Entrust aide Zerto a sécuriser l'intégrité de ses applications commerciales

Fondée en 2010, Zerto s'est construite sur le principe que les technologies de récupération en cas de défaillance ne devraient pas être une simple assurance, mais un avantage compétitif.

Zerto aide ses clients à accélérer leur transformation numérique en éliminant le risque et la complexité de la modernisation et de l'adoption du cloud grâce à une informatique robuste. En remplaçant plusieurs solutions anciennes par une seule IT Resilience Platform™, Zerto combine récupération en cas de défaillance, sauvegarde et mobilité du cloud en une seule solution. La plateforme de Zerto est disponible en continu et fonctionne à l'échelle de l'entreprise, ce qui permet de proposer une expérience client continue tout en simplifiant la mobilité de la charge de travail afin de protéger, de récupérer et de déplacer librement les applications dans les clouds multiples et hybrides.

Zerto a révolutionné les marchés informatiques et à repoussé les limites de la récupération en cas de défaillance. L'entreprise a développé un produit novateur en matière de technologie de protection des données continue, et dans un monde où la disponibilité permanente des technologies est non-négociable pour les entreprises, sa solution est bien plus qu'un outil de récupération après défaillance.

> **« Au niveau de la mise en place et du support, Entrust fait mieux que la concurrence. Les HSM nShield d'Entrust sont faciles à utiliser et à sauvegarder, et nous aimons l'interface graphique utilisateur (GUI). »**
>
> – Nadav Svirsky, directeur de l'infrastructure IT de l'entreprise, Zerto

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

Zerto

DÉFI COMMERCIAL

En tant que fournisseur principal de robustesse informatique, Zerto ne pouvait pas se permettre que ses systèmes soient vulnérables. La stratégie la plus efficace pour remédier à ce risque était de faire en sorte que son infrastructure à clé publique (PKI) soit digne de confiance.

Une infrastructure PKI est un ensemble de matériel, de logiciels, de politiques, de processus et de procédures nécessaires pour créer, gérer, distribuer, stocker et révoquer les certificats numériques et les clés publiques. Les PKI permettent d'établir l'identité des personnes, des appareils et des services, assurant ainsi un accès contrôlé aux systèmes et aux ressources, la protection des données et la transparence des transactions. Les applications commerciales de nouvelle génération s'en remettent de plus en plus à la technologie des PKI pour garantir une sécurité élevée dans le cadre de modèles commerciaux en constante évolution, de plus en plus dépendants de l'authentification en ligne des interactions électroniques et qui doivent respecter des réglementations sur la sécurité des données toujours plus strictes.

Afin de lier les clés publiques à leur utilisateur associé (le propriétaire de la clé privée), les PKI s'appuient sur des certificats numériques. Les certificats numériques sont les identifiants utilisés pour vérifier l'identité des utilisateurs lors d'une transaction. Tout comme un passeport atteste de l'identité d'une personne en tant que citoyen d'un pays, le certificat numérique établit l'identité des utilisateurs au sein de l'écosystème. Puisque les certificats numériques sont utilisés pour identifier les destinataires des données chiffrées ou pour vérifier l'identité du signataire, il est indispensable de protéger l'authenticité et l'intégrité du certificat pour préserver la fiabilité du système. En tant que fournisseur de confiance, cet aspect était une pierre angulaire du modèle commercial de Zerto.

DÉFI TECHNIQUE

Les autorités de certification (AC) émettent les identifiants numériques permettant d'identifier les utilisateurs. Les AC sont indispensables à la sécurité des PKI et des services qu'elles soutiennent, et peuvent donc faire l'objet d'attaques sophistiquées. Pour limiter le risque d'attaques contre les AC, il est indispensable de mettre en place des contrôles physiques et logiques ainsi que des mécanismes de renforcement de la sécurité comme les modules matériels de sécurité (HSM) afin de garantir l'intégrité d'une PKI.

Zerto utilise une plateforme Microsoft, et le département IT savait grâce à son expérience auprès de Microsoft que l'utilisation de HSM était la meilleure pratique pour sécuriser ses AC. Les HSM fournissent un environnement certifié indépendamment et résistant au sabotage. Ils sont indispensables pour sécuriser les clés et les processus commerciaux sensibles.

Zerto

> **Déployer les HSM nShield d'Entrust pour sécuriser nos AC nous assure la tranquillité. Notre direction pense que l'investissement en vaut la chandelle.**
>
> – Nadav Svirsky, directeur de l'infrastructure IT de l'entreprise, Zerto

SOLUTION

L'équipe informatique de Zerto avait travaillé avec plusieurs fournisseurs de HSM et ont choisi les HSM nShield® Solo d'Entrust. D'après Nadav Svirsky, directeur de l'infrastructure informatique de l'entreprise, parmi tous les fournisseurs disponibles, Zerto s'est tournée vers Entrust, car « la mise en place et le support d'Entrust sont meilleurs que ceux de la concurrence, les HSM nShield Solo d'Entrust sont plus faciles à utiliser et à sauvegarder et nous aimons également l'interface utilisateur graphique (GUI). »

RÉSULTATS

Zerto ne divulgue pas les résultats quantifiables de l'installation des HSM nShield d'Entrust pour protéger ses AC. L'objectif initial était de mettre en place les meilleures pratiques en matière de sécurité. À ce sujet, Svirsky remarque : « Nos clients doivent pouvoir avoir confiance en nos systèmes. Malheureusement, il est souvent impossible de voir la valeur de la sécurité des données, sauf en cas de problème. À ce moment-là, la réputation, les ventes et le prix des actions de l'entreprise dégringolent. C'est pourquoi déployer les HSM nShield Solo d'Entrust pour sécuriser nos AC nous assure la tranquillité. Notre direction pense que l'investissement en vaut la chandelle. »

Zerto

PERFORMANCE, FIABILITÉ ET PROTECTION

Besoin opérationnel

- Réduction des risques de problèmes de sécurité des données internes

Besoin technologique

- Sécurisation de la racine de confiance des serveurs d'AC pour un coût raisonnable

Solution

- Les HSM nShield Solo d'Entrust

Résultat

- Réduction des risques
- Tranquillité pour la direction de Zerto

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