

Soluções Thales eSecurity para Amazon Web Services



Cargas de trabalho seguras em nuvem híbridas, incluindo Amazon Web Services

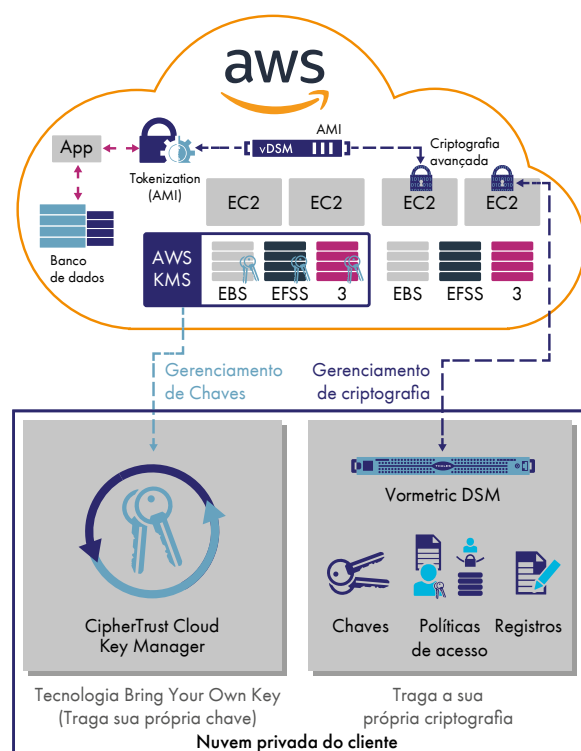
As cargas de trabalho de tecnologia da informação no Amazon Web Services (AWS) podem oferecer conveniência e economia. Porém, você ainda precisa seguir as regras de segurança, privacidade e conformidade, bem como as melhores práticas de proteção de dados. Além disso, você precisa de rapidez na mobilidade de dados em todas as nuvens que você usa atualmente e usará futuramente, uma necessidade que pode ser comprometida com soluções de criptografia específicas do provedor de nuvem.

Soluções de criptografia avançada com gerenciamento completo de chaves

O uso eficaz e seguro de serviços em nuvem envolve muitos momentos decisivos; por exemplo, como quando você considera usar dados sensíveis em uma nuvem. Você pode confiar na Thales para proteger sua transformação digital. As soluções de criptografia avançada e gerenciamento centralizado de chaves proporcionam proteção e controle dos dados armazenados em seu ambiente, no Amazon Web Services, e em outros provedores de nuvem. As tecnologias Thales permitem que você:

- Evite o bloqueio da solução de criptografia em nuvem do fornecedor e garanta a mobilidade dos dados que você precisa enquanto distribui cargas de trabalho e dados de forma eficiente e segura entre vários fornecedores de nuvem, inclusive o Amazon Web Services, com gerenciamento de criptografia independente e centralizado
- Aproveite as vantagens seguras do Amazon Key Management Services (AWS KMS) com uma solução de gerenciamento centralizado de chaves que abrangem múltiplas nuvens

- Identifique os ataques mais rapidamente com registro de acesso a dados de aplicativos SIEM líderes do setor
- Reduza ou elimine os riscos decorrentes de credenciais comprometidas com criptografia avançada, incluindo controles de acesso de usuário privilegiado
- Desenvolva suas aplicações para nuvem com recursos de segurança integrados, usando tokenização vaultless com mascaramento dinâmico de dados



Criptografia avançada para Amazon Web Services e outros

Se sua base for 100% do Amazon Web Services com controles rigorosos de segurança de dados, ou se você estiver executando nuvens híbridas com dados distribuídos em sua nuvem privada, em provedores de nuvem múltipla, você precisa de uma solução de criptografia de dados avançada. A Vormetric Transparent Encryption protege seus arquivos e banco de dados armazenados em instalações e em nuvens múltiplas, incluindo o AWS, sem qualquer alteração em aplicativos, banco de dados, infraestrutura ou práticas comerciais.

Vormetric Transparent Encryption:

- Reforça a segurança dos dados com controles de acesso não autorizado baseado em políticas granulares de acesso de usuários, incluindo a identidade do usuário (inclusive para administradores com privilégios root), e processo, dentre muitos outros
- Acelera a detecção de violação e satisfaz as normas de conformidade com registros detalhados de acesso a arquivos. Você pode direcionar os registros para o seu sistema de gerenciamento de eventos e informações de segurança (SIEM)
- Entrega um retorno sobre investimento mais rápido com uma implementação flexível e não invasiva. Os agentes de criptografia operam nas instâncias de computação do AWS EC2 ou de qualquer outro servidor que acesse o armazenamento, protegem o armazenamento EBS, EFS e S3, e estão disponíveis para muitas versões do Windows e distribuições Linux, inclusive do Amazon Linux.

Gerenciamento de chaves centralizado e seguro

O [Vormetric Data Security Manager](#) fornece gerenciamento centralizado de chaves, gerenciamento de políticas e registros da Vormetric Transparent Encryption, disponível como um equipamento FIPS 140-2 de nível 2 ou 3 ou um aplicativo virtual FIPS 140-2 nível 1. O equipamento físico é apropriado para ambientes locais do cliente para gerenciar agentes de criptografia do mundo inteiro em qualquer provedor de nuvem. O aplicativo virtual está disponível em muitos formatos de virtualização, incluindo VMware e KVM, bem como Amazon Web Services AMI e no Azure Marketplace.

Conformidade acelerada PCI-DSS

A solução [Vormetric Tokenization com Mascaramento Dinâmico de Dados](#) protege e anonimiza ativos sensíveis em data center, ambientes de big data ou nuvem para conformidade simplificada do Padrão de Segurança de Dados da Indústria de Cartão de Pagamento (PCI-DSS). A tokenização com preservação de formato ou aleatória protege os campos sensíveis e mantém a estrutura do banco de dados para uma implementação não-disruptiva. Assim, é fácil adicionar uma política de mascaramento dinâmico de dados aos seus aplicativos.

O Vormetric Tokenization Server está disponível como AWS AMI compartilhado.

Gerenciamento de chaves de criptografia AWS

As organizações 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 aproveita as APIs Traga sua própria chave (BYOK) do provedor de nuvem para diminuir a complexidade do gerenciamento de chaves e os custos operacionais, oferecendo aos clientes controle do ciclo de duração das chaves de criptografia com gerenciamento centralizado e visibilidade. A solução pode ser instalada rapidamente utilizando-se o CipherTrust Cloud Key Manager como serviço, e está disponível como AWS AMI compartilhado, ou pode ser instalada no ambiente do cliente ou em qualquer instalação de nuvem privada compatível para atender aos requisitos de conformidade mais rigorosos.

O CipherTrust Cloud Key Manager oferece as seguintes vantagens:

- Práticas de gerenciamento de chaves mais seguras combinadas com os benefícios de escala, custo e conveniência da nuvem
- Maior controle sobre as chaves—você comanda a geração, o armazenamento e a exportação das chaves usadas no KMS do AWS, no Microsoft Azure, e mais!
- Melhore a eficiência da TI com gerenciamento de chave de nuvem múltipla a partir de um único controle que faz rotação automática da chave e gerenciamento do ciclo de vida completo da chave

Cumpra seus requisitos de proteção

A Thales eSecurity simplifica a segurança das cargas de trabalho dos seus Serviços de Web da Amazon (AWS) para ajudá-lo a cumprir a conformidade com os regulamentos de segurança de dados. Os produtos da Vormetric Data Security Platform operam cargas de trabalho sem impactos no AWS e em suas instalações físicas, oferecendo política de centralização e gerenciamento de chaves. E a solução de gerenciamento de chaves em nuvem múltipla da Thales eSecurity lhe proporciona a conformidade com as melhores práticas e requisitos de proteção de dados.

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.

> thalesecurity.com <



Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel.: +1 888 744 4976 ou +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalessec.com
Ásia-Pacífico – Thales Transport & Security (HK) Ltd, 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 – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel.: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com