cpl.thalesgroup.com

THALES

Principais pilares da proteção de dados confidenciais em qualquer empresa

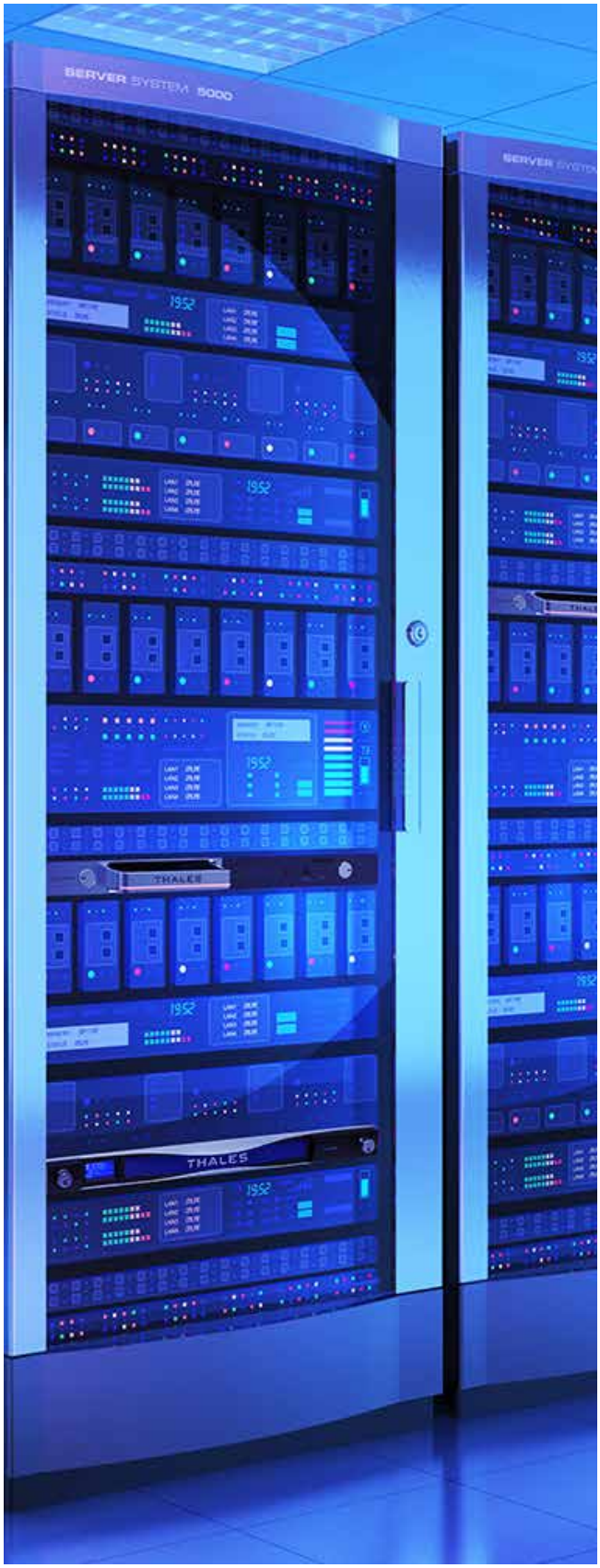
Artigo

Conteúdo

Visão geral

Tradicionalmente, as empresas têm focado a segurança de TI principalmente na defesa do perímetro, construindo muros para bloquear a entrada de ameaças externas na rede. Apesar de ser importante, isso não basta. Cibercriminosos violam frequentemente as defesas perimetrais, e como os dados estão frequentemente fora do alcance dessas defesas na nuvem, as empresas precisam aplicar uma estratégia de segurança centrada em dados que os proteja onde quer que estejam. Com atual proliferação de dados, criação de mais normas de privacidade globais e regionais, crescimento da adoção de nuvem, e ameaças persistentes avançadas, a segurança centrada em dados permite às empresas controlar seus dados independentemente de onde estejam, tornando-os ilegíveis para criminosos. Mas, para ser eficaz, esta proteção deve ser automática, sem depender da intervenção do usuário.

Este white paper descreve os desafios da segurança de dados nesta era de proliferação dos mesmos. Também fornece estratégias para descobrir e classificar seus dados críticos, e aplicar neles a segurança centrada nos dados.



Proliferação de dados, aumento de regulamentações e crimes cibernéticos mais sofisticados

Muitas arquiteturas já existentes de segurança de dados foram criadas com base no pressuposto de que os dados serão guardados no centro de dados e utilizados localmente. O ambiente tradicional de TI era controlado pela equipe de TI de ponta a ponta. A equipe de TI possuía e operava a infraestrutura, segurança e aplicações e, por isso, tinham uma imensa visibilidade e controle de dados e usuários. Todos os acessos a dados e aplicações passavam por camadas de segurança de perímetro, como firewalls, firewalls da próxima geração, VPN, antivírus, sistema de prevenção de intrusão etc.

Transfira a segurança para além do perímetro para defender o que mais importa

Arquitetura já existente de segurança de dados

Segurança baseada em perímetro confiável

Arquitetura de segurança centrada em dados

A segurança protege os dados em qualquer lugar

No entanto, em empresas modernas, estes pontos de controle já não existem. Por mais forte que seja o perímetro em redor do centro de dados, a segurança que proporciona é meramente conceitual, porque:

1. A segurança de perímetro não pode ser dimensionada para a movimentação e proliferação de dados

A adoção generalizada de serviços em nuvem, ambientes de big data e tecnologias de IoT significa que as empresas estão movimentado enormes quantidades de dados muito rapidamente, muitas vezes para infraestruturas e parceiros terceirizados. Isso apresenta uma série de desafios:

- Diversas formas de dados, incluindo dados estruturados, semi-estruturados e não estruturados
- Pontos de controle de segurança perimetral que acrescentam latência e problemas de desempenho que violam os acordos de nível de serviço (SLA) e, por isso, os usuários têm frequentemente acesso direto aos serviços de nuvem.
- Insiders por todas as partes: os insiders não são mais seus funcionários dentro do seu perímetro. Seus dados estão agora nas mãos de contratados, fornecedores de serviços e outros terceiros. Estes "insiders" são indivíduos que não foram verificados, não podem ser monitorizados nem controlados.

2. Complexidade operacional e normas de regulamentação

A transferência de dados para a nuvem, containers, tecnologias de big data, e ferramentas diferentes de múltiplos vendedores aumentam a complexidade. Com perímetros de segurança cada vez mais confusos, as empresas precisam pagar, implementar, e gerir políticas consistentes e unificadas para os recursos de TI distribuídos. Todas as empresas têm uma mistura de plataformas já existentes e novas.

O crescimento explosivo de dados é ainda mais complicado devido ao número crescente de normas de privacidade globais e regionais com diferentes requisitos de conformidade. Para cumprir as normas de maneira eficaz, as empresas já não podem confiar em abordagens de silos e já existentes para proteger seus dados.

Tudo isso torna os ambientes de dados atuais cada vez mais complexos. Assim, não surpreende que as empresas considerem a complexidade operacional como a principal barreira à implementação da segurança de dados. Diretores de segurança da informação (CISOs) e diretores de dados (CDOs) reconhecem cada vez mais a necessidade de soluções de segurança de dados abrangentes e integradas que proporcionem uma forte proteção de dados confidenciais, independentemente do local onde estes são armazenados ou utilizados.

Uma vez que as arquiteturas de segurança de dados já existentes não abordam muitas das características do mundo moderno centrado nos dados, elas não conseguem proteger as empresas contra vazamento de dados causados por criminosos cada vez mais determinados. Se os CISOs e CDOs atuais querem acabar com o ciclo reacionário de medidas e contramedidas, então precisam adotar uma abordagem completamente nova de segurança.

A complexidade operacional é a principal barreira para instalar a segurança de dados

Estratégia de três pontos para proteger dados confidenciais da sua empresa

As arquiteturas de segurança já existentes falharam frequente e dramaticamente, porque refletem visões desatualizadas de como as empresas interagem com seus dados. A segurança dos dados de hoje em dia precisa reconhecer não só que os dados são o bem mais valioso da empresa, mas também que estão em constante proliferação exponencial.

A segurança centrada em dados protege os dados em si e não apenas endpoints, redes e aplicações entre os quais se move. Consequentemente, os dados em si ficam seguros e podem fluir por sistemas quando a empresa necessita, sem maiores riscos. Em vez de desacelerar o progresso e inibir a proliferação de dados, a segurança centrada em dados permite à empresa tirar o máximo beneficio de seus dados onde quer que estejam armazenados e são utilizados.

Este gráfico demonstra os três pilares centrais da segurança centrada em dados.

Os três principais pilares da segurança de dados

nº 1
Descobrir e classificar dados confidenciais

- Descoberta e classificação eficiente de dados confidenciais
- Compreender claramente os dados e seus riscos

nº 2
Proteção de dados confidenciais

- Proteger dados confidenciais com criptografia, controles de acesso e tokenização
- Tornar os dados ilegíveis e inúteis, se forem roubados ou vazados

nº 3
Controlar chaves de criptografia

- Gerenciamento centralizado de chaves
- Gerenciar o ciclo de vida de chaves
- Gestão unificada de chaves e políticas de criptografia

Deve-se criar uma abordagem de segurança centrada em dados no DNA da empresa. Esta abordagem holística baseia-se na experiência da Thales em trabalhar com centenas de CISOs, CDOs, CIOs, e arquitetos de empresas encarregados pela segurança e proteção de dados, bem como nas melhores práticas exigidas por numerosos regulamentos e normas industriais. Para adotar esta abordagem de segurança de dados, as empresas precisam de fazer o seguinte:

1. Descobrir e classificar seus dados confidenciais

Dados confidenciais espalham-se pela empresa, pela nuvem e por muito além dela. Geralmente, a segurança de TI tem visibilidade limitada sobre onde os dados são armazenados e quem tem acesso aos mesmos. Os riscos de distribuição de dados variam de roubo de dados a violações de conformidade. Comece por identificar onde residem os dados mais confidenciais em seu data center local, e depois os transfira para seus ambientes maiores, como serviços em nuvem e de hospedagem. Inicie pesquisando seus servidores de armazenamento e arquivos, aplicações, bases de dados e máquinas virtuais. Identifique dados em toda a empresa, onde quer que estejam, e classifique sua confidenciabilidade e importância com base em políticas internas e regulamentos externos.

Descobrir, identificar e classificar seus dados confidenciais é o primeiro passo crítico neste processo, mas também precisa ser possível repetir o processo independente de tecnologia ou geografia. As soluções atuais de descoberta e classificação de dados fornecem painéis de controle visuais e detalhados que ajudam a compreender claramente que tipo de dados confidenciais você possui, onde se encontram e sua pontuação de risco. As pontuações de risco agregam vários parâmetros, como nível de proteção, número de elementos encontrados, localização, quantidade de dados confidenciais etc., e permitem às empresas identificar a confidenciabilidade dos objetos de dados, como arquivos e bases de dados. Assim, as empresas podem proteger dados e mitigar riscos; por exemplo, dando prioridade à remediação ou tomando decisões profissionais sobre compartilhamento de dados com terceiros ou migração para a nuvem.

A descoberta e classificação de dados é o primeiro passo para uma segurança de dados eficaz

2. Proteção de seus dados confidenciais

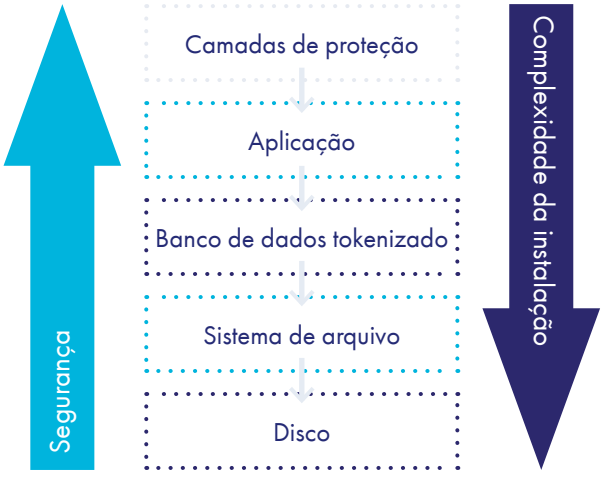
Idealmente, para proteger dados confidenciais, é preciso estabelecer em toda a empresa uma estratégia básica de criptografia, que minimize a fuga de dados e os riscos de violações com exposição.

Com seus dados descobertos e classificados, é possível determinar o risco que cada conjunto de dados acrescenta ao seu negócio e dar prioridade a como e onde implementar controles de acesso e mecanismos de segurança de ocultação, como criptografia de arquivos com controles de acesso granulares e tokenização com mascaramento dinâmico de dados. Isso significa proteger os dados, tornando mais difícil o acesso de usuários não autorizados e tornando-os ilegíveis e inúteis, se forem roubados ou vazados.

Atualmente, a criptografia é um dos métodos de segurança de dados mais populares e eficazes utilizados por empresas. A criptografia de dados transforma os dados em dados codificados, para que apenas usuários autorizados possam acessá-los como texto claro. Enquanto que a criptografia transforma os dados utilizando um algoritmo específico, a tokenização protege os dados confidenciais através da substituição por dados não confidenciais. A tokenização cria uma forma simbólica irreconhecível dos dados que mantém o formato dos dados originais. Os dados tokenizados também podem ser armazenados no mesmo tamanho e formato que os dados originais Assim, o armazenamento dos dados tokenizados não requer alterações no esquema ou processo da base de dados. Se o tipo de dado armazenado não tiver este tipo de estrutura - por exemplo arquivos de texto, PDFs, MP3s etc., a memorização simbólica não é uma forma adequada de ocultação. Neste caso, a criptografia a nível do sistema de arquivos seria apropriada. Desta maneira, o bloco original de dados é transformado em uma versão criptografada deles.

Ao determinar o tipo de solução de criptografia de dados que melhor satisfará seus requisitos, há várias considerações. Em um nível elevado, os tipos de criptografia de dados podem ser desvendados pelo local onde são empregados na tecnologia. Há quatro níveis da tecnologia em que a criptografia de dados é tipicamente utilizada: disco, sistema de arquivos, base de dados, e aplicação. Em geral, quanto mais baixa for a criptografia, mais simples e menos intrusiva será a implementação. No entanto, o número e os tipos de ameaças que estas abordagens de criptografia de dados podem enfrentar são poucos. Por outro lado, ao empregar a criptografia mais elevada, geralmente as empresas podem identificar níveis mais elevados de segurança e mitigar mais ameaças.

A segurança aumenta, mas a complexidade do desenvolvimento também aumenta quando implementado em nível mais alto



3. Controle de chaves de criptografia

A segurança dos processos criptográficos depende da segurança das chaves criptográficas utilizadas para criptografar os dados. Se as chaves utilizadas para criptografar ou tokenizar dados forem roubadas com os dados criptografados ou tokenizados, os dados não ficam seguros, porque podem ser decifrados e lidos em texto simples. Para que a criptografia e a tokenização consigam proteger dados confidenciais com sucesso , as próprias chaves de criptografia precisam ser protegidas, gerenciadas e controladas pela empresa, não por terceiros ou por provedores de nuvem.

Quando as empresas instalam um número cada vez maior de soluções de criptografia em diferentes silos, em cada ambiente ou solução, elas precisam gerir políticas inconsistentes, diferentes níveis de proteção e custos crescentes. O caminho mais simples através deste labirinto é a transição para um modelo centralizado de gestão de chaves. A gestão de chaves criptográficas envolve a administração de todo o ciclo de vida delas e a proteção contra perda ou uso indevido. As chaves têm um ciclo de vida: são criadas, têm tempo de vida útil e, por fim, aposentadas. A gestão do ciclo de vida de chaves inclui geração, utilização, armazenamento, distribuição, arquivamento e eliminação delas. Algumas das vantagens da gestão centralizada de chaves são:

- Gestão unificada de chaves e políticas de criptografia
- Revogação de chaves em todo o sistema
- Redução do risco de erros humanos na definição de permissões de usuários e administrativas
- Alta disponibilidade e escalabilidade
- Validação FIPS 140-2 segura
- Redução de custos com automatização
- Informações consolidadas de auditoria
- Backup e recuperação simplificados
- Maior segurança com separação abrangente de funções

Gerenciamento centralizado de chaves criptográficas

Vantagens da segurança centrada em dados eficaz

Com uma solução de segurança eficaz centrada em dados é possível enfrentar os desafios de segurança decorrentes da proliferação de dados e da urgência de normas globais e regionais de privacidade, e preparar sua empresa para um futuro mais seguro.

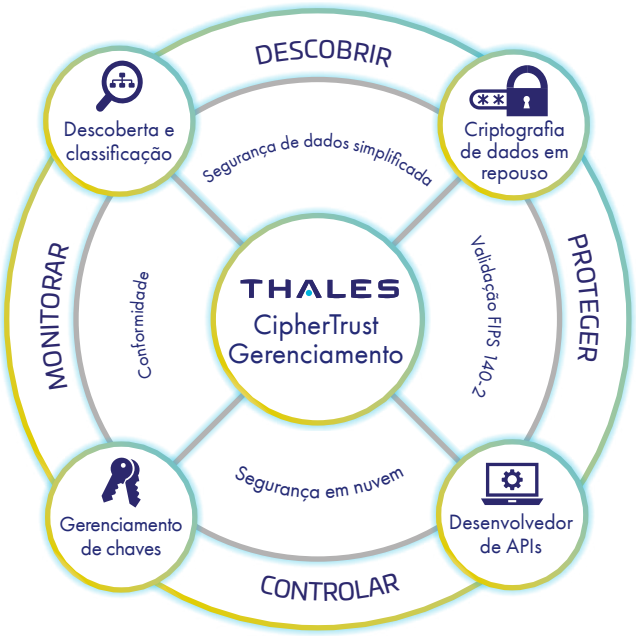
Uma solução de segurança centrada em dados instalada devidamente:

- Ajuda empresas a mitigar riscos e reduzir custos. As empresas podem reduzir custos através da operacionalização das infraestruturas de segurança existentes em escala global, reduzindo processos manuais que são trabalhosos, repetitivos e propensos a erros, e protegendo seu investimento no futuro ao permitir novas tecnologias.
- Fornece uma visão abrangente e contínua de todos os dados e facilitar a governança de políticas e controles de segurança.
- Ajuda as empresas a compreender seus dados e seus riscos e a dar prioridade à remediação.
- Protege os dados, para que se possam movimentar em segurança através de múltiplos ambientes locais e em nuvem, mantendo ao mesmo tempo seu perfil de proteção.
- Assegura que os dados estejam protegidos contra usuários mal intencionados e ameaças persistentes avançadas (APTs) que tentam roubar informações confidenciais.
- Reduz multas e ajuda as empresas a cumprir normas governamentais, organizacionais e industriais. As empresas podem monitorizar infrações e aplicar políticas e regras de segurança enquanto criam relatórios automatizados e auditam procedimentos de segurança.
- Cria uma posição legal defensável em resposta a uma violação de dados ou a um problema de auditoria.

Como a Thales pode ajudar a implementar uma estratégia de segurança de três pontos

A Thales é líder mundial em proteção de dados. Fornecemos tudo o que uma empresa precisa para descobrir, proteger e gerir seus dados, identidades e propriedade intelectual: descoberta e classificação de dados, criptografia, gestão avançada de chaves, tokenização e gestão de autenticação e acesso. A CipherTrust Data Security Platform da Thales unifica a descoberta e classificação de dados, proteção de dados e controles de acesso granular sem precedentes com gerenciamentos de chaves centralizado – tudo em uma única plataforma. Isto resulta em menos recursos dedicados às operações de segurança de dados, controles de conformidade onipresentes e risco significativamente reduzido em todo o seu negócio.

CipherTrust Data Security Platform



Principais recursos da CipherTrust Data Security Platform

- Descoberta e classificação de dados
  - Análise de riscos com visualização de dados
- Técnicas de proteção de dados
  - Criptografia transparente para arquivos, bancos de dados, big data e containers
  - Proteção de dados de aplicações
  - Tokenização com mascaramento dinâmico de dados
  - Criptografia com preservação de formato
  - Mascaramento de dados estáticos
  - Controles de acesso de usuário privilegiado
- Gerenciamento centralizado de chaves da empresa
  - Conformidade FIPS 140-2
  - Gerenciamento de chaves em nuvem múltipla
  - Ecossistema parceiro de integrações KMIP sem precedentes
  - Gerenciamento de chave de criptografia de banco de dados (Oracle TDE, big data, MS SQL, SQL Server Always Encrypted, etc.)
- Monitoramento e relatório
- Console de gerenciamento centralizado

Vantagens da CipherTrust Data Security Platform

Segurança de dados simplificada

Descobre, protege e controla dados confidenciais em qualquer lugar com proteção de dados unificada de última geração. A CipherTrust Data Security Platform simplifica a administração da segurança de dados com um console de gestão centralizada que equipa as empresas com ferramentas poderosas para descobrir e classificar dados confidenciais, combater ameaças externas, proteger contra o abuso de informações privilegiadas e estabelecer controle contínuo, mesmo quando os dados são armazenados em nuvem ou em outra infraestrutura de um provedor externo. As empresas podem facilmente descobrir e resolver falhas de privacidade, dar prioridade à proteção e tomar decisões informadas sobre os mandatos de privacidade e segurança antes de uma implementação de transformação digital.

Conformidade mais rápida

Entidades reguladoras e auditores exigem que as empresas tenham o controle de dados regulados e confidenciais e que disponham de relatórios que comprovem isso. Os recursos de segurança de dados abrangentes da CipherTrust Data Security Platform, incluindo descoberta e classificação de dados, criptografia, controle de acesso granular, registros de auditoria, tokenização e gerenciamento de chave suportam a segurança de dados omnipresente e os requerimentos de privacidade. Estes controles podem ser rapidamente acrescentados a novas instalações ou em resposta à evolução de requisitos de conformidade. A natureza centralizada e extensível da plataforma permite a adição rápida de novos controles através da adição de licenças e da instalação de scripts de conectores necessários em resposta a novos requisitos de proteção de dados.

Migrações seguras para a nuvem

A CipherTrust Data Security Platform oferece soluções avançadas de criptografia e gestão centralizada de chaves que permitem às empresas armazenar dados confidenciais em segurança na nuvem. A plataforma oferece soluções avançadas de criptografia em nuvem múltipla Bring Your Own Encryption (BYOE) para evitar o bloqueio de criptografia de fornecedores de nuvens e assegurar a mobilidade dos dados para protege-los eficazmente através de múltiplos fornecedores de nuvens com gestão centralizada e independente de chaves de criptografia. As empresas que não podem trazer sua própria criptografia ainda podem seguir as melhores práticas da indústria através do gerenciamento de chaves externo usando o CipherTrust Cloud Key Manager. O CipherTrust Cloud Key Manager suporta casos de uso de tecnologia Bring Your Own Key (BYOK) em múltiplas infraestruturas de nuvens e aplicações SaaS. Com a CipherTrust Data Security Platform, as proteções mais fortes protegem os dados confidenciais e as aplicações de uma empresa na nuvem, ajudando-a a cumprir os requisitos de conformidade e a ter mais controle sobre os dados, onde quer que sejam criados, utilizados ou armazenados.

Custo total de compra e propriedade menor

A CipherTrust Data Security Platform pode reduzir o custo total de compra e propriedade de uma solução para empresas de todos os tamanhos, simplificando a segurança dos dados, acelerando o tempo de conformidade e proporcionando segurança e controle de nuvem múltipla. Construída sobre uma infraestrutura extensível, a plataforma permite às empresas de TI e de segurança descobrir, classificar e proteger dados em repouso de toda a empresa de uma maneira uniforme e repetível. A utilização de uma abordagem já existente pode muitas vezes exigir produtos caros e dedicados, que podem necessitar de uma maior integração e tempo extra de funcionários para geri-la, não permitindo qualquer possível poupança de custos. Os diversos produtos disponíveis na CipherTrust Data Security Platform podem ser instalados individualmente ou em combinação, e preparam sua empresa para o próximo desafio de segurança ou requisito de conformidade com o menor custo total de propriedade. Ao integrar a descoberta e classificação de dados, análise de risco, proteção de dados e relatórios em uma única plataforma, a solução CipherTrust libera o pessoal de TI e o orçamento para tarefas mais estratégicas e dá poder à abertura e liberdade de colaboração que a empresa moderna necessita - sem sacrificar a segurança.

Resumo

Os ataques aos dados estão se tornando mais sofisticados porque eles estão ficando mais valiosos, e as empresas precisam proteger suas informações mais confidenciais e defender sua reputação. A segurança centrada em dados é a única abordagem que proporciona conformidade e uma proteção significativa contra as atuais ameaças à cibersegurança. Estratégias eficazes de segurança centradas em dados baseadas nos três pilares de descoberta e classificação de dados, proteção de dados, e gestão centralizada de chaves de criptografia permitem às organizações extrair valor de forma segura de dados sensíveis e adotar com confiança tecnologias de transformação digital.

Com as soluções centradas em dados da Thales, é possível proteger de forma rentável e eficiente dados confidenciais estruturados e não estruturados em toda a sua empresa.

THALES

Entre em contato

Para localização de escritórios e informações de contato, visite

> cpl.thalesgroup.com <