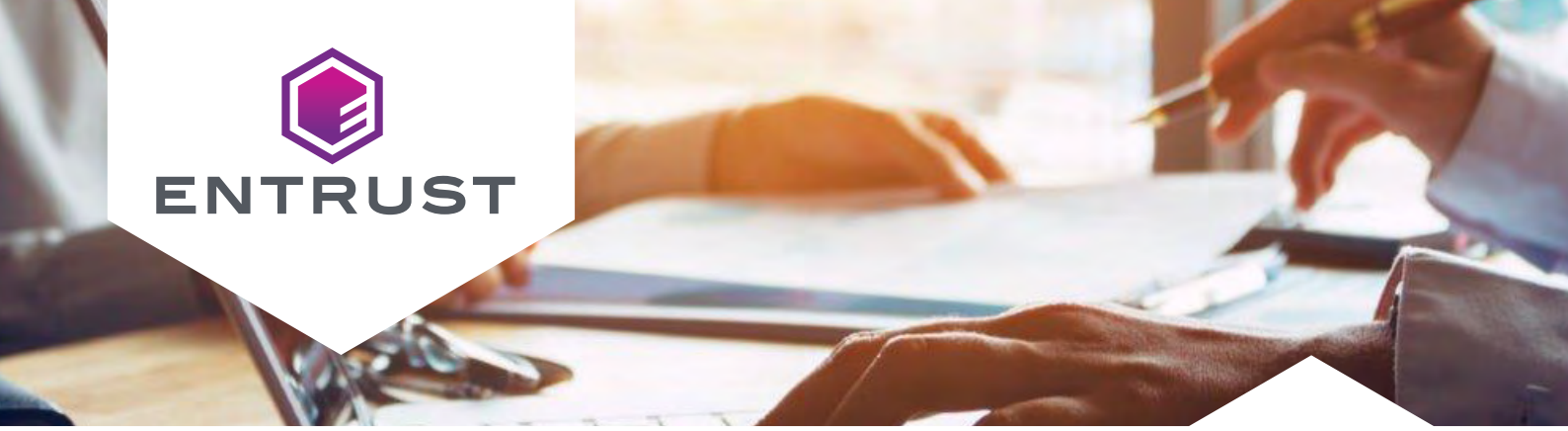


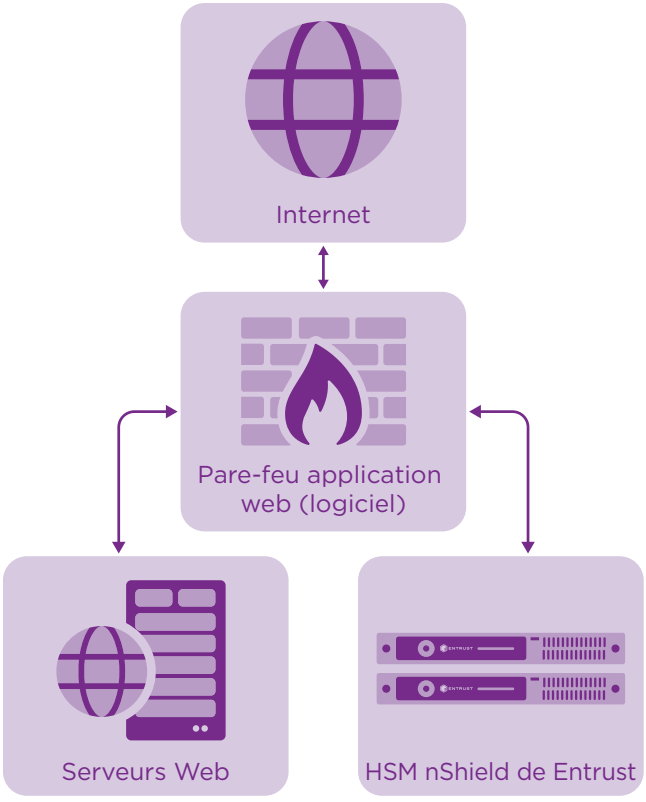
Les modules matériels de sécurité (HSM) nShield de Entrust renforcent la sécurité des pare-feu des applications web

NFINITY
STRATEGIC TECHNOLOGY PARTNER PROGRAM

Des clés principales hautement protégées

CARACTÉRISTIQUES

- Protéger les sites web et les applications contre la fraude, le vol de données et autres cyberattaques
- Sécuriser les clés et les certificats dans des limites de chiffrement rigoureusement définies utilisant des mécanismes de contrôle d'accès très performants, de sorte que les clés ne puissent être utilisées qu'à leur fin autorisée
- Veiller à la disponibilité en utilisant des fonctions très élaborées de gestion des clés, de stockage et de redondance qui garantissent que les clés sont toujours accessibles lorsque l'on en a besoin
- Obtenir des performances supérieures afin de pouvoir prendre en charge des taux de transaction de plus en plus exigeants
- Faciliter l'audit et le respect de la législation en vigueur sur la protection des données



Les principaux pare-feu d'applications web utilisent des HSM nShield pour protéger la clé principale utilisée pour chiffrer les clés privées et les mots de passe.

DÉCOUVREZ-EN PLUS SUR ENTRUST.COM/FR/HSM

Les HSM nShield renforcent la sécurité des pare-feu des applications web

Le défi : la connectivité croissante conduit à de nouvelles attaques

Les applications web et les services basés sur le cloud sont des outils essentiels pour les entreprises d'aujourd'hui, mais ils représentent une exposition supplémentaire aux risques de sécurité des données. Pour faire face à ces risques, les entreprises mettent en place des pare-feu pour applications web (WAF), qui filtrent et surveillent le trafic et peuvent détecter, bloquer et éviter des attaques telles que les scripts intersites, l'injection SQL, les attaques ZETA, les infections par des logiciels malveillants, l'usurpation d'identité et d'autres menaces.

Si les WAF utilisent le chiffrement pour garantir des connexions validées et protéger la confidentialité et l'intégrité des données, cela doit aller de pair avec une protection robuste des clés de chiffrement. Le stockage des clés de chiffrement en dehors d'un dispositif de chiffrement peut rendre une organisation vulnérable aux attaques tout en créant un faux sentiment de sécurité.

En outre, de nombreux mandats de conformité, tels que PCI DSS et les réglementations nationales sur les infrastructures critiques, exigent une protection renforcée des clés de chiffrement. L'utilisation de modules matériels de sécurité (HSM) pour la protection des clés répond non seulement aux normes de conformité, mais fait également partie des meilleures pratiques du secteur de la sécurité.

La solution : des pare-feu pour les applications web intégrés avec les HSM nShield

Les pare-feu pour les applications web de nouvelle génération aident les entreprises à bloquer, détecter et éviter les attaques, ainsi qu'à chiffrer le contenu pour garantir des connexions validées et la protection des données sensibles. Les modules matériels de sécurité (HSM) d'Entrust s'intègrent aux principaux pare-feu des applications web pour protéger la clé principale utilisée pour chiffrer toutes les clés privées et les mots de passe, ainsi que les clés privées utilisées pour le chiffrement SSL/TLS, offrant ainsi des racines de confiance inattaquables et une sécurité réseau renforcée. La gamme de HSM nShield® a obtenu les certifications FIPS 140-2 et Critères Communs, garantissant que l'environnement de pare-feu des applications web répond aux exigences de conformité.

Les HSM nShield renforcent la sécurité des pare-feu des applications web

Pourquoi choisir les HSM nShield

Les HSM nShield de Entrust protègent les clés et les mots de passe des comptes utilisateurs privilégiés dans un environnement dédié et renforcé. Les clés de chiffrement traitées en dehors des limites de chiffrement d'un HSM certifié sont nettement plus vulnérables aux attaques, ce qui peut mener à la divulgation d'informations confidentielles. Les HSM représentent le seul moyen éprouvé et vérifiable de protéger ses documents chiffrés importants. Les HSM nShield permettent de :

- Sécuriser les clés et les certificats au sein d'un dispositif de chiffrement soigneusement conçu
- Utiliser des mécanismes de contrôle d'accès robustes afin que les clés ne soient utilisées que pour leur usage autorisé
- Veiller à la disponibilité en utilisant des fonctions très élaborées de gestion des clés, de stockage et de redondance qui garantissent que les clés sont toujours accessibles lorsque l'on en a besoin
- Obtenir des performances supérieures afin de pouvoir prendre en charge des taux de transaction de plus en plus exigeants
- Favoriser la conformité aux mandats relatifs aux infrastructures critiques, aux administrations publiques, au secteur bancaire et à d'autres secteurs

Entrust travaille depuis des dizaines d'années avec des fournisseurs de solutions et d'applications pour répondre à un large éventail de problèmes rencontrés par les entreprises vis-à-vis de la protection des données, notamment :

- L'identification des appareils pour l'Internet des objets
- Le cloud computing, les big data et la sécurité des applications
- La conformité réglementaire et les mandats de l'industrie
- La protection de la propriété intellectuelle
- La sécurité des accréditations

Partenariat nFinity

Le pare-feu de nouvelle génération de Palo Alto Networks® s'intègre aux HSM nShield Connect pour renforcer la sécurité de la clé principale utilisée pour chiffrer les clés privées et les mots de passe. Le HSM protège et gère également les clés privées utilisées dans le processus de déchiffrement SSL/TLS, fournissant une racine de confiance qui améliore le niveau de sécurité complet du réseau.

En savoir plus

Pour en savoir plus sur les HSM nShield d'Entrust, rendez-vous sur **entrust.com/fr/HSM** Pour en savoir plus sur les solutions de protection numérique d'Entrust pour les identités, l'accès, les communications et les données, rendez-vous sur **entrust.com/fr**

Pour en savoir plus sur les HSM nShield d'Entrust

HSMinfo@entrust.com

entrust.com/fr/hsm

À PROPOS DE LA SOCIÉTÉ ENTRUST

Entrust sécurise un monde en mouvement avec des solutions qui protègent les identités, les paiements et les données, dans tous les pays. Aujourd'hui, les gens souhaitent des parcours plus fluides et plus sûrs quand ils traversent les frontières, font des achats, utilisent des services administratifs en ligne ou des réseaux d'entreprises. Notre gamme unique de solutions pour la sécurité numérique et l'émission de titres sécurisés permet de répondre précisément à ces souhaits. Grâce à nos 2 500 collaborateurs, notre réseau international de partenaires et des clients dans plus de 150 pays, les organisations les plus fiables au monde nous font confiance.

Découvrez-en plus sur
entrust.com/fr/HSM

ENTRUST

Nous contacter :
HSMinfo@entrust.com