Confidential Computing : réinventer les modèles de sécurité avec AWS Nitro System

Le monde financier est confronté à des défis de sécurité croissants, avec des cyberattaques toujours plus sophistiquées. Le confidential computing, ou informatique confidentielle, est une des réponses à ces défis en renforçant la sécurité des données.

STEPHAN HADINGER,

Directeur de la Technologie AWS France

1. Pourquoi le Confidential Computing permet-il de renforcer la sécurité ?

Le confidential computing est une approche qui protège les données sensibles lorsqu'elles sont en cours de traitement. **Cette approche est complémentaire au chiffrement des données au repos (stockées) et en transit (pendant le transfert), car elle sécurise les données en mémoire, là où elles sont aussi vulnérables aux attaques.** Le confidential computing est apparu sur le devant de la scène au début des années 2010 et, depuis lors, il a suscité un vif intérêt dans le domaine de la recherche et développement (R&D). Les investissements massifs consacrés à cette technologie témoignent de son potentiel et de sa capacité à transformer la manière dont les entreprises gèrent et sécurisent les données. Dans le secteur financier, où la confidentialité et l'intégrité des informations sont cruciales, le confidential computing joue un rôle essentiel pour préserver la sécurité des données et la confiance des clients.

2. Comment AWS réinvente les modèles de sécurité en proposant AWS Nitro System par défaut sur ses services?

Amazon Web Services (AWS), leader dans le domaine du cloud, a développé une solution innovante appelée **AWS Nitro System.** Il s'agit d'un ensemble de technologies qui permet d'améliorer les performances et la sécurité des services cloud d'AWS. **C'est une exclusivité AWS,** notamment disponible dans la Région Paris d'AWS depuis 2017. Concrètement, ce sont des cartes accélératrices que nous mettons dans chaque serveur. Ces cartes améliorent les performances, réalisent du chiffrement à la volée de toutes les données entrantes et sortantes. Mais surtout ces cartes créent une barrière physique de sécurité.

AWS Nitro System empêche même les opérateurs d'AWS d'accéder aux données des clients. **On peut comparer le système Nitro à un coffre-fort sans serrure** : même si quelqu'un voulait accéder aux données à l'intérieur, il ne pourrait pas le faire, faute d'outils. En utilisant le système AWS Nitro, la sécurité des données est renforcée car il élimine la possibilité d'accès non autorisé par les clients et restreint techniquement l'accès à tout opérateur, y compris les employés d'AWS. AWS Nitro System crée ainsi une barrière physique qui empêche tout accès à vos données pendant les courts moments où ces données sont en clair dans les unités de traitement des serveurs. Le développement du système Nitro a permis de repenser radicalement

l'architecture de virtualisation pour offrir une sécurité optimale aux clients. AWS a réussi à créer une solution de sécurité puissante et flexible adaptée aux besoins des entreprises du secteur financier.

3. Donner aux clients le contrôle de leurs données.

Grâce au confidential computing, AWS Nitro System met en place un environnement où AWS ne peut techniquement pas accéder aux données de ses clients, sans leur autorisation explicite. Cette approche est cruciale pour protéger les données des entreprises financières contre les demandes d'accès de la part d'autorités étrangères. Elle s'inscrit dans une approche plus globale d'AWS concernant la sécurité : **donner aux clients le contrôle de leurs données.**

Aujourd'hui, le contrôle des ressources numériques, ou souveraineté numérique, est plus important que jamais. C'est pourquoi nous avons récemment lancé l'***AWS Digital Sovereignty Pledge*** – notre engagement à offrir à tous les clients AWS l'ensemble le plus avancé d'outils et de fonctionnalités de contrôle disponibles dans le cloud au service de la souveraineté.

Contrôle de l'emplacement de vos données
AWS a toujours permis à ses clients de contrôler l'emplacement de leurs données. Aujourd'hui en Europe, par exemple, les clients ont le choix de déployer leurs données dans l'une des huit Régions existantes. Nous nous engageons à fournir encore plus de services et de capacités pour protéger les données de nos clients. Nous nous engageons également à développer nos capacités existantes pour fournir des contrôles de localisation des données encore plus précis et transparents. Nous allons également étendre les contrôles de localisation des données pour les données opérationnelles, telles que les informations relatives à l'identité et à la facturation.

Contrôle fiable de l'accès aux données
Le système AWS Nitro, qui constitue la base des services informatiques d'AWS, utilise du matériel et des logiciels

spécialisés pour protéger les données contre tout accès extérieur pendant leur traitement sur les serveurs EC2. Nous nous engageons à continuer à développer des restrictions d'accès supplémentaires qui limitent tout accès aux données de nos clients, sauf indication contraire de la part du client ou de l'un de ses prestataires de confiance.

La possibilité de tout chiffrer, partout
Aujourd'hui, nous offrons à nos clients des fonctionnalités et des outils de contrôle pour chiffrer les données, qu'elles soient en transit, au repos ou en mémoire. Tous les services AWS prennent déjà en charge le chiffrement, la plupart permettant également le chiffrement sur des clés gérées par le client et inaccessibles à AWS. Nous nous engageons à continuer d'innover et d'investir dans des outils de contrôle au service de la souveraineté et des fonctionnalités de chiffrement supplémentaires afin que nos clients puissent chiffrer l'ensemble de leurs données partout, avec des clés de chiffrement gérées à l'intérieur ou à l'extérieur du cloud AWS.

Depuis décembre 2022, AWS permet à ses clients, directement ou via un tier de confiance, de gérer et sécuriser les clés de chiffrements à l'extérieur du Cloud AWS. En France, ATOS et THALES proposent notamment de tels services.

La résilience du cloud
La souveraineté numérique est impossible sans résilience et sans

capacités de continuité d'activité lors de crise majeure. Le contrôle des charges de travail et la haute disponibilité de réseau sont essentiels en cas d'événements comme une rupture de la chaîne d'approvisionnement, une interruption du réseau ou encore une catastrophe naturelle. Actuellement, AWS offre la plus haute disponibilité de réseau de tous les fournisseurs de cloud. Chaque Région AWS est composée de plusieurs zones de disponibilité (AZ), qui sont des portions d'infrastructure totalement isolées. Pour mieux isoler les difficultés et obtenir une haute disponibilité de réseau, les clients peuvent répartir les applications sur plusieurs zones dans la même Région AWS. Pour les clients qui exécutent des charges de travail sur place ou dans des cas d'utilisation à distance ou connectés par intermittence, nous proposons des services qui offrent des capacités spécifiques pour les données hors ligne, le calcul et le stockage à distance. Nous nous engageons à continuer d'améliorer notre gamme d'options souveraines et résilientes, permettant aux clients de maintenir leurs activités en cas de perturbation ou de déconnexion.

Conclusion

Le confidential computing, et plus particulièrement AWS Nitro System, redéfinissent la manière dont les entreprises financières peuvent protéger leurs données sensibles. **AWS Nitro System est une technologie de pointe qui renforce la sécurité des données pour les entreprises dans le domaine financier.** En combinant le chiffrement en mémoire avec le chiffrement au repos et en transit, le Confidential Computing s'impose comme une protection essentielle pour les entreprises qui manipulent des informations financières sensibles. ■