de dados analisados por uma empresa. Uma empresa pode analisar um ou todos os seus armazenamentos de dados até o limite da quantidade de dados definido pela licença. A CipherTrust Data Discovery and Classification usa a permissão de dados como forma de licenciamento, fornecendo prazos para licença de 1 a 3 anos. Quando o período especificado expirar ou quando toda a franquia de dados for utilizada antes da expiração do período especificado, independentemente do que ocorrer primeiro, o acesso à solução será interrompido. Se o cliente quiser continuar a usar o sistema, precisará adquirir um plano adicional.

Como um cliente pode monitorar os dados que consumiu?

O cliente pode monitorar seu consumo de dados nas configurações do painel de controle do CipherTrust Manager. Ele exibe a quantidade total de dados adquiridos, o total usado até o momento e a quantidade restante disponível para digitalizar novos dados. Caso a quantidade de dados consumida seja maior do que o total disponível, uma mensagem de aviso será exibida.

Como é calculada a capacidade restante da franquia de dados?

O modelo de licença de quantidade de dados é baseado na quantidade máxima agregada de dados já analisados para cada armazenamento de dados descoberto até o momento (o cálculo é feito por caminho*). Portanto, um dado alterado não será considerado como consumo adicional de dados, a menos que a quantidade total de dados analisada aumente, em comparação com a quantidade máxima já verificada nesse caminho para o armazenamento de dados.

Por exemplo, se em um arquivo de 4 MB, apenas um byte foi alterado, já que o tamanho geral do arquivo não está aumentando, não será consumida uma quantidade adicional de dados. Observe que, mesmo que o tamanho de um determinado arquivo aumente, mas haja outros arquivos cujo tamanho diminua para compensar o aumento da quantidade de dados em arquivos individuais, a quantidade geral de dados que está sendo verificada ainda é a mesma ou menor do que a quantidade máxima de dados já verificados e, portanto, a franquia de consumo de dados não será afetada.

Ao considerar os bancos de dados, o modelo de consumo de franquia de dados baseia-se na quantidade máxima agregada de dados já verificados em cada uma das fontes/armazenamentos de dados exclusivos que foram verificados até o momento. Por exemplo, se em um banco de dados Oracle com 500 GB de dados houver um registro atualizado, a nova varredura do banco de dados não terá impacto sobre a franquia de consumo de dados. Somente quando o tamanho do banco de dados aumenta, a franquia de consumo de dados é afetada.

*caminho configurado na varredura, que pode ser um diretório, arquivo ou tabela.

O que acontece no final do período da licença, mesmo quando uma capacidade não utilizada está disponível?

Após o esgotamento do período da licença, o cliente não poderá usar a funcionalidade da DDC. No entanto, a capacidade de visualizar relatórios de varredura antigos ainda estará disponível. Mas novas varreduras não serão possíveis sem uma licença válida em uso.

Quais recursos são fornecidos na renovação da licença DDC?

Após a renovação, a capacidade de consumo de dados permanece a mesma e, mesmo que o cliente não tenha consumido toda a franquia de dados no ano anterior, isso não será acrescentado à nova franquia, pois o período de validade terminou. Também é importante levar em conta que o consumo de dados do ano anterior ainda é consumido no servidor após a inserção da nova licença, já que se supõe que as varreduras anteriores e o armazenamento de dados ainda estarão sendo analisados.

Exemplo:

- Licença 1: 15 TB com prazo de 1 ano

Após a conclusão do primeiro ano, o cliente consumiu apenas 10 TB de 15 TB e renovou a licença:

- Licença 2: 15 TB com prazo de 1 ano

Após a inserção da licença 2, a quantidade total de dados será de 15 TB e o consumo de dados permanecerá em 10 TB, não sendo redefinido.

A única maneira de redefinir a licença é fazer uma nova instalação, mas isso significa perder todos os dados do ano anterior.

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