thalesesecurity.com

THALES

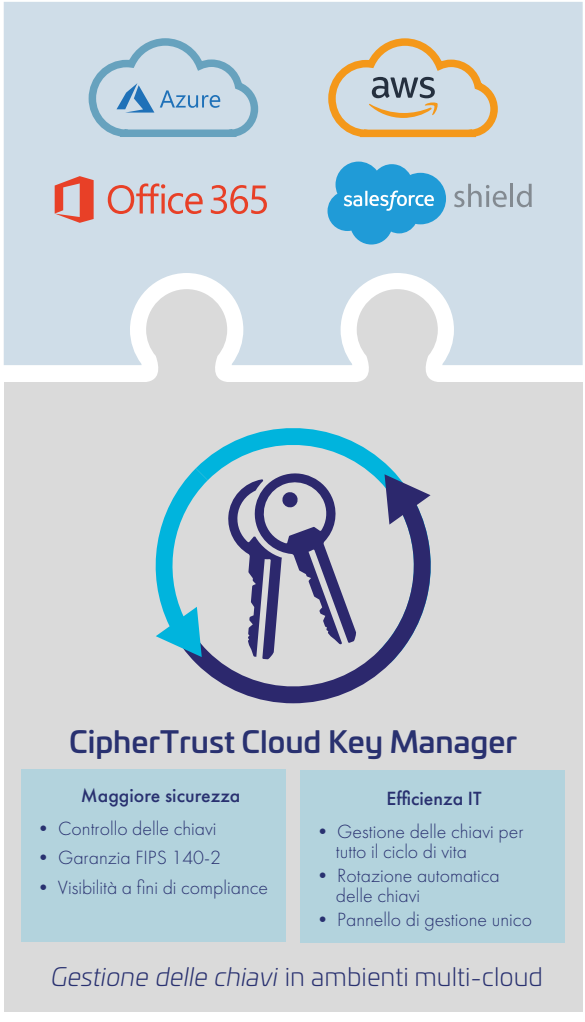
CipherTrust Cloud Key Manager

Numerosi provider di infrastrutture, di piattaforme e di software erogati come servizi (IaaS, PaaS e SaaS) offrono funzionalità di crittografia dei dati a riposo con gestione delle chiavi di crittografia a cura del fornitore del servizio. Tuttavia, molti obblighi sulla protezione dei dati del settore o interni alle aziende, nonché le buone pratiche del settore definite dalla Cloud Security Alliance, impongono che l'archiviazione e la gestione delle chiavi da remoto, e le operazioni di crittografia associate, spettino al provider di servizi cloud. I provider possono soddisfare questi requisiti offrendo servizi "Bring Your Own Key" (BYOK) che permettono ai clienti di avere il controllo delle chiavi utilizzate per cifrare i loro dati. Il controllo delle chiavi da parte del cliente consente la separazione, la creazione, il possesso e il controllo, nonché la revoca, delle chiavi di crittografia o dei segreti tenant utilizzati per la loro creazione.

Il CipherTrust Cloud Key Manager sfrutta le API BYOK del provider di servizi cloud per ridurre la complessità e i costi operativi della gestione delle chiavi, offrendo ai clienti il controllo delle chiavi di crittografia per tutto il loro ciclo di vita con una visibilità e una gestione centralizzate.

Assumi il controllo delle tue chiavi crittografiche nel cloud

- Sfrutta il valore dei servizi "Bring Your Own Key" con la gestione delle chiavi crittografiche nel cloud per tutto il loro ciclo di vita
- Rispetta gli obblighi più severi in materia di protezione dei dati tramite la creazione e l'archiviazione di chiavi conformi fino al livello 3 della certificazione FIPS 140-2
- Migliora l'efficienza in ambito IT affidandoti a una gestione centralizzata delle chiavi in ambienti multi-cloud



Il controllo delle chiavi è indispensabile

Il requisito di protezione dei dati sensibili in tutte le soluzioni Infrastructure-as-a-Service, Platform-as-a-Service e Software-as-a-Service (IaaS, PaaS e SaaS) ha comportato un ampliamento delle offerte di crittografia dei provider di servizi cloud. Nel frattempo, la Cloud Security Alliance e gli analisti del settore sostengono che le chiavi di crittografia debbano essere conservate dai clienti. Le problematiche della conservazione delle chiavi aumentano quando si devono proteggere e gestire fino a centinaia di chiavi master su più cloud. Inoltre, vi è la necessità di sapere come, quando e da chi vengono utilizzate le chiavi di crittografia. Il CipherTrust Cloud Key Manager permette una gestione completa delle chiavi per tutto il loro ciclo di vita al fine di soddisfare i relativi requisiti di sicurezza a livello multi-cloud.

I cloud supportati includono:

- Microsoft Azure
- Microsoft Office365
- Microsoft Azure Stack
- Cloud nazionali Microsoft Azure Cina e Germania
- Amazon Web Services
- Salesforce.com
- Salesforce Sandbox

Elevata protezione delle chiavi di crittografia

Il controllo delle chiavi da parte del cliente presenta la necessità di generarle e archiviarle in sicurezza. CipherTrust Cloud Key Manager sfrutta la sicurezza del Vormetric Data Security Manager o degli hardware security module (HSM) per creare chiavi e archiviarle secondo lo standard di sicurezza FIPS 140-2. Grazie al requisito di meccanismi di sicurezza delle chiavi, come l'archiviazione sicura di chiavi di backup su cloud, CipherTrust Cloud Key Manager agisce da key escrow per i cloud supportati e consente il controllo completo dei metadati delle chiavi sia durante l'upload che per le chiavi in uso.

Maggiore efficienza IT

CipherTrust Cloud Key Manager offre funzionalità di vario tipo a sostegno di un'efficienza IT di livello superiore:

- La gestione centralizzata delle chiavi consente l'accesso a ciascun provider di servizi cloud da un'unica finestra del browser, anche su più account o sottoscrizioni
- La rotazione automatica delle chiavi garantisce efficienza IT e migliore sicurezza dei dati
- Il login federato fornisce un meccanismo semplice per concedere l'accesso ai dati delle chiavi. Gli accessi ai servizi cloud vengono autenticati e autorizzati dal provider del servizio. Non sono necessari database di accessi né configurazioni LDAP o AD
- Per i carichi di lavoro che lo richiedono, CipherTrust Cloud Key Manager può imporre la creazione di chiavi del provider di servizi cloud *native* e fornirne la gestione per l'intero ciclo di vita
- Poiché le tecnologie e la terminologia delle chiavi variano, CipherTrust Cloud Key Manager presenta il funzionamento delle chiavi nella semantica del provider di servizi cloud
- Hai già creato migliaia di chiavi affidandole al tuo provider di servizi cloud? CipherTrust Cloud Key Manager effettuerà la sincronizzazione del suo database con le chiavi in mano al provider di servizi cloud

Gli strumenti di conformità necessari

I file di log e i report preconfezionati specifici del cloud di CipherTrust Cloud Key Manager permettono la creazione rapida di report di compliance. I file di log possono essere anche diretti a un server syslog o a un sistema SIEM.

Opzioni di implementazione in linea con le singole esigenze

CipherTrust Cloud Key Manager offre varie possibilità di implementazione pratica per soddisfare le tue esigenze in materia di sicurezza e deployment:

- Tutti i software presentano il certificato di protezione delle chiavi FIPS 140-2 livello 1. È possibile creare un'istanza sia dell'appliance virtuale CipherTrust Cloud Key Manager che del Data Security Manager virtuale su Amazon Web Services e Microsoft Azure oppure implementarli in un qualsiasi cloud pubblico o privato utilizzando VMware.
- I clienti che abbiano necessità di una sicurezza FIPS 140-2 livello 3 o 2 possono implementare o utilizzare le appliance Vormetric Data Security Manager esistenti o gli HSM supportati nei data center on premise o ospitati.

Soluzioni per la sicurezza dei dati multi-cloud

CipherTrust Cloud Key Manager semplifica la necessità di avere e gestire chiavi di crittografia per i servizi sul cloud, una soluzione cruciale per soddisfare gli obblighi del settore e interni all'organizzazione in materia di protezione dei dati. Altri prodotti di Thales eSecurity per la sicurezza multi-cloud, tra cui Bring Your Own Advanced Encryption, sono tutti dotati di una gestione delle chiavi centralizzata con certificazione FIPS, che permette di cifrare e controllare l'archiviazione sul cloud per ridurre la possibilità di fuga di dati sensibili in azienda.

Informazioni su Thales

Le persone a cui ti affidi per tutelare la tua privacy si affidano a Thales per proteggere i propri dati. Le organizzazioni si ritrovano ad affrontare sempre più spesso momenti decisivi in materia di sicurezza dei dati. Qualunque sia l'obiettivo del momento, dal creare una strategia di crittografia al passare al cloud o garantire il rispetto degli obblighi di compliance, puoi contare su Thales per proteggere la tua trasformazione digitale.

Tecnologia decisiva per momenti decisivi.

> thalesesecurity.it <

Americhe – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel: +1 888 744 4976 o +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia-Pacifico – 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@thalesesecurity.com
Europa, Medio Oriente, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ, Regno Unito • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thalesesecurity.com