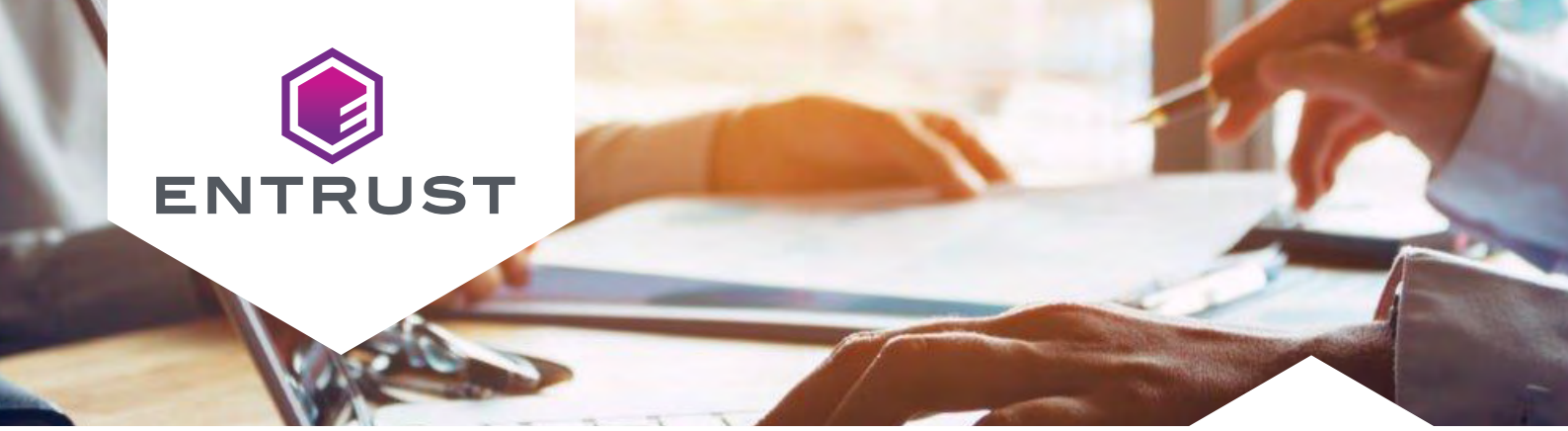


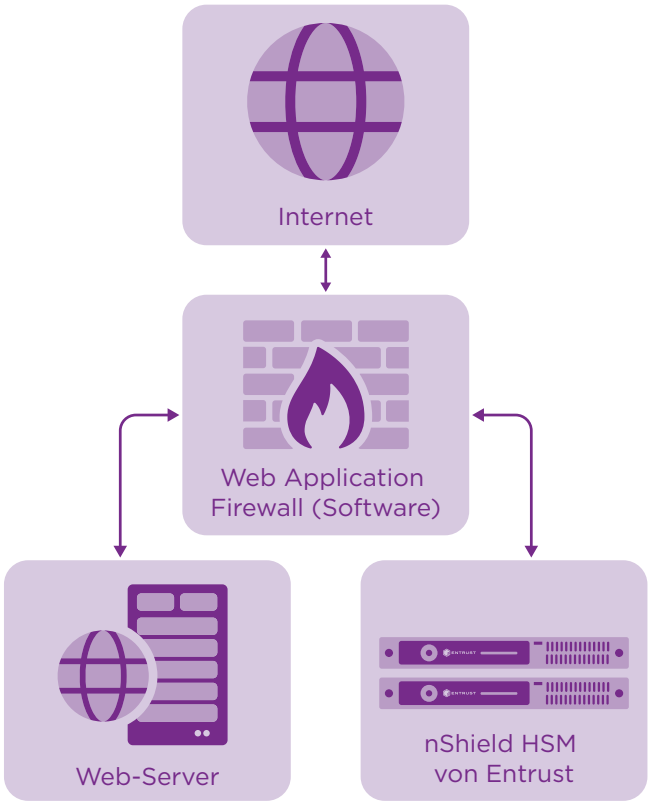
nShield-Hardware-Sicherheitsmodule verbessern die Sicherheit von Web Application Firewalls

NFINITY
STRATEGIC TECHNOLOGY PARTNER PROGRAM

Hochsicherer Schutz für Master-Schlüssel

ECKPUNKTE

- Schutz von Websites und Anwendungen vor Betrug, Datendiebstahl und anderen Cyber-Angriffen.
- Sicherung der Schlüssel und Zertifikate innerhalb sorgfältig konzipierter kryptographischer Grenzen und mittels einer robusten Zugriffskontrolle, damit die Schlüssel ausschließlich zu den autorisierten Zwecken verwendet werden.
- Gewährleistung der Verfügbarkeit von Schlüsseln durch ausgereifte Management-, Speicher- und Redundanzfunktionen, damit bei Bedarf jederzeit auf diese Schlüssel zugegriffen werden kann.
- Leistungsstarke Unterstützung für stetig zunehmende Transaktionsvolumina.
- Einfache Prüfung und Einhaltung von Datensicherheitsvorschriften.



Führende Web Application Firewalls schützen den Master-Schlüssel für private Schlüssel und Passwörter mit nShield HSM.

WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

nShield HSM verbessern die Sicherheit von Web Application Firewalls

Die Herausforderung

Webanwendungen und Cloud-basierte Dienste sind in Unternehmen nicht mehr wegzudenken. Allerdings stellen sie auch ein zusätzliches Risiko für die Datensicherheit dar. Daher implementieren Unternehmen Web Application Firewalls (WAF), die den Datenverkehr filtern und überwachen. Sie erkennen, blockieren und verhindern Angriffe wie Cross-Site-Scripting, SQL-Injection, Zero-Day-Exploits, Malwareinfektionen, Identitätsbetrug und sonstige Bedrohungen.

WAFs gewährleisten mittels Verschlüsselung validierte Verbindungen sowie den Schutz und die Integrität von Daten. Das setzt aber gleichzeitig voraus, dass die kryptographischen Schlüssel umfassend gesichert werden. Unternehmen, die Ihre Schlüssel außerhalb kryptographischer Grenzen aufbewahren, unterliegen häufig einem falschen Gefühl von Sicherheit – tatsächlich sind sie so anfällig für Angriffe.

Darüber hinaus verlangen viele regulatorische Vorgaben wie PDI DSS und nationale Verordnungen für kritische Infrastruktur umfassende Schutzmaßnahmen für kryptographische Schlüssel. Hardware-Sicherheitsmodule (HSM) schützen diese Schlüssel und erfüllen nicht nur die geltenden Normen, sondern sind auch branchenweit als bewährtes Verfahren anerkannt.

Die Lösung: Web Application Firewalls mit nShield HSM

Web Application Firewalls blockieren, erkennen und verhindern Angriffe. Außerdem verschlüsseln sie Inhalte und stellen so validierte Verbindungen und den Schutz sensibler Daten sicher. Die Hardware-Sicherheitsmodule (HSM) von Entrust können in führende Web Application Firewalls integriert werden. Sie schützen die Master-Schlüssel der privaten Schlüssel und Passwörter sowie die privaten Schlüssel für die SSL-/TLS-Verschlüsselung. Die HSM dienen als unangreifbarer Vertrauensanker und sorgen für optimierte Netzwerksicherheit. The nShield®-Reihe ist gemäß FIPS 140-2 und Common Criteria zertifiziert und gewährleistet, dass die Umgebung der Web Application Firewalls den geltenden Vorgaben entspricht.

nShield HSM verbessern die Sicherheit von Web Application Firewalls

Was nShield besonders macht

nShield HSM von Entrust schützen die Schlüssel privilegierter Benutzerkonten und Passwörter in einer speziell für diesen Zweck entwickelten Hardware-Umgebung. Schlüssel, die außerhalb der kryptographischen Grenzen zertifizierter HSM verwendet werden, sind deutlich anfälliger für Angriffe, was zur Offenlegung von Daten führen kann. HSM sind die einzige bewährte und prüfbare Möglichkeit, um wertvolles kryptographisches Material zu schützen. nShield HSM:

- sichern Schlüssel und Zertifikate innerhalb sorgfältig ausgelegter kryptographischer Grenzen
- wenden robuste Zugriffskontrollen an, damit Schlüssel ausschließlich für autorisierte Zwecke verwendet werden
- gewährleisten durch ausgereifte Management-, Speicher- und Redundanzfunktionen die Verfügbarkeit von Schlüsseln, damit bei Bedarf jederzeit auf diese zugegriffen werden kann
- bieten leistungsstarke Unterstützung für stetig zunehmende Transaktionsvolumina
- unterstützen die Einhaltung von Vorschriften für kritische Infrastrukturen, Regierungsbehörden, Banken und weitere Branchen.

Entrust arbeitet seit Jahrzehnten mit Anbietern von Lösungen und Anwendungen daran, die vielen Probleme zu meistern, vor denen Unternehmen beim Thema Datenschutz stehen. Dazu gehören:

- Zugangsberechtigungen von Geräten für das Internet der Dinge
- Sicherheit von Cloud-Computing, Big Data und Anwendungen
- Einhaltung von regulatorischen und brancheninternen Vorgaben
- Schutz geistigen Eigentums
- Sichere Berechtigungsnachweise

nFinity Partner

Die Firewalls der nächsten Generation von Palo Alto Networks® optimieren gemeinsam mit nShield Connect HSM die Sicherheit der Masterschlüssel für private Schlüssel und Passwörter. Darüber hinaus schützen und verwalten die HSM die bei der SSL-/TLS-Entschlüsselung verwendeten privaten Schlüssel – und fungieren als Vertrauensanker, der die Sicherheit des gesamten Netzwerks verbessert.

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.

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