nShield Bring Your Own Key gibt Kunden mehr Kontrolle über die Sicherheit ihrer Daten

Cloud-Komfort trifft Sicherheit

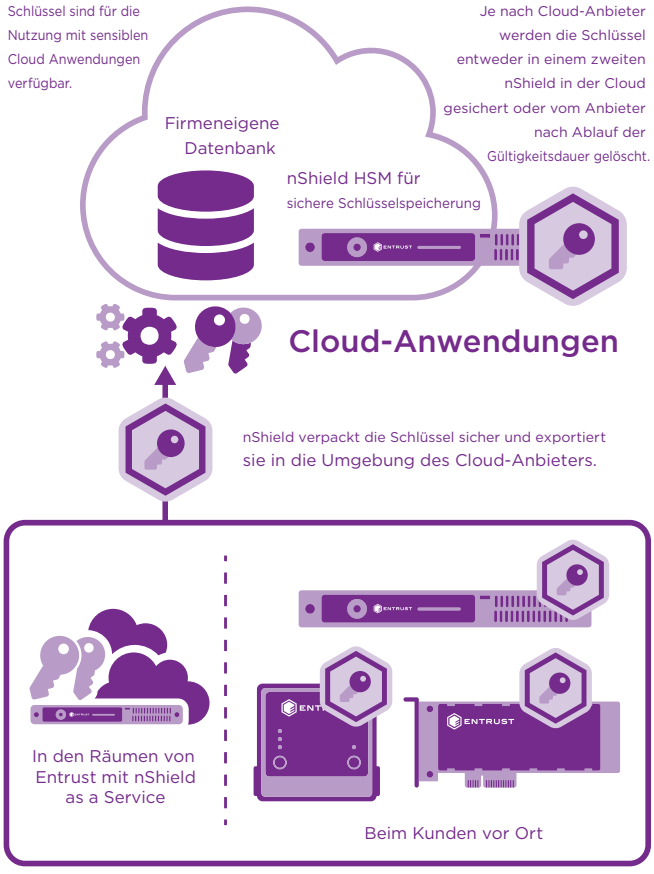
ECKPUNKTE

- Sicherere Schlüsselverwaltungsverfahren, mit denen Sie die Sicherheit Ihrer sensiblen Daten in der Cloud erhöhen
- Stärkere Schlüsselerstellung mithilfe des nShield-Hochentropie-Zufallsgenerators von Entrust, geschützt durch FIPS-zertifizierte Hardware
- Mehr Kontrolle über Ihre Schlüssel: Verwenden Sie eigene nShield-Hardware-Sicherheitsmodule in Ihrer eigenen Umgebung, um Ihre Schlüssel zu erstellen und sicher in die Cloud zu exportieren
- Einheitlichere Schlüsselverwaltung – unabhängig davon, ob Ihre Schlüssel in der Cloud oder On-Premises verwendet werden

Mit nShield-Hardware-Sicherheitsmodulen (HSM) von Entrust können Sie Ihre eigenen Schlüssel (BYOK) in Ihren Cloud-Anwendungen verwenden, unabhängig davon, ob Sie Amazon Web Services (AWS), Google Cloud Platform (GCP) oder Microsoft Azure nutzen.

Mit den hochsicheren HSM von nShield profitieren Sie weiterhin von der Flexibilität und Wirtschaftlichkeit von Cloud-Diensten.

Dabei stärken Sie gleichzeitig die Sicherheit Ihrer Schlüsselverwaltungsverfahren und erhalten mehr Kontrolle über Ihre Schlüssel.



Die einzigartige Security World-Architektur von Entrust speichert Masterschlüssel dauerhaft und stellt sie im Notfall wieder her

WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

Mehr Kontrolle über die Datensicherheit für Cloud-Kunden

Das kann nShield BYOK

Mit nShield BYOK verwenden Sie Ihre nShield HSM zur Erstellung, Speicherung und Verwaltung der Schlüssel, mit denen Sie Ihre sensiblen Anwendungen, Datenbanken und Massenspeicher in der Cloud sichern. nShield BYOK bietet folgende Funktionen:

- Bauen Sie auf Hardware-Vertrauensanker: Ihre nShield HSMs sind extrem zuverlässige, gemäß FIPS 140-2 Level 3 zertifizierte, manipulationssichere Geräte. Diese HSM dienen als Vertrauensanker für Ihre Cloud-Dienste und ermöglichen Ihnen die sichere Erstellung und Speicherung Ihrer kryptographischen Schlüssel und Signaturschlüssel.
- Verwenden Sie nShield zur Verwaltung Ihrer Schlüssel: Vertrauen Sie auf Ihre nShield HSM, um die Schlüssel für Ihre sensiblen Daten in der Cloud zu erstellen, zu verpacken und sicher an Ihre Cloud-Anwendungen zu übermitteln.
- Kontrollieren Sie die Verfügbarkeit Ihrer Schlüssel: Da Sie allein Ihre nShield HSM kontrollieren – egal ob On-Premises oder in der nShield as a Service-Umgebung – bestimmen Sie selbst, wann Schlüssel erstellt und exportiert werden. Indem Sie den Masterschlüssel kontrollieren, steuern Sie auch, wann und ob weitere Exporte zu Ihrem Cloud-Anbieter erfolgen.
- Wählen Sie Ihren Cloud-Anbieter: Mit nShield BYOK entscheiden Sie, welchen Cloud-Anbieter Sie für die einzelnen Schlüssel verwenden. Das gibt Ihnen die Flexibilität, für Ihre verschiedenen Anwendungen aus Ihren On-Premises- bzw. nShield as a Service-Umgebungen die richtige Cloud auszuwählen. Gleichzeitig profitieren Sie von der hochsicheren nShield-Schlüsselerstellung und dem daraus folgenden Schutz.

Erste Schritte mit nShield BYOK

Für die Verwendung von nShield BYOK für AWS, GCP oder Azure benötigen Sie ein nShield HSM. Sie können aus den folgenden Lösungen wählen:

- nShield Connect, ein am Netzwerk angeschlossenes Gerät
- nShield Solo, eine in einen Server integrierte PCIe-Karte
- nShield Edge, ein Gerät mit USB-Anschluss für kleinvolumige Anwendungen
- nShield as a Service unter Verwendung abonnementbasierter nShield Connect HSM

Wählen Sie BYOK von Entrust für höchste Sicherheit in Microsoft Azure. Siehe: **docs.microsoft.com/en-us/azure/key-vault/keys/hsm-protected-keys-Entrust** Wenn Sie bei der Bereitstellung Unterstützung benötigen, bieten wir Ihnen das folgende Optionspaket an:

Bring Your Own Key, Azure Professional Services
Dieses Paket umfasst nShield Edge, eine vom Entrust Professional Services Team umgesetzte Integration sowie ein Jahr Wartung.

nShield Connect-, Solo- oder Edge-HSM und Professional Services sind auch einzeln erhältlich.

Wenn Sie nShield BYOK mit AWS, GCP oder Microsoft Azure unter Anwendung der offenen Standards von Microsoft nutzen möchten, benötigen Sie das folgende Paket von Entrust:

Optionspaket für Cloud-Integration
Dieses Optionspaket enthält alles, was Sie benötigen, um mithilfe Ihrer lokalen nShield HSM Schlüssel für AWS, GCP oder Microsoft Azure mit Azure BYOK zu erstellen, sicher zu transportieren und zu vermieten.

Sie können nShield BYOK selbst in AWS, GCP oder Azure integrieren, oder Sie nutzen die Professional Services von Entrust, um eine nahtlose und effiziente Verbindung herzustellen.

Mehr Kontrolle über die Datensicherheit für Cloud-Kunden

So funktioniert nShield BYOK

Entrust bietet die nötigen Funktionen, mit denen Sie Ihre nShield HSM verwenden können, um Schlüssel zu generieren, langfristig zu speichern und Ihre Schlüssel in die Cloud zu exportieren. Sobald Ihre Schlüssel aus Ihrer On-Premises- oder nShield as a Service-Umgebung in die Cloud exportiert wurden, verwalten Sie diese mithilfe einer der folgenden Methoden:

Wenn Sie Microsoft Azure nutzen:
wählen Sie BYOK von Entrust für höchste Sicherheit. So erfüllen Sie die erforderlichen Bedingungen, um einen Schlüssel auf Azure hochzuladen. Außerdem ist strikt vorgegeben, zu welchen Zwecken Microsoft den Schlüssel anschließend verwenden darf.

Sie übertragen Ihre Schlüssel sicher auf das in Azure laufende nShield HSM, so dass Sie die Sicherheit des HSM auf beiden Seiten erhalten.

Wenn Sie AWS oder GCP nutzen:
vermieten Sie Ihre Schlüssel an AWS oder GCP zur vorübergehenden Nutzung in der Cloud. Nach einer vorab festgelegten Zeitspanne werden Ihre Schlüssel in der Cloud zerstört. Gegebenenfalls können Sie die in Ihrem HSM gespeicherten Schlüssel erneut vermieten.

Egal welchen öffentlichen Cloud-Dienst Sie wählen – da Sie Ihren Schlüssel selbst erstellen und seinen Export kontrollieren, sind Sie in der Lage, starke Sicherheitsvorkehrungen für sensible Daten und Anwendungen in der Cloud zu treffen.

HSM von Entrust

nShield HSM von Entrust gehören zu den leistungsstärksten, sichersten und am einfachsten integrierbaren HSM-Lösungen am Markt. So erleichtern sie die Einhaltung regulatorischer Vorschriften und bieten höchste Daten- und Anwendungssicherheit für Unternehmen sowie Finanz- und Regierungsbehörden. Unsere einzigartige Security World-Architektur für die Schlüsselverwaltung bietet starke, granulare Schlüsselkontrollen hinsichtlich Zugriff und Nutzung.

Weitere Informationen

Mehr Informationen zu den nShield HSMs von Entrust finden Sie auf **entrust.com/HSM**. Auf **entrust.com** erfahren Sie zudem mehr über die digitalen Sicherheitslösungen für Identitäten, Zugriff, Kommunikation und Daten von Entrust.

Mehr Informationen zu Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ÜBER ENTRUST CORPORATION

Entrust ermöglicht vertrauenswürdige Identitäten und Zahlungen sowie verlässlichen Datenschutz und hält damit die Welt sicher in Bewegung. Ein nahtloses und sicheres Umfeld ist heute mehr denn je unerlässlich, sei es bei Grenzübertritten, beim Einkaufen, beim Zugriff auf E-Government-Dienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet für genau diese Interaktionen eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen. Mit 2.500 Mitarbeitern und einem weltweiten Partnernetzwerk ist Entrust für Kunden in über 150 Ländern tätig, die sich bei ihren sensibelsten Operationen auf uns verlassen.

Weitere Informationen auf
entrust.com/HSM

Kontakt:
HSMinfo@entrust.com