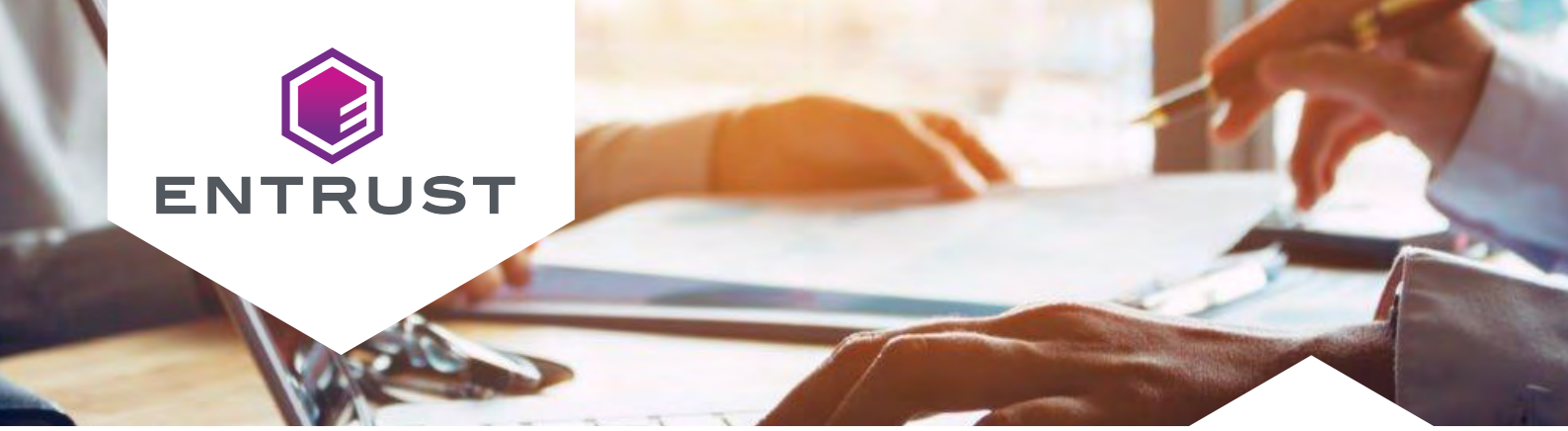


Une gestion sécurisée de l'accès utilisateur privilégié avec les HSM nShield

Une protection hautement sécurisée des données d'identification des comptes privilégiés

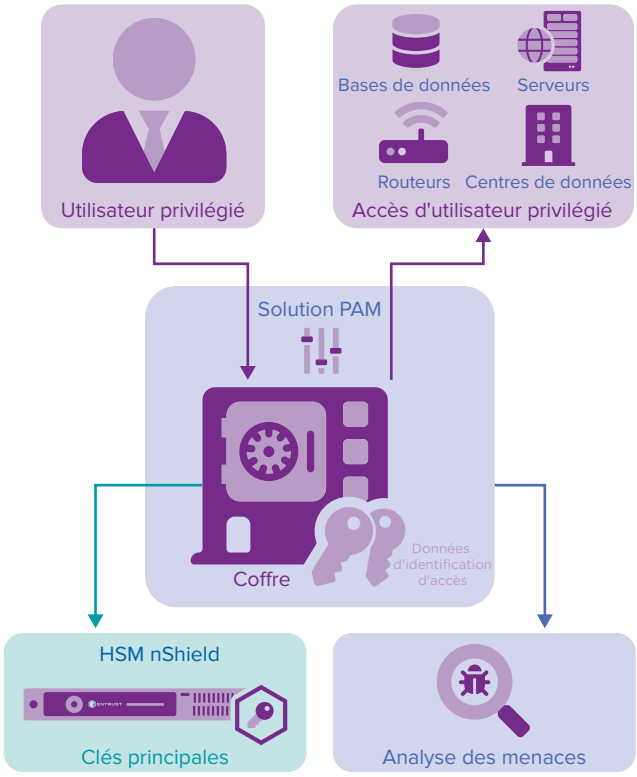
CARACTÉRISTIQUES

- Clés de chiffrement utilisées pour accéder au coffre sécurisées dans un HSM inviolable certifié FIPS 140-2 niveau 3
- Protection et gestion d'un grand nombre de clés de comptes privilégiés dans les limites du matériel protégé
- Intégration des solutions d'accréditation et de gestion de comptes privilégiés
- Facilitation de l'audit et du respect de la législation en vigueur sur la protection des données
- Renforcement de la sécurité des accès privilégiés
- Amélioration de la transparence et du contrôle des mots de passe privilégiés

Le défi : les pirates cherchent des occasions d'exploiter les comptes privilégiés

Les organisations établissent des comptes privilégiés pour des personnes de confiance qui disposent d'un accès et de privilèges uniques en fonction de leurs postes et de leurs responsabilités. Par exemple, un utilisateur privilégié pourrait être en mesure de mettre à niveau un système d'exploitation, d'ajouter ou de supprimer des logiciels, ou d'accéder à des fichiers et des répertoires qui sont inaccessibles aux utilisateurs de base.

Les attaques contre les infrastructures informatiques des entreprises visent de plus en plus à accéder aux données d'identification des comptes utilisateurs privilégiés. Ces données d'identification sont très intéressantes pour les pirates, car un compte compromis peut facilement mener aux informations les plus sensibles d'une entreprise. Les comptes privilégiés peuvent également être utilisés de manière abusive pour accéder à un plus grand nombre de comptes, et les données d'identification compromises peuvent passer inaperçues pendant un certain temps car le pirate semble être un utilisateur de confiance.



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

Une gestion sécurisée de l'accès utilisateur privilégié

Les organisations exigent un contrôle total des autorisations d'accès aux comptes privilégiés, y compris la possibilité de vérifier leur utilisation, d'imposer des restrictions de temps automatiques et de révoquer instantanément l'accès si nécessaire. De telles fonctionnalités ne sont pas disponibles lorsque les données d'identification de comptes privilégiés sont gérées via un tableur ou d'autres processus manuels.

Tout comme d'autres systèmes et données d'identification essentiels à l'entreprise, les comptes privilégiés nécessitent une protection chiffrée garantie par des clés de chiffrement indispensables hautement sécurisées.

La solution : des solutions de gestion de l'accès utilisateur privilégié intégrées aux HSM nShield

Les entreprises déploient des outils de gestion d'accès utilisateur privilégié (PAM) pour autoriser, gérer et vérifier l'accès aux comptes et aux données par des utilisateurs et des applications spécifiques. Les outils de PAM permettent aux clients de :

- Protéger les données d'identification des comptes privilégiés dans un coffre sécurisé et chiffré
- Limiter l'accès à des systèmes spécifiques en fonction du rôle de l'utilisateur
- Autoriser l'accès pendant une période de temps donnée et automatiquement révoquer l'accès une fois la période expirée
- Suivre et contrôler l'activité de chaque utilisateur privilégié

Comme pour toute utilisation du chiffrement, la protection la plus sûre du coffre chiffré intègre un module matériel de sécurité (HSM) pour protéger les clés de chiffrement racines.

Les HSM nShield® de Entrust sont intégrés aux principales solutions PAM pour offrir une protection FIPS 140-2 niveau 3 et Critères communs EAL 4+ pour les clés qui protègent les données d'identification des comptes privilégiés. La solution combinée offre une couche de sécurité supplémentaire qui protège à la fois les données d'identification d'accès et les portes qu'elles ouvrent aux comptes privilégiés et aux données sensibles qu'elles contiennent.

Les HSM de Entrust

Les HSM nShield d'Entrust représentent l'une des solutions HSM les plus performantes, les plus sécurisées et les plus faciles à intégrer, permettant de respecter les réglementations et de fournir les plus hauts niveaux de sécurité pour les données et les applications des entreprises, des organismes financiers et des administrations publiques.

Notre architecture de gestion de clés Security World permet un contrôle granulaire et très robuste de l'accès aux clés et de leur usage.

Une gestion sécurisée de l'accès utilisateur privilégié

Partenariat nFinity

BeyondTrust

Password Safe de BeyondTrust unifie la gestion des mots de passe privilégiés et des sessions privilégiées, offrant une exploration, une gestion, un contrôle et une surveillance sécurisés pour tout identifiant privilégié. Password Safe permet aux organisations d'obtenir un contrôle et une transparence complets sur les comptes privilégiés.

Password Safe de BeyondTrust s'intègre aux HSM nShield de Entrust pour sécuriser et gérer les clés de chiffrement utilisées pour protéger les données d'identification d'accès utilisateur privilégié stockées.

BROADCOM

La solution Privileged Access Manager de Broadcom est une solution automatisée pour la gestion des accès d'utilisateur privilégié dans les environnements physiques, virtuels et cloud. Disponible sous forme d'appareil physique renforcé ou d'une instance de machine virtuelle, la solution renforce la sécurité en protégeant les données d'identification administratives sensibles tels que les mots de passe principaux et administrateurs, en contrôlant l'accès d'utilisateur privilégié, en appliquant les politiques de manière proactive, et en surveillant et en enregistrant l'activité des utilisateurs privilégiés sur l'ensemble des ressources informatiques.

La solution Privileged Access Manager de Broadcom s'intègre aux HSM nShield de Entrust pour chiffrer et déchiffrer les données d'identification stockées.

CYBERARK

La solution de sécurité d'accès privilégié est une plateforme unifiée d'entreprise qui permet aux organisations de gérer et de sécuriser tous les comptes privilégiés. La solution sécurise les données d'identification, y compris les mots de passe et les clés SSH, contrôle l'accès à ces comptes, et isole et enregistre les sessions privilégiées qui sont utilisées pour l'audit et l'analyse technique.

Combinées avec les HSM nShield Connect, ces solutions maximisent la sécurité des clés de chiffrement utilisées pour accéder aux comptes privilégiés.

En savoir plus

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

NFINITY
STRATEGIC TECHNOLOGY PARTNER PROGRAM

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