



ENTRUST

nShield as a Service

Accesso semplice ed efficiente alla crittografia "as a Service"

IN EVIDENZA

- Gestione e hosting di HSM per implementazioni su cloud
- Controllo totale sulle chiavi, ovunque le applicazioni siano in esecuzione
- Crittografia basata sul cloud e gestione delle chiavi in un ambiente multi-cloud
- Esecuzione sicura del codice di applicazioni in cloud
- Riduzione dei costi per le attività di sicurezza business-critical
- Riduzione dei costi e dei tempi di manutenzione e monitoraggio

Con la rapida evoluzione dell'ambiente IT odierno, l'adozione di un approccio "cloud first" è uno degli obiettivi strategici di molte organizzazioni. Ospitare l'infrastruttura IT critica on-premise è ormai una scelta che appartiene al passato. Il passaggio al cloud offre numerosi vantaggi alle organizzazioni, che possono affidarsi alla scalabilità, alla flessibilità e alla resilienza garantite dai provider di servizi cloud, oltre a contare su oneri di manutenzione ridotti e una spesa operativa mensile maggiormente prevedibile. Tale cambiamento comporta preoccupazioni aggiuntive quando le applicazioni sul cloud si basano su hardware security module (HSM), dispositivi a protezione delle chiavi di crittografia che costituiscono la root of trust dei dati crittografati di un'organizzazione.

Gli HSM rappresentano un elemento fondamentale dell'infrastruttura critica di un'organizzazione e contribuiscono a soddisfare i requisiti normativi o di certificazione; in passato venivano ospitati in data center on-premise e gestiti da un team addetto alla sicurezza in loco. A causa dei requisiti sempre più elevati imposti ai team aziendali addetti alla sicurezza, trovare professionisti qualificati in grado di amministrare gli HSM è una sfida costante. Il valore aggiunto di nShield as a Service, che offre le stesse caratteristiche e funzionalità degli HSM on-premise, risiede nel vantaggio dell'implementazione del servizio sul cloud, che consente ai clienti di raggiungere i propri obiettivi "cloud first", lasciando la gestione e la manutenzione dei dispositivi nelle mani degli esperti di Entrust.

Crittografia "as a Service"

nShield as a Service è una soluzione per la creazione, l'accesso e la protezione delle chiavi di crittografia, che vengono mantenute separate dai dati sensibili. La soluzione utilizza HSM nShield Connect dedicati certificati ai sensi dello standard FIPS 140-2 e eIDAS (EN 419 221-5). Il modello ospitato sul cloud consente alle organizzazioni di integrare o sostituire gli HSM nei loro data center, senza perdere i vantaggi derivanti dalla proprietà dei dispositivi. Grazie a nShield as a Service, le imprese possono destinare un budget più prevedibile per la sicurezza, gestire la capacità in base alla domanda, ridurre la portata dei data center e il tempo dedicato alle attività di monitoraggio e manutenzione ordinaria.

» nShield as a Service

I clienti interagiscono con gli HSM nShield basati sul cloud in modo del tutto analogo a dei dispositivi nei loro data center, senza la necessità di installazione e manutenzione dell'hardware. In questo modo, il tempo tra l'approvvigionamento iniziale e l'uso effettivo degli HSM risulta spesso più breve, con una conseguente implementazione più rapida delle applicazioni in tutta sicurezza.

In linea con la strategia e le esigenze di sicurezza della tua azienda

nShield as a Service è una soluzione flessibile che ben si adatta a strategie di sicurezza molto diverse, dal potenziamento della capacità dell'HSM per la gestione di picchi occasionali dei carichi di lavoro e la migrazione selettiva di servizi specifici al cloud, fino all'adozione di un approccio "cloud-first" per le funzioni di crittografia.

Dal momento che nShield as a Service si avvale della stessa ineguagliabile architettura Security World delle implementazioni on-premise nShield, i clienti possono utilizzare un approccio ibrido che combina sia nShield as a Service che HSM on-premise. nShield Security World è un framework scalabile per la gestione delle chiavi alla base delle soluzioni nShield. Garantisce un'esperienza unificata per gli amministratori e gli utenti e l'interoperabilità su tutti i dispositivi sia nel cloud sia on-premise.¹ In questo modo, la scalabilità degli HSM risulta facile ed efficiente, su misura per l'ambiente specifico, l'approccio operativo e le esigenze di sicurezza di ciascun cliente.

Grazie alla sicurezza dell'esecuzione garantita da CodeSafe, i clienti hanno accesso su richiesta a un numero maggiore di funzionalità di elaborazione sicure. Solo nShield as a Service consente ai clienti di eseguire agevolmente la migrazione dell'esecuzione sicura del loro codice da un HSM on-premise al cloud.

I vantaggi di nShield as a Service

Rispetto ad altre opzioni, nShield as a Service offre diversi vantaggi decisivi:

- I clienti sono proprietari delle risorse Security World e delle chiavi, da utilizzare nell'ambiente nShield sia "as a Service" sia on-premise.
- Solo nShield as a Service offre ai clienti il controllo su richiesta per la migrazione dell'esecuzione sicura del loro codice da un HSM on-premise al cloud.
- nShield as a Service garantisce una protezione delle chiavi certificata conforme allo standard FIPS 140-2 di livello 3 E eIDAS (secondo il profilo di protezione EN 419 221-5), non disponibile per alcune soluzioni di protezione delle chiavi sul cloud.
- I clienti possono continuare a usare le stesse applicazioni aziendali con gli HSM nShield basati sul cloud e gestire i picchi occasionali dei carichi di lavoro grazie ad HSM di maggiori capacità.
- A differenza degli HSM offerti dai singoli fornitori di servizi cloud, che tendono a vincolare i clienti ai loro ambienti, nShield as a Service è compatibile con le soluzioni di provider diversi.

Nota 1. Consulta il nostro white paper su nShield Security World per maggiori dettagli.



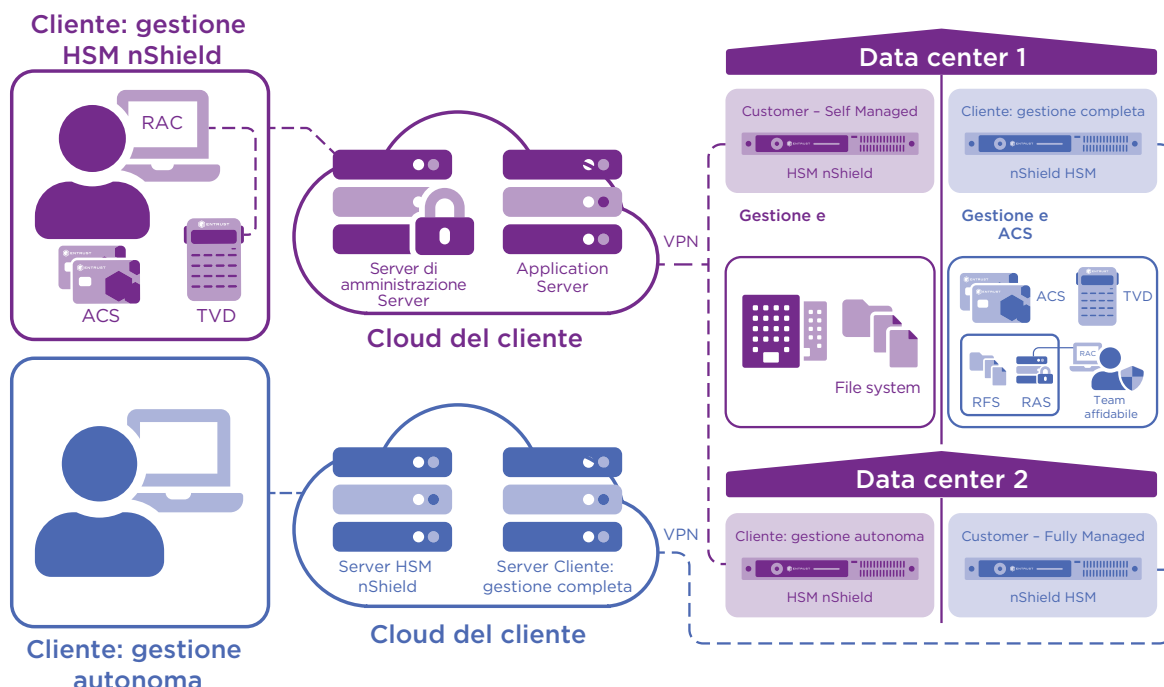
nShield as a Service

- nShield as a Service supporta l'implementazione su ambienti cloud ibridi e garantisce una migrazione delle chiavi semplice nel caso di ritorno a una soluzione on-premise.
- nShield as a Service offre ai clienti un servizio HSM dedicato. I clienti mantengono il totale controllo sulle chiavi di crittografia, con una separazione completa delle responsabilità.

Opzioni di implementazione e funzionalità di nShield as a Service

nShield as a Service è disponibile come soluzione a gestione autonoma o completa, come indicato in maggior dettaglio nello schema seguente.

Opzioni di implementazione di nShield as a Service



LEGENDA ACS: Administrator Card Set (set di schede amministratore) TVD: Trusted Verification Device (dispositivo di verifica affidabile) RAS: Remote Administration Server (server di amministrazione remota) RFS: Remote File System (file system remoto) RAC = Remote Admin Client (client di amministrazione remota)

Caratteristiche dell'implementazione di nShield as a Service	Gestione autonoma	Gestione completa
Accesso all'hardware nShield Connect dedicato ospitato in un data center sicuro	✓	✓
Kit di amministrazione remota per connessione e interazione sicure con HSM nShield in cloud	✓	✓
Manutenzione e assistenza <ul style="list-style-type: none"> • Monitoraggio del servizio • Installazione ordinaria o straordinaria di aggiornamenti e patch verificati • Assistenza 24 ore su 24, 7 giorni su 7 	✓	✓
Gestione completa dell'installazione <ul style="list-style-type: none"> • Mansioni di sicurezza svolte da personale qualificato <ul style="list-style-type: none"> - Creazione di nShield Security World - Aggiunta dei vari HSM - Cerimonie di generazione chiavi e firma 		✓
<ul style="list-style-type: none"> • Policy e procedure conformi a ISO/IEC 27001: 2013 (certificato di registrazione disponibile su richiesta) • Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) - Livello 1 	✓	✓
<ul style="list-style-type: none"> • Tutto il personale operativo è autorizzato ai sensi dello standard BS7858 (solo per i data center in Regno Unito) 	✓	✓

Per ulteriori informazioni
sugli HSM Entrust
nShield, visita il sito
HSMinfo@entrust.com
entrust.com/HSM

ENTRUST CORPORATION

Entrust permette al mondo di continuare a muoversi 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    

