cpl.thalesgroup.com

THALES

CipherTrust Manager

Panoramica

CipherTrust Manager permette alle organizzazioni una gestione centralizzata delle chiavi di crittografia per Thales CipherTrust Data Securiy Platform e prodotti di terze parti. Semplifica le attività di gestione delle chiavi per il ciclo di vita, inclusa una generazione sicura delle chiavi, il backup e il ripristino, il clustering, la disattivazione e l'eliminazione.

Fornisce un controllo dell'accesso sulle chiavi e sui criteri basato sui ruoli, un'assistenza multi-tenancy e relazioni e audit solidi di tutte le operazioni di gestione e codifica delle chiavi.

CipherTrust Manager è il punto di gestione centrale per CipherTrust Data Security Platform. La console unica di gestione facilita la scoperta e la classificazione dei dati e permette di proteggere dati sensibili ovunque si trovino utilizzando un set completo di connettori CipherTrust Data Protection di Thales.

CipherTrust Manager è disponibile in fattori di forma sia virtuali che fisici che possono utilizzare Thales Luna o moduli di sicurezza hardware (HSM) di terze parti con certificazione FIPS 140-2 per archiviare in tutta sicurezza chiavi master con un solido root-of-trust. Queste appliance possono essere implementate on premise come anche in infrastrutture cloud private o pubbliche. Ciò consente ai clienti di affrontare i requisiti normativi e di compliance, nonché le best practice del settore in materia di sicurezza dei dati.

Vantaggi

- Una gestione centralizzata delle chiavi e delle politiche per vari archivi di dati e infrastrutture cloud on premise
- Rischio aziendale ridotto grazie a data unificato, classificazione e protezione di dati sensibili
- Gestione semplificata grazie ad un portale di licenza self-service e alla visibilità sulle licenze in uso
- Opzioni di deployment cloud-friendly con il supporto per AWS, Azure, Google Cloud VMware , Oracle Cloud Infrastructure e altri
- Un supporto esteso dell'hardware security module (HSM) per un maggiore controllo delle chiavi
- Un ineguagliabile ecosistema di partner di integrazioni con un'archiviazione aziendale, server, database, applicazione e provider SaaS leader del settore

Funzionalità essenziali

- **Gestione dell'intero ciclo di vita delle chiavi e operazioni automatiche:** CipherTrust Manager semplifica le attività di gestione delle chiavi di crittografia per tutto il loro ciclo di vita, inclusa una generazione sicura delle chiavi, il backup e il ripristino, il clustering, la disattivazione e l'eliminazione. Facilita le operazioni automatiche basate su criteri e genera segnalazioni per eventi rilevanti.
- **Amministrazione e controllo degli accessi centralizzati:** Uniforma le operazioni di gestione delle chiavi con un controllo degli accessi basato sui ruoli e fornisce una revisione completa dei protocolli degli audit. Autentica e autorizza gli amministratori e gli utenti delle chiavi che utilizzano credenziali AD e LDAP.
- **Data Discovery and Classification:** Fornisce una console unica per data discovery e classificazione di dati sensibili integrata con un set completo di connettori di protezione dei dati per la crittografia o la tokenizzazione dei dati al fine di ridurre i rischi aziendali e aderire alle normative di compliance.
- **Licenze self-service:** Ottimizzazione della distribuzione di licenze dei connettori tramite un portale di licenze rivolto ai clienti. La nuova console di gestione offre una visibilità e un controllo migliorati delle licenze in uso.
- **Gestione segreti:** Offre la capacità di creare e gestire oggetti segreti e opachi da utilizzare sulla piattaforma.
- **Assistenza multi-tenancy:** Offre le funzionalità necessarie per creare numerosi domini con una separazione di compiti per assistere organizzazioni di grandi dimensioni con sedi distribuite.
- **API REST facili da usare per gli sviluppatori:** Offre nuove interfacce REST, oltre alle API KMIP e NAE-XML, permette ai clienti di generare e gestire le chiavi da remoto.
- **Clustering HA flessibile e condivisione delle chiavi intelligente:** Offre l'opzione di effettuare il clustering contemporaneo di appliance fisiche e/o virtuali per garantire un'elevata disponibilità come anche un più elevato volume di transazioni crittografate.
- **Relazioni e audit solidi:** Include il monitoraggio di tutti i cambiamenti degli stati delle chiavi, l'accesso degli amministratori e i cambiamenti dei criteri in vari format di protocollo (RFC-5424, CEF, LEEF) per un'integrazione semplificata con gli strumenti SIEM. Inoltre, i clienti possono generare avvisi via e-mail preconfigurati / personalizzabili. Gli audit trail vengono archiviati in sicurezza e viene garantita la non disconoscibilità.
- **Interfacce veloci con l'NIC Bonding:** Le nuove appliance k470 e k570 forniscono schede di interfacce di rete (NIC) opzionali da 2x1 GB / 2x10 GB, come anche un bonding NIC per aumentare la larghezza di banda disponibile.
- **Diversi casi d'uso di crittografia:** CipherTrust Manager supporta un set completo di casi d'uso di crittografia e tokenizzazione grazie ai connettori CipherTrust Data Security Platform e un ecosistema di partner.

Per saperne di più

Altre soluzioni per la gestione delle chiavi di Thales

Specifiche delle appliance

Appliance fisici di CipherTrust Manager

Caratteristica	k470	k570
Numero massimo di chiavi	1.000.000	1.000.000
Numero massimo di sessioni concomitanti	1.000	1.000
Certificazione FIPS 140-2	Si integra con Thales Luna Network e Cloud HSM e HSM di terze parti	Dotato di FIPS 140-2 Livello 3 HSM incorporato
Opzioni di schede di interfacce di rete (NIC)	• 4x1 GB • 2x1 GB / 2x10 GB • Supporto di bonding NIC incluso	
API supportate	• REST • JCE • NAE-XML • NET	• REST • JCE • NAE-XML • NET

Appliance virtuali di CipherTrust Manager

Caratteristica	k170v	k470v
Numero massimo di chiavi	25.000	1.000.000
Numero massimo di sessioni concomitanti	100	1.000
Requisiti di sistema	• HD: 100 GB • RAM: 4-8 GBB • NIC: 1 -2 • CPU: 2 o più	• HD: 200 GB o più • RAM: 16 GB o più • NIC: 2 o più • CPU: 4 o più
Certificazione FIPS 140-2	• Certificazione di livello 1 in sviluppo • Integrabile con HMS FIPS 140-2 L3 come root-of-trust	
API supportate	• REST • NAE-XML • KMIP • PKCS#11 • JCE,.NET,MSCAPI, MS CNG, NAE-XML	
Cloud Provider supportati	• AWS • Microsoft Azure • Google Cloud	• OpenStack • Hyper-V • Oracle

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, potete contare su Thales per proteggere la vostra trasformazione digitale.

Tecnologia decisiva per momenti decisivi.

> cpl.thalesgroup.com <

Contattaci – Visita la pagina cpl.thalesgroup.com/it/contact-us per ottenere tutte le sedi degli uffici Thales e le informazioni per contattarci.