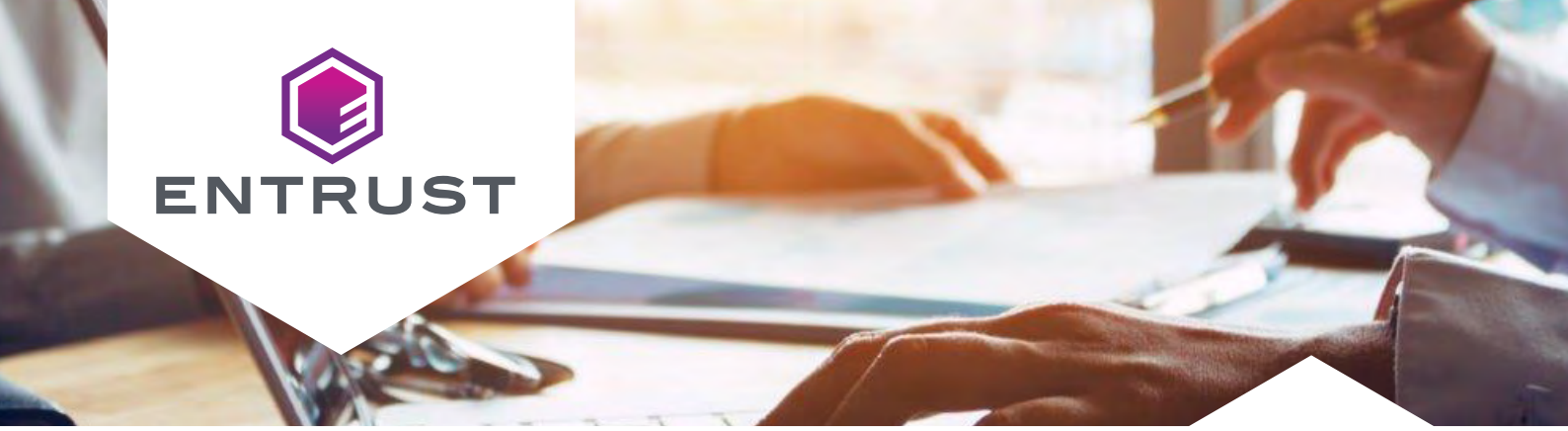

Entrust und führende Datenbankanbieter gewährleisten optimierte Datensicherheit und die Einhaltung von Vorgaben

Optimierter Schutz für Datenbanken mit nShield-Hardware-Sicherheitsmodulen (HSM)

ECKPUNKTE

- Schützt Data-at-Rest für On-Premises- sowie Cloud-basierte Bereitstellungen
- Ermöglicht die Einhaltung strikter Richtlinien und Vorgaben zur Datensicherheit
- Gewährleistet hohe Sicherheit durch die Trennung von Schlüsseln und Datenbanken
- Verwaltet kryptographische Schlüssel, Richtlinien und Zugriff zentral
- Sichert kryptographische Schlüssel in einem manipulationsicheren, nach FIPS 140-2 Level 3 und Common Criteria EAL4+ zertifizierten Hardware-Sicherheitsmodul

Die Herausforderung:

Unternehmen speichern sensible Daten wie die personenbezogenen Informationen von Verbrauchern, geistiges Eigentum und Finanzberichte in komplexen Datenbanken. Ohne angemessenen Schutz laufen sie Gefahr, Opfer von Datenschutzverletzungen zu werden. Das kann ihren Ruf schädigen und hat den Verstoß gegen Vorschriften sowie erhebliche finanzielle Auswirkungen zur Folge. Unternehmen schützen diese wertvollen Data at Rest in der Regel durch Transparent Data Encryption (TDE) oder Cell-Level Encryption (CLE), die nativer Bestandteil führender Datenbanklösungen sind.

Je nach Datenbankprodukt können die Daten auf Datenbank-, Tabelspace-, Spalten- oder Zellebene verschlüsselt werden. Viele Unternehmen verschlüsseln auch die entsprechenden Protokoll- und Berichtdateien, die möglicherweise sensible Daten enthalten. Daher ist es unerlässlich, die Schlüssel, mit denen diese Dateien und Datenbanken verschlüsselt werden, zu schützen. Diese dürfen keinesfalls in fremde Hände gelangen. Diebstahl oder das Abhandenkommen der Schlüssel kann zu einer Gefährdung der Datenbankeinträge und damit zum Verstoß gegen geltende Vorschriften führen, was wiederum finanziellen Schaden nach sich zieht.

Damit die kryptographischen Schlüssel sicher geschützt sind, sollten sie getrennt von den Assets, die sie sichern, aufbewahrt werden, und zwar auf eine Weise, die den Datenschutzverordnungen und bewährten Verfahren der Branche entspricht. Gleichzeitig müssen die Schlüssel jederzeit verfügbar sein. Nur so können die Datenbank und die Anwendungen, die deren Inhalte nutzen, optimale Leistung erbringen.

Optimierter Schutz für Datenbanken mit nShield HSM

Die Lösung: Datenbankverschlüsselung mit nShield HSM

nShield-Hardware-Sicherheitsmodule (HSM) von Entrust dienen den Lösungen führender Datenbankanbieter als Vertrauensanker für kryptographische Datenbankschlüssel.

Sie statten die Masterschlüssel, die zum Schutz dieser Datenbankschlüssel verwendet werden, mit einer zusätzlichen Sicherheitsschicht aus. nShield HSM bieten nach FIPS 140-2 Level 3 und Common Criteria EAL4+ zertifizierte Sicherheit für Ihre wichtigen Schlüssel, ohne dass Änderungen an bestehenden Anwendungen, Datenbankstrukturen oder -prozessen erforderlich sind.

Der Schutz der Schlüssel wird durch Richtlinien geregelt. Daher sind Insider-Angriffe wenig wahrscheinlich und das Risiko einer Datenschutzverletzung ist gering. Die Kombination bietet prüfbare Sicherheit und ermöglicht die Einhaltung regulatorischer und rechtlicher Vorgaben einschließlich des Payment Card Industry Data Security Standard (PCI DSS).

Was nShield besonders macht

Die flexiblen Bereitstellungsmodelle der nShield HSM wie Clustering und Failover erleichtern den Schutz und die Verwaltung von kryptographischen Datenbankschlüsseln. Somit gewährleisten sie die Kontinuität Ihrer kritischen Systeme entsprechend Ihrer Ansprüche an Disaster Recovery und Datenspeicherung.

Sie sind als spezielle Karte für einzelne Server oder als gemeinsam genutzte Netzwerkgeräte für virtuelle Umgebungen erhältlich. nShield HSM sorgen dafür, dass die Verwaltung von Sicherheitsrichtlinien von den administrativen Funktionen getrennt wird und unterstützen Sie so dabei, den wechselnden Anforderungen Ihres Unternehmens gerecht zu werden.

nShield® HSM bieten:

- Schutz der Hardwareschlüssel: Die kryptographischen Schlüssel für Datenbanken werden isoliert von der Datenbankverwaltung in einer geschützten, manipulationssicheren Umgebung gespeichert, damit sie nicht kopiert oder manipuliert werden können.
- Durchsetzung von Benutzerrechten und Rollen: Sie setzen erweiterte Rechte für den Zugriff auf verschlüsselte Daten in der Datenbank durch.
- Engmaschige Schlüsselkontrolle: Administratoren werden mittels Smartcards authentifiziert und der Zugriff auf die kryptographischen Schlüssel von Datenbanken somit streng kontrolliert.
- Aufgabentrennung: Die Verantwortung für wichtige Aufgaben und Verfahren wird auf mehrere Administratoren verteilt.
- Unterstützung bei der Einhaltung von Vorgaben: Sie entsprechen den Vorgaben, die umfassenden Schutz der Kundendaten fordern.

Microsoft SQL Server · IBM DB2 · ORACLE DATABASE

nFinity Partner

Weitere Informationen

Mehr Informationen zu den nShield HSM 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.

Weitere Informationen auf
entrust.com/HSM

ENTRUST

Kontakt:
HSMinfo@entrust.com