cpl.thalesgroup.com

THALES

Soluções de criptografia de banco de dados Thales

Desafios de segurança de banco de dados

Nas empresas de hoje, os bancos de dados abrigam alguns dos dados mais sensíveis e regulamentados - os mesmos dados buscados por funcionários mal-intencionados e invasores externos. Muitos ataques a banco de dados foram divulgados nos últimos anos, expondo centenas de milhões de registros e resultando em danos financeiros e à reputação das organizações afetadas.

Ponto Central de Falha

Os bancos de dados representam um ponto de agregação central - e um ponto de foco para hackers. Nos bancos de dados residem muitos ativos corporativos, incluindo informações confidenciais e controladas, como dados de pagamento de clientes, prontuários de pacientes e propriedade intelectual. Em suma, seus bancos de dados, locais ou em nuvem, retêm dados que são importantes para seus negócios e desejados por possíveis invasores.

Controles de segurança insuficientes

Controles de segurança insuficientes expõem sua organização a fraudes e violações de dados. Por exemplo, quando a criptografia de banco de dados e o gerenciamento de chaves correspondente são manipulados no banco de dados, o administrador do banco de dados (DBA) controla os dados e as chaves. As soluções de criptografia de banco de dados geralmente desconsideram o potencial de abuso interno, bem como ameaças persistentes avançadas, nas quais um invasor imita um usuário privilegiado.

Gerenciamento de chaves complexo e ineficiente

À medida que os ambientes de banco de dados se expandem, os principais desafios de gerenciamento também aumentam. O uso de várias ferramentas de gerenciamento de chaves é complexo e cria mais oportunidades para erros e fraudes. Embora os provedores de banco de dados ofereçam funcionalidade de gerenciamento de chaves, isso só funciona quando a empresa usa os bancos de dados específicos desse provedor. Como cada instância do banco de dados de um provedor exige uma chave de criptografia separada, o gerenciamento das chaves para bancos de dados diferentes resulta em mais complexidade e agrava os riscos de perda ou roubo de chaves. Leia o relatório da Aberdeen sobre o espantoso custo do gerenciamento de chaves díspares.

A criptografia nativa de bancos (TDE) é suficiente?

Os bancos de dados Oracle e Microsoft SQL Server fornecem funcionalidade criptografia nativa de bancos (TDE), permitindo a criptografia no banco de dados ou no nível do campo. É muito provável, no entanto, que você também precise criptografar os arquivos de log e relatório que contêm dados confidenciais sobre esses bancos de dados. E para muitas organizações, os dados em outros aplicativos e bancos de dados também precisarão ser criptografados, exigindo investimentos em vários produtos de criptografia, sistemas de gerenciamento e armazenamento de chaves e esforços de implementação.

As limitações e riscos das abordagens tradicionais

Tradicionalmente, as equipes de segurança se concentram em estabelecer e reforçar as defesas de perímetro. No entanto, essas defesas deixam os bancos de dados da sua organização expostos a uma variedade de ameaças internas:

- Usuários privilegiados podem explorar sua visibilidade e permissões para acessar dados privados, sabotar configurações e ocultar seus rastros
- Outros funcionários podem abusar de seus privilégios de acesso ou podem, inadvertidamente, burlar políticas e deixar os dados expostos
- Os invasores externos que obtêm acesso às credenciais de administrador ou usuário podem explorar essas permissões para realizar ataques

Para cumprir as políticas organizacionais e os mandatos regulatórios, sua equipe de segurança precisa lidar com essas ameaças, estabelecendo fortes defesas para seus bancos de dados.

Criptografia de banco de dados e gerenciamento de chaves com fortes controles de acesso

Com as soluções da Thales, sua organização pode estabelecer uma defesa forte e abrangente para bancos de dados e os dados valiosos contidos neles. As soluções da Thales apresentam criptografia robusta e gerenciamento de chaves, controles de acesso granulares e login para ajudar a proteger seus ambientes de banco de dados local e na nuvem. Suas equipes de segurança podem criptografar dados confidenciais e aplicar políticas granulares que limitam quem tem acesso para descriptografar esses dados.

Soluções para criptografia de banco de dados

Vormetric Data Security Manager

O Vormetric Data Security Manager, ou DSM, fornece uma plataforma central para gerenciar criptografia, políticas, chaves e inteligência de segurança. Oferecido como um dispositivo físico ou virtual, o DSM permite que seus administradores gerenciem centralmente a criptografia em milhares de bancos de dados e possui certificação FIPS 140-2 (todos os três níveis).

Vormetric Transparent Encryption

O Vormetric Transparent Encryption fornece para sua equipe de segurança criptografia no nível de arquivo, controle de acesso e inteligência de segurança. O Vormetric Transparent Encryption pode ser implantado sem ter que re-arquitetar aplicativos, infraestrutura ou práticas. Os bancos de dados podem ser protegidos no nível de arquivo ou volume.

Vormetric Application Encryption

A Vormetric Application Encryption facilita a adição de criptografia no nível de coluna a um aplicativo de banco de dados existente. As equipes de desenvolvimento podem implementar a solução sem precisar adquirir experiência em criptografia ou gerenciamento de chaves. Com a Vormetric Application Encryption, sua organização pode proteger dados confidenciais em campos ou colunas em qualquer banco de dados. Você pode criptografar os dados antes de serem gravados no banco de dados - e garantir que eles sejam criptografados no servidor de aplicativos, em trânsito e no banco de dados.

Vormetric Tokenization com mascaramento dinâmico de dados

A Vormetric Tokenization facilita a proteção de campos confidenciais nos bancos de dados. Também fornece proteção para dados em uso com mascaramento de dados dinâmicos com base em políticas.

CipherTrust Cloud Key Manager para serviços em nuvem

Com o CipherTrust Cloud Key Manager, sua organização pode estabelecer controles bem definidos sobre as chaves de criptografia e as políticas que regulam a criptografia de bancos de dados por serviços em nuvem. O CipherTrust Cloud Key Manager centraliza o gerenciamento de chaves de criptografia em vários ambientes de nuvem, oferecendo uma variedade de recursos de automação do ciclo de vida das chaves.

Benefícios da criptografia de banco de dados Thales

As soluções de criptografia de banco de dados Thales oferecem vários benefícios chave:

Simplicidade administrativa

As soluções ajudam a minimizar o tempo e o esforço associados à implementação e manutenção da criptografia do banco de dados com uma plataforma unificada e centralizada para gerenciar a criptografia de dados em repouso e o gerenciamento de chaves em uma empresa.

Implementação flexível e ampla cobertura de ambiente

Ao utilizar a implementação flexível de políticas centralizadas e gerenciamento de chaves da Thales, você pode abordar políticas de segurança e requisitos de conformidade em bancos de dados e arquivos - estejam eles localizados em nuvem, em infraestruturas virtuais ou em infraestruturas tradicionais. As soluções da Thales oferecem flexibilidade significativa na implementação da segurança na nuvem, se você deseja usar chaves geradas em seu próprio HSM, gerenciar chaves criadas no seu provedor de nuvem ou criptografar dados no local antes de enviá-los para a nuvem. Qualquer que seja a abordagem necessária, sua organização mantém o controle sobre chaves e dados.

Aplicação de política granular de acesso de usuário privilegiado

Com a Vormetric Transparent Encryption, as equipes de segurança podem aplicar políticas granulares de acesso de usuário com menos privilégios - por usuário, processo, tipo de arquivo, hora do dia e outros parâmetros. As equipes de segurança podem controlar não apenas se os usuários têm acesso a dados em texto claro, mas quais comandos do sistema de arquivos estão disponíveis. As organizações podem criar uma camada de separação entre sistemas e os dados que possuem. Dessa maneira, as equipes de segurança podem permitir que os administradores gerenciem configurações e manutenção contínua em servidores de banco de dados específicos, sem poder visualizar os dados confidenciais que residem nesses sistemas.

Suporte a dados estruturados e não estruturados

As soluções de criptografia de banco de dados da Thales fornecem à sua organização de TI um método consistente e repetível para gerenciar criptografia, chaves, políticas de acesso e inteligência de segurança para todos os dados estruturados e não estruturados.

Controles abrangentes de conformidade e trilhas de auditoria

Os logs detalhados de auditoria de acesso a dados fornecidos pela Vormetric Transparent Encryption ajudam a lidar com muitos controles gerais de conformidade e regulamentação para criptografia de dados, soberania de dados, política de menor privilégio e auditoria de acesso a dados. Os logs de inteligência podem provar a um auditor que as políticas de criptografia, gerenciamento de chaves e acesso estão funcionando de maneira eficaz. Os logs também revelam quando usuários e processos acessam dados, sob quais políticas, se as solicitações foram permitidas ou negadas, e mesmo quando um usuário privilegiado envia um comando como "alternar usuário" para tentar imitar outro usuário. Por fim, a integração pré-construída nos principais sistemas de Gerenciamento de Informações e Eventos de Segurança (SIEM) significa que os dados de log são imediatamente acionáveis.

Ambientes de dados suportados

Banco de dados: IBM DB2, Microsoft SQL Server, MongoDB, MySQL, NoSQL, Oracle, Sybase, Big Data: Hadoop, NoSQL, SAP HANA, Teradata

Saiba mais

Visite www.cpl.thalesgroup.com para saber mais sobre como podemos ajudá-lo a proteger seus bancos de dados confidenciais.

Sobre a Thales

As pessoas em quem você confia para proteger sua privacidade confiam na Thales para proteger seus dados. Em termos de segurança de dados, as organizações enfrentam cada vez mais momentos decisivos. Seja na criação de uma estratégia de criptografia, migração para a nuvem ou cumprimento de normas de conformidade, você pode confiar na Thales para proteger sua transformação digital.

Tecnologia decisiva para momentos decisivos.

> cpl.thalesgroup.com <

Américas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel.:+1 888 343 5773 ou +1 512 257 3900 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Ásia-Pacífico – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel.:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europa, Oriente Médio e África – 350 Longwater Ave, Green Park,Reading, Berkshire, RG2 6GF, United Kingdom • Tel.:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com