

CipherTrust Cloud Key Manager



Muitas infraestruturas, plataformas e provedores de software como serviço oferecem recursos de criptação de dados em repouso com chaves de criptografia gerenciadas pelo provedor de serviços. Entretanto, muitas normas de proteção de dados internas ou da indústria, bem como melhores práticas do setor conforme definidas pela Cloud Security Alliance, exigem que as chaves sejam armazenadas e controladas remotamente, distantes do provedor de serviços de nuvem e das operações de criptografia associadas. Os provedores podem cumprir esses requisitos, oferecendo serviços "Bring Your Own Key" (BYOK - traga a sua própria chave) para permitir ao cliente controle das chaves usadas para criptografar seus dados. O controle de chaves pelo cliente permite separação, criação, apropriação e controle, incluindo a revogação de chaves de criptografia ou senhas de clientes usadas para criá-las.

Aproveitando as APIs BYOK do provedor de nuvem, o CipherTrust Cloud Key Manager reduz a complexidade do gerenciamento de chaves e os custos operacionais, oferecendo aos clientes controle do ciclo de vida das chaves de criptografia com gerenciamento centralizado e visibilidade. A solução pode ser implantada quase que instantaneamente usando o CipherTrust Cloud Key Manager como serviço ou pode ser instalada no ambiente do cliente para atender aos requisitos de conformidade mais rigorosos.

Tenha controle das suas chaves de criptografia em nuvem

- Agregue valor aos serviços de "traga sua própria chave" com gerenciamento de chaves com criptografia em nuvem de ciclo de vida completo
- Cumpra com os mais rigorosos requisitos de proteção de dados com validação de criação e armazenamento de chaves com certificação FIPS 140-2 de nível 3
- Ofereça maior eficiência com gerenciamento centralizado de chaves em ambientes de diversas nuvens
- Liberdade para escolher a implantação como serviço ou em ambiente do cliente



A necessidade do controle de chaves

O requisito de proteção de dados confidenciais em Infraestrutura, Plataforma e Software como Serviço (IaaS, PaaS e SaaS) resultou em ofertas de criptografia de provedor de nuvem mais amplas. Enquanto isso, a Cloud Security Alliance e analistas do setor afirmam que as chaves de criptografia devem ser mantidas pelos clientes. Os desafios de manter as chaves aumentam, com até centenas de chaves mestras por assinatura sendo protegidas e gerenciadas em diversas nuvens. Há também a necessidade de saber como, quando e por quem as chaves de criptografia são usadas. O CipherTrust Cloud Key Manager fornece gerenciamento completo do ciclo de vida das chaves para atender aos requisitos de gerenciamento completo e seguro de chaves em diversas nuvens.

O suporte de nuvens inclui:

- Microsoft Azure
- Microsoft Office365
- Microsoft Azure Stack
- Microsoft Azure e Nuvens Nacionais Azure da China e da Alemanha
- Amazon Web Services
- Salesforce.com

Forte segurança de chaves de criptografia

Controle de chaves pelo cliente apresenta requisitos para garantir a geração e o armazenamento de chaves. O CipherTrust Cloud Key Manager amplia a segurança do [Vormetric Data Security Manager](#) ou suporta módulos de segurança de hardware (HSM) para criar chaves e armazená-las com segurança FIPS 140-2. Com o requisito de mecanismos de segurança de chaves, como o armazenamento seguro de chaves de backup em nuvem, o CipherTrust Cloud Key Manager atua como um depósito de chaves para nuvens suportadas e permite o controle de metadados completos de chaves tanto durante o upload como para as chaves em uso.

Maior eficiência de TI

O CipherTrust Cloud Key Manager oferece diversos recursos para suporte com eficiência de TI melhorada.

- O gerenciamento centralizado de chaves lhe dá acesso a cada provedor de nuvem a partir de uma simples janela do navegador, incluindo contas ou assinaturas múltiplas
- A rotação automática de chave oferece maior eficiência de TI e melhor segurança de dados
- O login unificado para cada provedor fornece um mecanismo simples para conceder acesso de usuário a dados importantes. O login nos serviços em nuvem são autenticados e autorizados pelo provedor do serviço – não há exigência de login no banco de dados ou configuração AD ou LDAP
- Para cargas de trabalho que exigirem, o CipherTrust Cloud Key Manager pode solicitar a criação de chaves no provedor de nuvem *nativo* e fornecer gerenciamento de ciclo de vida completo para elas

- Com diversas tecnologias e terminologias chave, o CipherTrust Cloud Key Manager apresenta operações importantes na semântica do provedor de nuvem
- Já criou milhares de chaves em seu provedor de nuvem? O CipherTrust Cloud Key Manager sincronizará seu banco de dados com chaves criadas no provedor de nuvem.

As ferramentas de conformidade que você precisa

Os registros específicos de nuvem do CipherTrust Cloud Key Manager e os relatórios previamente programados fornecem relatórios de rápida conformidade. Os registros também podem ser direcionados para um servidor syslog ou SIEM.

Software como serviço

O CipherTrust Cloud Key Manager como serviço combina a simplicidade de uma solução baseada em nuvem com o controle requerido pelas normas de conformidade internas e da indústria. O recurso como serviço elimina a necessidade de instalar e manter uma solução de gerenciamento de chaves em nuvem de alta disponibilidade no ambiente do cliente, com a geração e o armazenamento de chaves locais com certificação FIPS 140-2 de nível 1.

Opções de instalação no local

O CipherTrust Cloud Key Manager também está disponível em fatores de forma adequados para uma variedade de opções de implantação em ambiente do cliente com segurança de chaves com certificação FIPS 140-2 de nível 3. As aplicações virtuais estão disponíveis no Azure Marketplace e para Amazon Web Services e VMware.

Soluções para seguranças de dados de nuvem múltipla

O CipherTrust Cloud Key Manager simplifica a necessidade de manter e gerenciar chaves de criptografia para serviços em nuvem, uma solução essencial para o cumprimento das normas de proteção de dados organizacionais e da indústria. Os produtos de segurança em nuvem múltipla da Thales eSecurity, incluindo o [Bring Your Own Advanced Encryption](#) (Traga sua própria criptografia avançada), todos com gerenciamento de chaves centralizado, validados pela certificação FIPS, permitem que você criptografe e controle o armazenamento em nuvem para reduzir a possibilidade de vazamento dos seus 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 hora de criar uma estratégia de criptografia, migrar para a nuvem ou cumprir normas de conformidade, você pode confiar na Thales para proteger sua transformação digital.

Tecnologia decisiva para momentos decisivos.