Fiche solution

Processeurs Intel® Xeon® Scalable de 5e génération
Informatique confidentielle

Gestion des secrets avec HashiCorp Vault et Intel® TDX (Intel® Trust Domain Extensions)

HashiCorp Vault protège et gère les clés de chiffrement privées, les informations d'identification et autres secrets, réduisant ainsi la surface d'attaque des fonctions de sécurité réseau. Grâce à la protection matérielle Intel® TDX, Vault est encore plus isolé et protégé d'autres VM (machines virtuelles) et logiciels système. Intel® TDX est généralement disponible sur les processeurs Intel® Xeon® Scalable de 5e génération.

La complexité et le coût de la cybersécurité sont plus élevés que jamais, tout comme les dommages que peuvent causer des attaques imparfaitement neutralisées. Selon IBM, le coût global moyen lié à une violation des données ressort à 4,45 millions de dollars pour 2023, un montant qui a grimpé de 15,3 % au cours des trois dernières années et continue de croître[1]. Face à l'immédiateté et l'ampleur de ces menaces, les entreprises ont pour impératif de se conformer aux meilleures pratiques, d'innover là où elles le peuvent et de protéger leurs données vitales. D'ailleurs, 51 % d'entre elles prévoient d'augmenter leurs investissements en matière de sécurité à la suite d'une violation[1].

Elles sont nombreuses à vouloir accroître leur dispositif de sécurité, sans être entravées par les coûts ou les perturbations, en renforçant le chiffrement des données dans leurs opérations. Les solutions de mise en réseau axées sur la sécurité, comme le ZTNA (pour accès au réseau Zero Trust) et les services SASE (Secure Access Service Edge), gagnent également du terrain, ce qui accroît toujours plus le recours au chiffrement. Cette stratégie explique l'importance prise par les systèmes de gestion des secrets, à même d'assurer le stockage sécurisé de clés de chiffrement privées et d'autres informations d'identification (mots de passe, certificats…). Pour tous ces cas, le chiffrement des données, qu'elles soient au repos ou en transit, réduit la surface d'attaque et aide à protéger les données sensibles.

À ceci près que les données comprenant des clés de chiffrement et d'autres secrets ne sont généralement pas chiffrées lorsqu'elles sont sollicitées, ce qui les expose à un risque de compromission. Les processus qui compromettent ces secrets dans l'espace mémoire partagé sont habituellement isolés les uns des autres par des stratégies logicielles, parfois vulnérables aux attaques par escalade de privilèges et à la violation du système d'exploitation, de l'hyperviseur ou de tout autre logiciel système.

L'informatique confidentielle renforce cette isolation à l'aide de technologies ancrées dans le matériel, sous la couche logicielle du système et hors de portée d'attaques logicielles. Ces technologies de réduction de la vulnérabilité et de protection des données en cours de traitement connaissent un essor, loin de se démentir.

TAILLE DU MARCHÉ DE L'INFORMATIQUE CONFIDENTIELLE

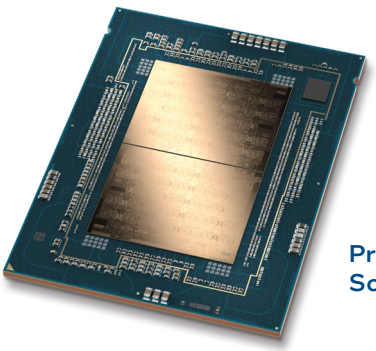
94,4 % (en CAGR)
2023-2026[2]

53,31 MILLIARDS DE DOLLARS
D'ici à 2026[2]

Avec son système de gestion des secrets Vault, HashiCorp se trouve à la pointe de cette évolution vers la mise en œuvre d'une informatique confidentielle dédiée à l'entreprise. Combinés, Vault et Intel® TDX (Intel® Trust Domain Extensions) peuvent venir en aide aux clients qui ont besoin d'environnements informatiques confidentiels pour leurs charges de travail sensibles. Intel® TDX, qui intègre désormais généralement les processeurs Intel® Xeon® Scalable de 5e génération, isole Vault au niveau de la VM afin de protéger tout secret en cours de traitement des autres locataires de la VM, de l'hyperviseur, des logiciels système et des administrateurs.

Une plateforme de pointe pour des charges de travail performantes et isolées

Avec HashiCorp Vault, les processeurs Intel® Xeon® Scalable de 5e génération forment le socle matériel de l'informatique confidentielle. En plus d'Intel® TDX, la plateforme offre performances et efficacité énergétique. Les ressources d'exécution présentent des performances élevées par cœur, et ce jusqu'à 64 cœurs, avec des accélérateurs intégrés pour l'IA, le chiffrement et d'autres charges de travail critiques. Cette plateforme équilibrée se caractérise également par 16 % de bande passante mémoire en plus[3] et une augmentation du LLC (cache de dernier niveau) de 3 fois supérieure aux processeurs Intel® Xeon® de 4e génération[4].



Processeurs Intel® Xeon® Scalable de 5e génération

La plateforme comprend deux modèles de processeurs optimisés pour les charges de travail de sécurité réseau, conçus pour un débit élevé, et une faible latence sur les charges de travail comprenant pare-feu de nouvelle génération, SD-WAN et SASE, offrant également une applicabilité au calcul générique dans le Cloud.

- **Les processeurs Intel® Xeon® Gold 6548N** (2 sockets, 32 cœurs, 2,8 GHz) sont adaptés à la mise en œuvre de mesures de sécurité de niveau intermédiaire.
- **Les processeurs Intel® Xeon® Platinum 8571N** (1 socket, 52 cœurs, 2,4 GHz) sont adaptés à la mise en œuvre de mesures de sécurité de niveau élevé et disposent d'un LLC jusqu'à trois fois supérieur.

Grâce à la combinaison de HashiCorp Vault et des processeurs Intel® Xeon® Scalable de 5e génération, les entreprises peuvent envisager de nouveaux modèles commerciaux alliant protection des données sensibles partagées et de la propriété intellectuelle, et performance pour un rapport qualité/prix susceptibles de réduire les coûts d'exploitation.

L'informatique confidentielle isole les données sensibles ou réglementées des tiers privilégiés ainsi que des logiciels et des utilisateurs non autorisés, en se fondant sur une racine de confiance matérielle allant du bas vers le haut de la pile de solutions, ce qui crée un TEE (environnement d'exécution fiable) doté d'un socle matériel de bas niveau à même d'éliminer les dépendances logicielles et les vulnérabilités connexes. Le TEE protège Vault et l'intégrité des opérations effectuées sur celle-ci. Contrairement aux stratégies logicielles, le TEE est protégé de tout accès non autorisé par des logiciels ou utilisateurs, quel que soit leur niveau de privilège.

Les processeurs Intel® Xeon® Scalable de 5e génération améliorent considérablement les technologies d'informatique confidentielle des modèles précédents en raison du TEE disponible au niveau de la VM et de l'isolation applicative, qui peuvent être utilisés indépendamment l'un de l'autre. Intel® TDX (Intel® Trust Domain Extensions) permet de renforcer l'isolation et la confidentialité des VM. Au sein d'une VM confidentielle, Intel® TDX, le système d'exploitation invité et les applications de la VM sont isolés : ils n'offrent pas d'accès à l'hôte du Cloud, l'hyperviseur et d'autres VM confidentielle, de la plateforme. Cela simplifie la migration des VM existantes vers un TEE, n'entraînant qu'une baisse des performances estimée à moins de 5 % sur HashiCorp Vault[5].

Les processeurs Intel® Xeon® Scalable de 5e génération proposent également le chiffrement Intel® TME (Intel® Total Memory Encryption), comme technologie chargée de l'exécution de l'informatique confidentielle de Vault basée sur Intel® TDX. Grâce à Intel® TME, l'hyperviseur peut chiffrer séparément plusieurs VM (ou conteneurs) avec des clés de chiffrement uniques appartenant aux locataires. Cette technologie matérielle de chiffrement incorporée ne nécessite aucune modification des applications et présente des performances notables. L'ingénierie conjointe de HashiCorp et d'Intel a permis à Vault de se positionner sur le marché de l'informatique confidentielle de nouvelle génération.

HashiCorp Vault : une gestion des secrets et du chiffrement

L'informatique confidentielle vise essentiellement la protection des secrets applicatifs (clés de chiffrement, mots de passe, jetons, certificats et autres données sensibles). HashiCorp Vault est un système de gestion des secrets qui exécute des services de chiffrement, d'authentification et d'autorisation pour assurer avec fiabilité le stockage, la gestion, le contrôle et la vérifiabilité des secrets.

Les données protégées peuvent être stockées et gérées dans Vault qui restreint fortement l'accès et le contrôle tout en offrant des mesures de gouvernance vérifiables. On accède au contenu de Vault par interface graphique et interface de ligne de commande, l'accès programmatique se faisant par API HTTP. Avant tout accès, Vault procède à une validation, une authentification et une autorisation des clients (utilisateurs, machines, applications...), ce qui contribue à la solidité et à la cohérence de la sécurité. Ces mécanismes sont essentiels pour comprendre et contrôler les schémas d'accès aux données critiques.

Vault utilise des jetons clients qui régissent l'accès en fonction de règles client individualisées qui limitent les ressources auxquelles il est possible d'accéder et les actions qui peuvent être effectuées sur ces ressources. Les jetons peuvent être créés manuellement et attribués aux clients, voire être générés en libre-service à l'aide d'un service logiciel. Le référentiel Vault les protège d'une exposition involontaire. Il gère également l'authentification et l'autorisation pour un contrôle d'accès efficace.

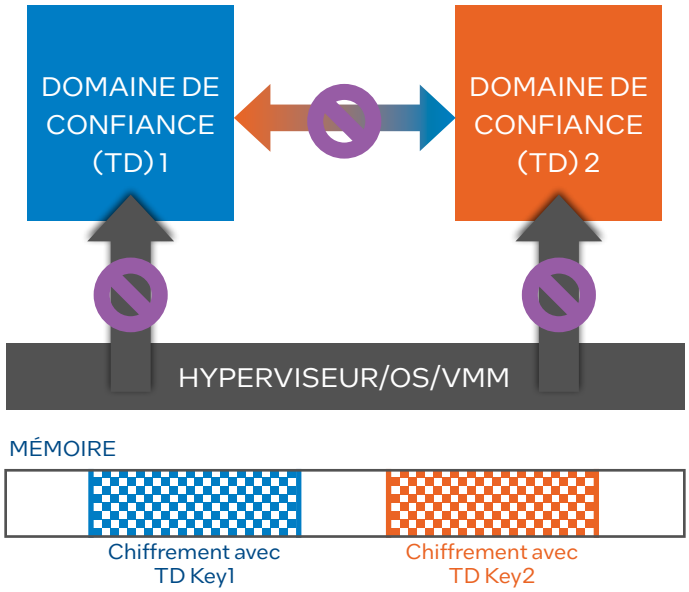
Outre la protection des accès, Vault offre également des fonctionnalités d'analyse et de gestion qui permettent de comprendre et de régir les parties, les applications et les services accédant à des secrets spécifiques, sur toutes les plateformes. Vault a pour principales caractéristiques :

- **Stockage sécurisé des secrets**. Vault chiffre les paires clé/valeur secrètes avant de les écrire sur le support de stockage, offrant ainsi une couche de protection supplémentaire, au-delà de la protection du support de stockage lui-même.
- **Secrets dynamiques**. Vault peut générer à la demande des secrets de courte durée, comme des identifiants pour une base de données ou un volume de stockage, et les révoquer automatiquement après usage.
- **Chiffrement des données en temps réel**. Vault peut chiffrer et déchiffrer des données sans les stocker : les développeurs peuvent ainsi stocker des données cryptées dans des bases de données ou d'autres magasins de données classiques sans avoir à définir de schémas de chiffrement.
- **Bail et renouvellement**. L'espace de stockage conserve des baux pour chaque secret afin de régir la révocation automatique du secret au terme du bail ; les API intégrées fournissent le mécanisme permettant aux clients de renouveler les secrets.
- **Révocation des secrets intégrée**. Vault automatise la révocation d'ensembles de secrets (comme les secrets d'un type donné ou auxquels un utilisateur donné a accédé), un atout précieux pour le roulement des clés et les parades face à une intrusion.

Pour renforcer davantage l'isolation cryptographique des secrets, Vault peut être déployé dans une VM protégée par une informatique confidentielle basée sur Intel® TDX. Cette stratégie se conforme à ce que HashiCorp a voulu développer pour sa solution : la plateforme Vault peut en effet s'adapter telle quelle à l'informatique confidentielle, sans modification de code ni baisse rédhibitoire des performances.

Isolation et protection de Vault avec Intel® TDX

Intel® TDX accroît l'informatique confidentielle par un nouveau type d'invité VM, le TD ou domaine de confiance (Trust Domain). Chaque TD est responsable de sa propre barrière de protection, et fonctionne par une mémoire chiffrée qui est isolée au moyen de clés de chiffrement privées uniques et dédiées. Essentielle à la défense en profondeur, cette indépendance offre une protection secrète renforcée basée sur Vault. Elle contribue à éliminer les obstacles auxquels se heurtent les entreprises lorsqu'elles font évoluer leur stratégie de sécurité pour réseaux hautement distribués, notamment lorsqu'elles passent à de nouveaux modèles de sécurité tels que ZTNA et SASE.



Les locataires sont isolés grâce à des domaines de confiance, chacun étant chiffré à l'aide d'une clé unique.

Comme Intel® TDX place l'intégralité de la VM dans un domaine de confiance unique, les appels aux services en dehors de la frontière de confiance sont réduits pour Vault. Chaque cycle d'entrée et de sortie associé aux appels exige que la partie matérielle effectue des opérations pour protéger le cache et la mémoire lorsque le flux de contrôle transite par-delà la frontière de confiance. Faire en sorte que ces opérations soient moins nécessaires explique la faible surcharge de temps et les performances élevées de HashiCorp Vault basée sur Intel® TDX pour l'exécution d'une informatique confidentielle.

Conclusion

La disponibilité d'Intel® TDX dans les processeurs Intel® Xeon® Scalable de 5e génération fournit à HashiCorp Vault une protection de la mémoire au niveau de la VM, sans recourir à des modifications de code ni grever lourdement les performances. À mesure que les secrets d'application continuent de proliférer, cette protection préservera les mécanismes d'authentification, de chiffrement, d'autorisation et d'accès dont dépend la cybersécurité, en particulier pour les charges de travail sensibles. Les travaux d'ingénierie menés conjointement par HashiCorp et Intel poursuivront sur cette voie stratégique afin de concrétiser toujours plus les promesses de l'informatique confidentielle.

Pour en savoir plus

Intel® TDX (Intel® Trust Domain Extensions)

HashiCorp Vault

Cette solution vous est proposée par :

intel xeon + HashiCorp

[1] IBM, Coût d'une fuite de données - rapport 2023 (Cost of a Data Breach Report 2023). https://www.ibm.com/reports/data-breach.

[2] Fortune Business Insights, Taille, part et analyse d'impact après COVID-19 du marché de l'informatique confidentielle.("Confidential Computing Market Size, Share & COVID-19 Impact Analysis.") https://www.fortunebusinessinsights.com/confidential-computing-market-107794.

[3] Consultez [G12] à la page intel.com/processorclaims: processeurs Intel® Xeon® Scalable de 5e génération. Vos résultats peuvent varier.

[4] Consultez [G11] à la page intel.com/processorclaims: processeurs Intel® Xeon® Scalable de 5e génération. Vos résultats peuvent varier.

[5] Configurations du système : 6562C : 1 nœud, 2x processeur Intel® Xeon® Gold 6562C, 32 cœurs, HT activé, Turbo activé, mémoire totale 256 Go (16 connecteurs/16 Go/4800 MT/s), 1x contrôleur Ethernet X710 norme 10GBASE-T, 4x contrôleur Ethernet E810-C pour QSFP, BIOS American Megatrends International, LLC. 3B05.TEL4P1, Ubuntu 22.04 LTS, kernel 5.19.17-mvp23v3+6-generic, gcc (GCC) 11.4.0, Vault v1.14.1+ent, dpdk-stable-22.11.1, vault-benchmark v0.1.1, envoy 1.26.2, Open vSwitch 3.2.90, tdx-tools 2023ww22, requêtes par seconde mesurées avec une utilisation CPU de 100 %. Tests réalisés par Intel le 22 novembre 2023.

Les performances varient selon l'usage, la configuration et d'autres facteurs. Rendez-vous sur www.Intel.com/PerformanceIndex.

Les résultats de performances s'appuient sur des tests à la date telle que décrit dans les configurations et peuvent ne pas refléter la totalité des mises à jour disponibles publiquement. Pour obtenir plus de détails, veuillez lire les informations de configuration. Aucun produit ou composant ne peut être totalement sécurisé en toutes circonstances.

Vos coûts et résultats peuvent varier.

Intel ne contrôle ni n'audite les données de parties tierces. Nous vous recommandons de consulter d'autres sources afin de confirmer si les données référencées sont exactes.

Les technologies Intel® peuvent nécessiter du matériel, des logiciels ou l'activation de services compatibles.

1123/LH/MESH/353954-001US