nShield Bring Your Own Key offre ai clienti un maggiore controllo sulla sicurezza dei dati nel cloud

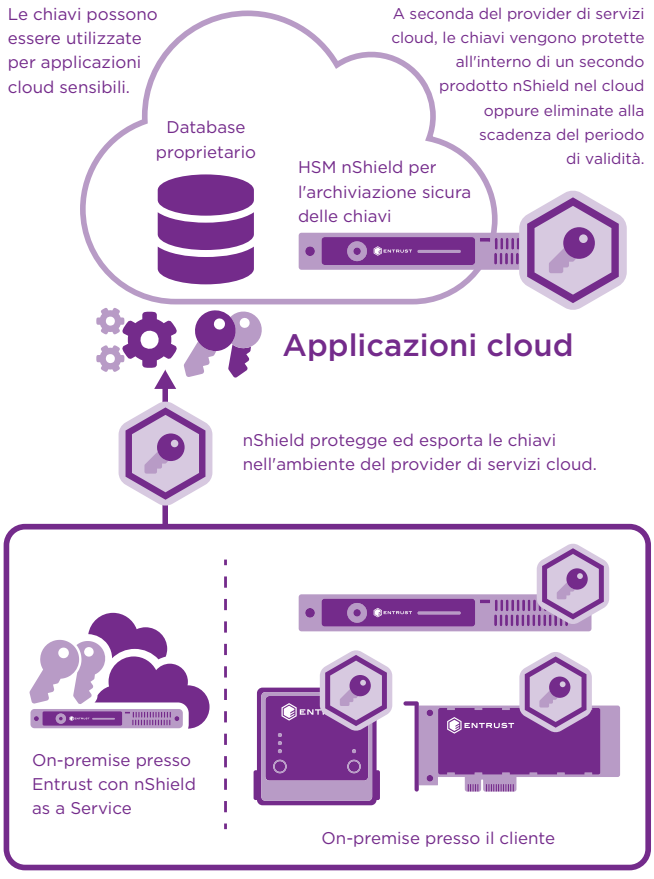
Tutti i vantaggi del cloud con un livello elevato di sicurezza

IN EVIDENZA

- Processi di gestione delle chiavi che aumentano la sicurezza dei dati sensibili nel cloud
- Maggiore affidabilità delle procedure di creazione delle chiavi grazie al generatore di numeri casuali a elevata entropia nShield® di Entrust, protetto da hardware certificato secondo lo standard FIPS
- Maggiore controllo sulle chiavi: i clienti utilizzano i propri hardware security module (HSM) nShield all'interno del loro ambiente per creare ed esportare le chiavi al cloud in tutta sicurezza
- Attività di gestione delle chiavi più coerenti, nel cloud e on-premise

Gli HSM nShield consentono alle aziende che si affidano ad Amazon Web Services (AWS), Google Cloud Platform (GCP) o Microsoft Azure di adottare un modello Bring Your Own Key (BYOK) per le proprie applicazioni cloud.

Caratterizzati da un livello elevato di affidabilità, i prodotti della serie nShield permettono di sfruttare la flessibilità e i costi contenuti dei servizi cloud, consolidando al tempo stesso la sicurezza dei processi di gestione delle chiavi e offrendo ai clienti un maggiore controllo.



L'esclusiva architettura Security World di Entrust offre un'archiviazione sicura a lungo termine delle chiavi master e funzionalità di disaster recovery

SCOPRI DI PIÙ SU ENTRUST.COM/HSM

Maggiore controllo sulla sicurezza dei dati nel cloud

Funzionalità di nShield BYOK

nShield BYOK si affida agli HSM nShield per generare, archiviare e gestire le chiavi utilizzate a protezione delle applicazioni, dei database e delle soluzioni di archiviazione più sensibili con hosting nel cloud. Tra le capacità offerte dalla soluzione spiccano:

- La garanzia di una root of trust hardware: certificati secondo lo standard FIPS 140-2 di livello 3, gli HSM nShield sono dispositivi a prova di manomissione che garantiscono un livello elevato di affidabilità. Costituiscono la root of trust dei servizi cloud dei clienti e consentono di generare e proteggere in maniera sicura le chiavi di crittografia e di firma.

- La possibilità di utilizzare i prodotti nShield per la gestione delle chiavi: gli HSM nShield generano e proteggono le chiavi, rendendole accessibili in tutta sicurezza da parte delle applicazioni con hosting nel cloud che contengono dati sensibili.

- Il controllo sulla disponibilità delle chiavi: che siano implementati on-premise o in un ambiente nShield as a Service, gli HSM nShield rimangono nelle mani del cliente, che può decidere in autonomia quando generare ed esportare le chiavi. Grazie al controllo sulla copia master, è il cliente a stabilire se e quando sono necessarie ulteriori esportazioni al provider di servizi cloud.

- La possibilità di scegliere il fornitore di servizi cloud: nShield BYOK lascia ai clienti la scelta del provider da utilizzare per ciascuna chiave. In questo modo, ciascun cliente può individuare il cloud più adatto agli ambienti nShield on-premise o as a Service delle proprie applicazioni, traendo vantaggio dai processi di generazione e protezione delle chiavi garantiti dai prodotti nShield.

Requisiti per utilizzare nShield BYOK

Per iniziare a usare nShield BYOK con AWS, GCP o Azure, è necessario disporre di un HSM nShield. Le soluzioni offerte comprendono:

- nShield Connect, un'appliance collegata alla rete
- nShield Solo, una scheda PCIe da incorporare all'interno del server
- nShield Edge, un dispositivo con collegamento USB per applicazioni a volume ridotto
- nShield as a Service, una soluzione in abbonamento per l'accesso agli HSM nShield Connect

Entrust BYOK permette di ottenere la massima sicurezza con Microsoft Azure. Consultare: **https://protect-eu.mimecast.com/s/PYBnCWnYocOBORVImMJzG?domain=docs.microsoft.com** È possibile acquistare il pacchetto seguente per ricevere assistenza con il deployment:

Bring Your Own Key,
Azure Professional Services
Questo pacchetto include un HSM nShield Edge, assistenza all'integrazione da parte del personale dei servizi professionali di Entrust e un anno di manutenzione.

Gli HSM delle serie nShield Connect, Solo ed Edge e i servizi professionali possono essere acquistati separatamente.

Il seguente pacchetto Entrust è necessario per utilizzare nShield BYOK con AWS, GCP o Microsoft Azure mediante il metodo a standard aperti di Microsoft:

Cloud Integration Option Pack
Questo option pack contiene quanto necessario a utilizzare gli HSM nShield on-premise per generare e trasferire le chiavi ad AWS o GCP.

Il cliente può occuparsi da sé dell'integrazione di nShield BYOK con AWS, GCP o Azure oppure affidarsi all'esperienza del personale dei servizi professionali di Entrust.

Maggiore controllo sulla sicurezza dei dati nel cloud

Funzionamento di nShield BYOK

Entrust garantisce i meccanismi che rendono possibile l'uso degli HSM nShield per generare le chiavi, proteggerle durante l'archiviazione a lungo termine ed esportarle nel cloud. Una volta esportate nel cloud da una soluzione nShield on-premise o as a Service, la gestione è affidata al cliente secondo uno degli approcci seguenti:

Con Microsoft Azure come provider...
Entrust BYOK permette di ottenere la massima sicurezza con Microsoft Azure, perché controlla le condizioni che devono essere rispettate per permettere di caricare la chiave in Azure e impone restrizioni severe alle attività consentite a Microsoft dopo il caricamento.

Il cliente trasferisce le chiavi all'HSM nShield in esecuzione all'interno dell'infrastruttura Azure, dove garantisce la sicurezza dell'intero processo.

Con AWS o GCP come provider...
Il cliente concede in lease le chiavi ad AWS o GCP per l'uso temporaneo nel cloud. Dopo un periodo prestabilito, le chiavi nel cloud vengono distrutte, ma, se necessario, il cliente può rinnovare il lease.

Grazie alla responsabilità di generazione delle proprie chiavi e al controllo delle esportazioni, il cliente può introdurre misure efficaci a protezione dei dati e delle applicazioni nel cloud, indipendentemente dal servizio di cloud pubblico scelto.

HSM Entrust

Gli HSM nShield di Entrust sono tra le soluzioni HSM disponibili sul mercato più performanti, sicure e facili da integrare; inoltre, favoriscono la conformità normativa e forniscono una sicurezza comprovata per i dati e le applicazioni aziendali, finanziarie e governative. La nostra esclusiva architettura di gestione delle chiavi Security World offre un controllo forte e granulare sull'accesso e sull'utilizzo delle chiavi.

Scopri di più

Per ulteriori informazioni sugli HSM nShield di Entrust, visita il sito **entrust.com/HSM**. Per saperne di più sulle soluzioni di sicurezza digitale di Entrust per identità, accesso, comunicazioni e dati, visita il sito **entrust.com**

Scopri di più sugli HSM nShield di Entrust:

HSMinfo@entrust.com

entrust.com/HSM

ENTRUST CORPORATION

Entrust permette al mondo di continuare ad avanzare in sicurezza attraverso sistemi di identificazione, pagamento e protezione dei dati ad alta affidabilità. Oggi più che mai, le persone si aspettano esperienze sicure e ottimizzate, che si tratti di attraversare le frontiere tra Stati, effettuare un acquisto, accedere ai servizi elettronici della pubblica amministrazione o collegarsi a una rete aziendale. Entrust offre un'ineguagliabile gamma di soluzioni di sicurezza digitale ed emissione di credenziali, il vero fondamento di tutte queste interazioni. Con oltre 2.500 colleghi, una rete di partner globali e clienti in più di 150 Paesi, non sorprende che le organizzazioni più fidate al mondo scelgano noi.

Scopri di più su
entrust.com/HSM

Per contattarci:
HSMinfo@entrust.com