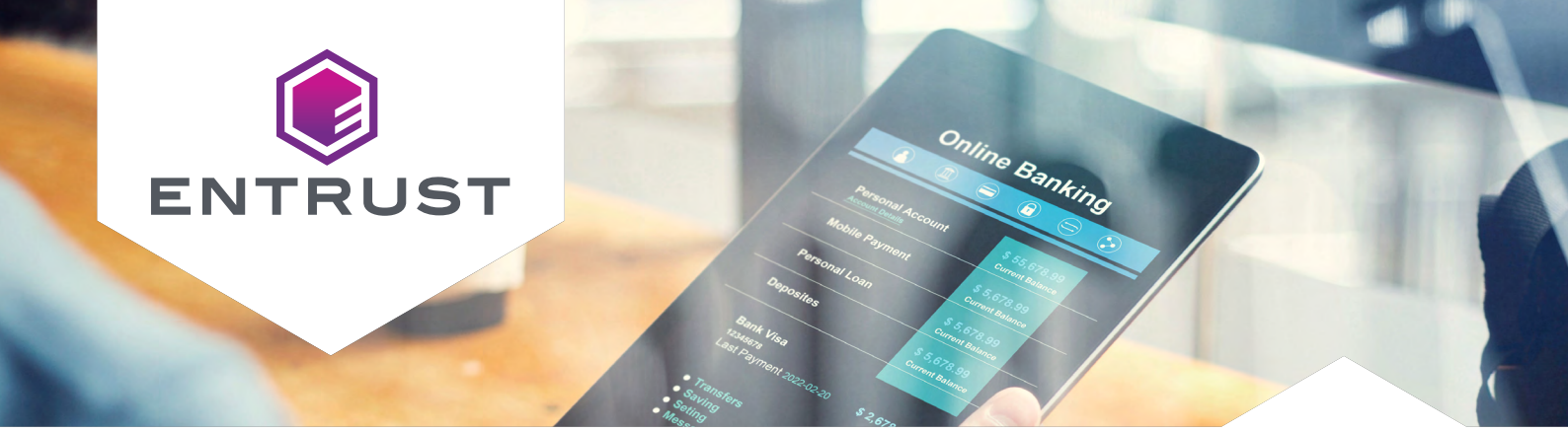


Une banque, qui figure parmi les dix plus importants établissements au monde, a choisi les HSM nShield d'Entrust afin de pouvoir offrir à ses clients et partenaires des services web fiables et sécurisés

DÉFI COMMERCIAL

Toute entreprise disposant d'une présence en ligne orientée client authentifie ses utilisateurs lorsqu'ils utilisent ses services, et les banques internationales de premier plan ne font pas exception. Avec le développement rapide de l'Internet et des transactions en ligne, les données confidentielles échangées en ligne et sur cloud sont devenues des cibles d'attaques de plus en plus fréquentes.

Les services en ligne utilisent des mécanismes de connexion afin de mettre en relation les navigateurs des utilisateurs finaux avec les serveurs web, et ces connexions sont protégées par le protocole SSL (Secure Sockets Layer), une technologie qui permet de chiffrer les données sur Internet. La norme SSL (la technologie derrière le symbole du cadenas dans le navigateur et plus précisément appelée sécurité de la couche transport ou TLS) est la forme de protection de référence pour toutes les communications sur Internet.

> **« Face à l'augmentation constante du trafic Internet et à la prolifération des attaques de logiciels malveillants basés sur le protocole SSL, telles que celles qui profitent de la faille Heartbleed, cette banque de premier plan avait besoin de renforcer et d'améliorer sa capacité à examiner de manière sécurisée le trafic SSL afin de s'assurer qu'aucun virus ou autre logiciel malveillant caché ne puisse infecter ses systèmes. »**

Banque internationale de premier plan

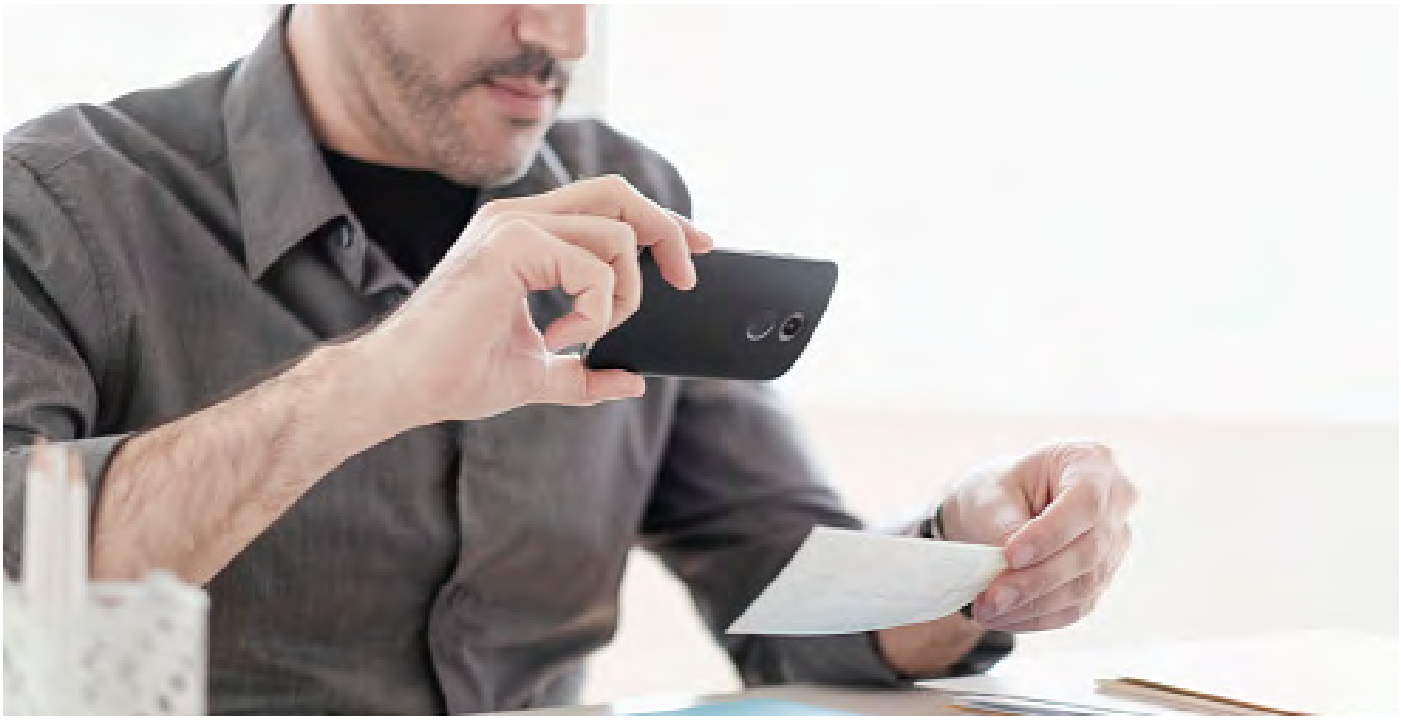
Afin de pouvoir fournir des services web fiables et sécurisés à leurs utilisateurs, les entreprises sont tenues de veiller au respect de la confidentialité, de l'intégrité et de la disponibilité des données traitées par le service. Face à l'augmentation constante du trafic Internet et à la prolifération des attaques de logiciels malveillants basés sur le protocole SSL, telles que celles qui profitent de la faille Heartbleed, cette banque de premier plan avait besoin de renforcer et d'améliorer sa capacité à examiner de manière sécurisée le trafic SSL afin de s'assurer qu'aucun virus ou autre logiciel malveillant caché ne puisse infecter ses systèmes. Ce projet a notamment porté sur l'inspection du trafic généré par les partenaires, les filiales et les employés de la banque.

DÉFI TECHNIQUE

L'augmentation de la quantité de trafic chiffré circulant sur les réseaux d'aujourd'hui fait que le protocole SSL est susceptible d'être un vecteur d'attaques, car des codes malveillants peuvent se cacher et passer inaperçus. L'inspection SSL est utilisée pour filtrer certains éléments potentiellement dangereux qui se cachent au sein d'un contenu chiffré. Elle consiste à intercepter le trafic d'un site web, à le déchiffrer et à l'inspecter, puis à le chiffrer à nouveau pour sa destination finale.

Les modules matériels de sécurité (HSM) procurent une couche de protection supplémentaire pour le nombre grandissant de clés SSL utilisées à la suite du processus de déchiffrement et de rechiffrement. Le déchiffrement, l'inspection et le rechiffrement du trafic lui permettant d'être inspecté et de poursuivre son trajet vers un serveur web (où il est à nouveau déchiffré) impliquent que les clés nécessaires à ce processus soient récupérées plus fréquemment. En général, les clés utilisées ne sont pas toutes les mêmes, d'où la nécessité d'une protection renforcée.

Les HSM établissent une base de confiance qui garantit que toutes les connexions critiques ne soient pas seulement protégées, mais qu'on puisse également s'y fier. Selon le responsable de la sécurité de la banque, il est possible d'inspecter le flux de trafic Internet sans module matériel de sécurité (HSM), mais cela est très dangereux.



Banque internationale de premier plan

Il convient donc de protéger la technologie qui déchiffre le trafic web, ce qui implique de protéger et de sécuriser les clés de déchiffrement. Les HSM remplissent ce rôle.

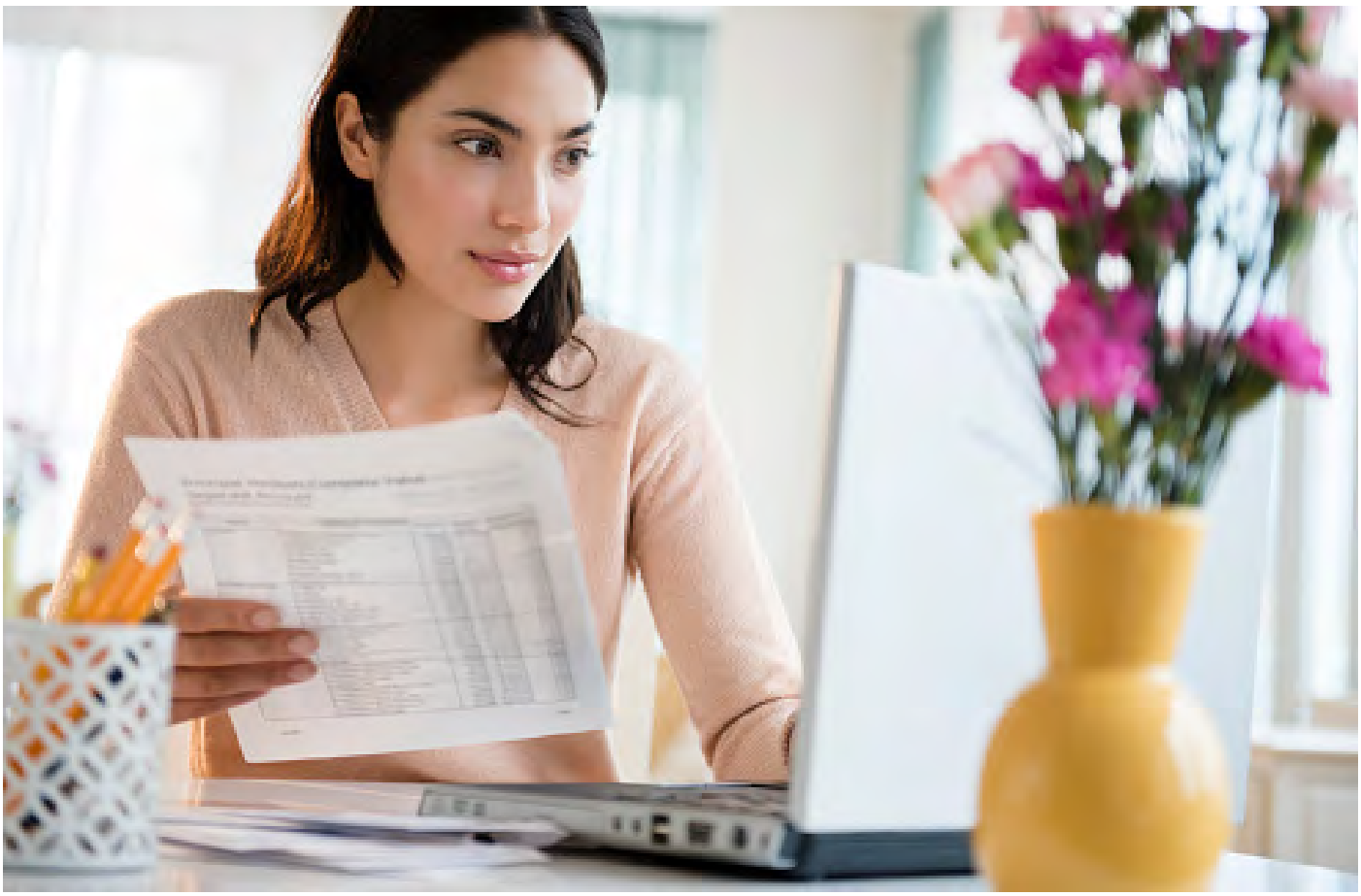
SOLUTION

La banque a choisi de déployer les HSM nShield Connect d'Entrust dans une double configuration « actif-actif » au sein de deux centres de données distants d'environ 10 kilomètres l'un de l'autre. Ces HSM répondent aux exigences de sécurité des 45 serveurs proxy actuellement en place et offrent une grande capacité de développement.

RÉSULTATS

Les HSM nShield d'Entrust ont vocation à multiplier au moins par cinq la capacité du système précédent. Cela permettra à l'organisation d'inspecter le trafic Internet à la recherche d'éventuels codes malveillants cachés et de garantir la sécurité du système au fur et à mesure de son développement.

Cette grande banque mondiale travaille avec Entrust depuis plus de 10 ans et a choisi Entrust comme fournisseur de HSM pour son expérience de la technologie et de la résolution des problèmes. L'équipe de services professionnels d'Entrust a également été déployée pour installer les HSM et former le personnel de la banque pour leur permettre de les utiliser.



Banque internationale de premier plan

Besoin opérationnel

- Fournir aux utilisateurs des services web fiables et sécurisés

Besoin technologique

- Surveiller le volume croissant du trafic Internet interne et assurer la protection de la technologie de suivi
- Protéger l'infrastructure informatique globale de l'organisation

Solution

- Mode « actif-actif » des HSM nShield Connect d'Entrust afin de gérer et protéger les clés SSL

Résultat

- Sécurité certifiée FIPS 140-2 niveau 3 et Critères Communs EAL4+
- Capacité cinq fois supérieure à celle du système précédent
- Grande évolutivité capable de facilement répondre aux futurs besoins

À PROPOS DE 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 portefeuille 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