



ENTRUST

nShield as a Service von Entrust für Micro Focus Voltage SecureData



Einfacher Zugang zu Cryptography as a Service

ECKPUNKTE

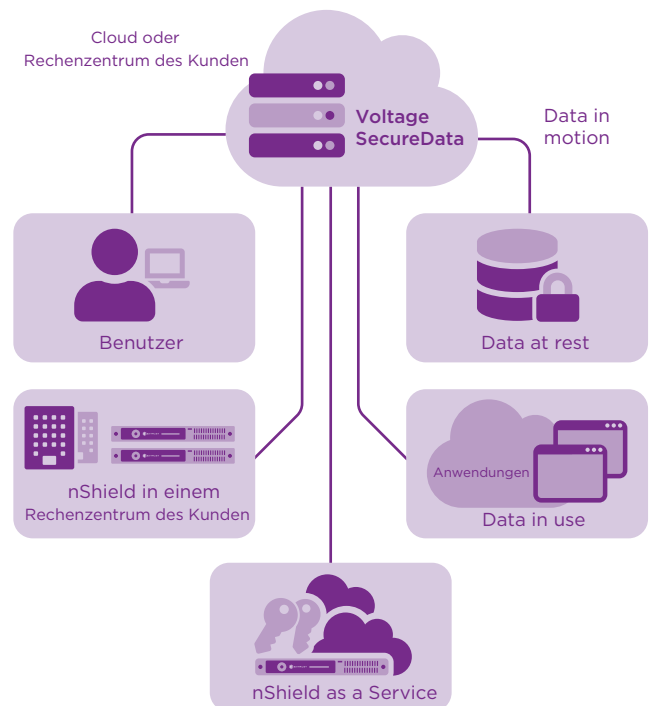
- Vollständige Kontrolle aller Schlüssel – überall dort, wo Anwendungen ausgeführt werden
- Ein leistungsstarkes nShield-Connect-Hardware-Sicherheitsmodul (HSM) für jeden einzelnen Client
- FIPS-zertifizierter Schutz innerhalb der Grenzen der nShield HSM
- Unterstützung mehrere Rechenzentren für die Einhaltung von Sicherheitsvorschriften und hohe Verfügbarkeit
- Problemlose Migration der nShield Security World auf nShield a Service

Das Problem: Wie kontrollieren Unternehmen nach der Migration in die Cloud ihre kryptographischen Schlüssel?

In der schnelllebigen IT-Umgebung vieler Unternehmen ist „Cloud First“ ein gemeinsames strategisches Ziel. Unternehmen wechseln in die Cloud, da sie von deren Skalierbarkeit, Flexibilität und Resilienz profitieren. Sie wünschen sich weniger Wartungsaufwand und vorhersehbare monatliche Betriebsausgaben. Um Sicherheit gewährleisten und Vorschriften einhalten zu können, ist unbedingt erforderlich, dass sie die Kontrolle über die Schlüssel behalten, die ihre Anwendungen und die verarbeiteten sensiblen Daten schützen.

Die Herausforderung: Gewährleistung höchster Sicherheit in der Cloud

Traditionell sind HSM in On-Premises-Rechenzentren untergebracht und werden von Sicherheitsteams vor Ort verwaltet. Sie sichern die Daten des Unternehmens und sind ein wesentlicher Teil seiner kritischen Infrastruktur. Auch nach dem Umzug in die Cloud wünschen sich Unternehmen die hohe Sicherheit,



Kunden nutzen Voltage SecureData gemeinsam mit nShield® HSM von Entrust. So können Sie Verschlüsselungsdienste ganz einfach zu nShield as a Service migrieren, um ihre kryptographischen Schlüssel zu schützen und einen Vertrauensanker bereitzustellen.



nShield as a Service von Entrust für Micro Focus Voltage SecureData

die HSM ihnen bieten. Der effiziente Zugang zu einem zugeordneten Cloud-basierten HSM gewährleistet auch nach dem Wechsel auf dieses neue Unternehmensmodell robuste Sicherheit und die Einhaltung von Vorschriften.

Die Lösung: Voltage SecureData von Micro Focus und nShield as a Service von Entrust

Voltage SecureData garantiert die Vertraulichkeit und den Datenschutz für Data at Rest, Data in Motion und Data in Use, die von unternehmenskritischen Prozessen und analytischen Anwendungen verwendet werden. Die Lösung nutzt Technologien der nächsten Generation wie Hyper Format Preserving Encryption (Hyper FPE), Hyper Secure Stateless Tokenization (Hyper SST), Format-Preserving Hash (FPH) und Datenmaskierung, um Daten unter Beibehaltung des Originalformats zu verschlüsseln und unkenntlich zu machen. Voltage SecureData bewahrt die referenzielle Integrität von Prozessen, Anwendungen und Diensten und macht Daten für Cyber-Angreifer wertlos. Die Lösung reduziert die Personal- und IT-Kosten deutlich. Dadurch können Unternehmen sich ganz auf ihr Geschäft konzentrieren, da sie wissen, dass ihre Daten geschützt sind und Datenschutzvorgaben eingehalten werden. Dank der Schlüsselverwaltung Voltage Stateless Key Management werden die Schlüssel on-the-fly hergeleitet. Dadurch werden Schlüsseldatenbanken sowie die Speicherung, Replikation und Sicherung von Schlüsseln überflüssig.

Voltage SecureData bindet nShield as a Service ein. Somit können Kunden ganz einfach kryptographische Schlüssel von bestehenden On-Premises-HSM migrieren. nShield as a Service ist ein Abonnementdienst und ermöglicht es, Schlüsselmaterial separat von sensiblen Daten zu erstellen, zu schützen und darauf zugreifen. Mit dieser Cloud-basierten Lösung können Unternehmen die HSM in ihren Rechenzentren durch fest zugeordnete und zertifizierte nShield Connect HSM ergänzen oder ersetzen. Das bietet ihnen die gleichen Vorteile, als wenn sie die Geräte selbst besitzen würden.

nShield as a Service wird in geografisch verteilten Rechenzentren bereitgestellt. Es lässt sich nahtlos in das Voltage Stateless Key Management von Micro Focus integrieren und bietet zuverlässige Sicherheit, indem es den Master-Root-Schlüssel für die Schlüsselherleitung in einem verstärkten Gerät hostet. Wichtige Verschlüsselungs-, Entschlüsselungs- und Schlüsselverwaltungsprozesse werden mit CodeSafe ausgeführt. Diese einzigartige Funktion ermöglicht es, Code innerhalb der physischen Grenzen einer gemäß FIPS 140-2 Level 3 verstärkten, manipulationssicheren Umgebung auszuführen, in der er vor möglicher Schadsoftware oder Insider-Angriffen geschützt ist. Nur nShield as a Service ermöglicht Kunden bei Bedarf die nahtlose Migration ihrer sicheren Codeausführung von einem On-Premises-HSM in die Cloud.

Warum nShield as a Service mit Voltage SecureData?

Mit nShield as a Service können Unternehmen Sicherheitsausgaben besser planen, Kapazitäten dem Bedarf anpassen, den Fußabdruck ihres Rechenzentrums verkleinern und den Zeitaufwand für die regelmäßige Wartung und Überwachung verringern. Die Abonnement-Kunden interagieren mit den Cloud-basierten nShield HSM auf dieselbe Weise wie mit Geräten in ihren eigenen Rechenzentren, müssen aber keine physische Hardware mehr erwerben, installieren und warten. Dadurch können gesicherte Anwendungen schneller bereitgestellt werden. nShield as a Service wird in Form eines Abonnements angeboten. Kunden abonnieren einen HSM und erhalten so vollständige Kontrolle über ihre kryptographischen Schlüssel. Aufgaben werden strikt getrennt, damit optimale Sicherheit erreicht werden kann.

nShield as a Service von Entrust für Micro Focus Voltage SecureData

Kunden können nShield as a Service genau wie ihre eigenen HSM in ihrem Rechenzentrum selbst remote verwalten, auch wenn sie sich für einen oder mehrere Cloud-Diensteentscheiden. Wenn sie Verwaltung und Wartung jedoch lieber den Experten von Entrust überlassen, können sie die vollständig verwaltete Option wählen. Die Kontrolle über ihre Schlüssel behalten die dennoch selbst. Der Managed Service unterstützt hybride Cloud-Bereitstellungen und bietet eine einfache Schlüsselmigration, falls Daten von einem Cloud-Anbieter zurück in eine On-Premises-Umgebung übertragen werden sollen.

Unabhängig von der Option, für die sie sich entscheiden, sind die Kunden Eigentümer ihrer Schlüssel und können sie mithilfe der Schlüsselverwaltungsarchitektur nShield Security World in der gesamten nShield-Umgebung verwenden. nShield HSM sind nach FIPS 140-2 Level 3, Common Criteria EAL4+ und eIDAS (EN 419 221-5 Schutzprofil) zertifiziert.

nShield as a Service bietet gegenüber der On-Premises-Bereitstellung von nShield HSM einige Vorteile. Da die Kunden, die Voltage SecureData nutzen, ihre Speicher und Workloads mehr

und mehr in Cloud-Umgebungen verlagern, sind sie auf der Suche nach einem HSM-basierten Vertrauensanker, mit dem sie die gewünschte hochverfügbare und leistungsstarke datenzentrische Lösung unterhalten können.

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.

Micro Focus Voltage

Micro Focus ist ein globales Softwareunternehmen mit 40-jähriger Erfahrung in der Bereitstellung und Unterstützung von Unternehmenssoftware, mit der Kunden mit geringem Risiko innovative Lösungen entwickeln können. Die Datensicherheitslösungen Micro Focus® Voltage bieten Hyper Format-Preserving Encryption, Hyper Secure Stateless Tokenization, Stateless Key Management und Datenmaskierung. Hochwertige regulierte Daten in Unternehmensanwendungen, Datenverarbeitungsinfrastruktur, hybrider IT/Cloud, Zahlungsökosystemen, missionskritischen Systemen und Big-Data-/IoT-Analyseplattformen werden so optimal geschützt. Weitere Informationen finden Sie auf www.microfocus.com

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.

Eigenschaften von nShield

	Cloud-basiert	On-Premises
Skalierbare, flexible, kostengünstige Bereitstellung (OpEx statt CapEx)	●	
Weniger Wartungs-/Überwachungsaufwand	●	
Freisetzung interner Sicherheitsressourcen	●	
Unterstützung mehrerer Rechenzentren	●	
Vollständige Kontrolle über wichtige Schlüssel	●	●
Übertragung der Sicherheitsverantwortung auf die vertrauenswürdigen Mitarbeiter von Entrust	Vollständig verwaltet	
Zugang zu leistungsstarken nShield-HSM (Connect XC-High)	●	●
Sicherung der Schlüssel und des Ausführungscodes innerhalb gemäß FIPS 140-2 zertifizierter Grenzen	●	●
Hohe Verfügbarkeit, damit sie bei Bedarf jederzeit auf ihre Schlüssel zugreifen können.	●	●

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

