Fiche produit

Sécurité accélérée
Processeurs Intel® Xeon® Scalable

Accélérer l'innovation et améliorer la protection des données avec les moteurs intégrés Intel® Security Engines

Maintenez les performances tout en aidant à préserver la confidentialité des données et l'intégrité du code grâce aux Intel® Security Engines et aux processeurs Intel® Xeon® Scalable de 5e génération.

Plateforme Intel® Xeon® Scalable : mettez à profit vos données, tout en contribuant à leur confidentialité et à leur protection grâce à l'informatique confidentielle.

Aujourd'hui, la pratique standard est de crypter les données, qu'elles soient stockées ou en transit. Cependant, les entreprises se heurtent au défi de la protection des données lorsque le processeur et la mémoire les traitent activement. À ce stade, les données sensibles (informations personnelles identifiables, dossiers médicaux, transactions financières...) sont vulnérables à des exploits éventuels, à une divulgation accidentelle ou à des manquements à une obligation de conformité.

Dans un monde toujours plus axé sur l'information, les entreprises doivent protéger leurs données contre tout accès non autorisé. Les processeurs Intel® Xeon® Scalable dotés d'Intel® Security Engines fournissent une solution matérielle à l'informatique confidentielle, afin que les entreprises puissent extraire des informations, déployer des modèles d'IA et exploiter la puissance des données tout en veillant à leur confidentialité.

Grâce aux processeurs Intel® Xeon® de 5e génération, les entreprises peuvent créer des enclaves sécurisées au sein de leurs processeurs dans lesquelles les données sensibles peuvent être traitées et analysées sans être exposées à d'autres logiciels, collaborateurs ou fournisseurs de Cloud. Cette approche ouvre de nouvelles possibilités : des données auparavant trop sensibles pour être analysées peuvent à présent être exploitées. En protégeant les données pendant leur utilisation, les processeurs Intel® Xeon® Scalable de 5e génération peuvent aider au respect des obligations en matière de confidentialité et de conformité qui incombent aux organisations.

Grâce aux enclaves sécurisées, les données sont protégées contre les accès non autorisés pendant leur traitement effectif. En sollicitant Intel® SGX (Intel® Software Guard Extensions) et Intel® TDX (Intel® Trust Domain Extensions), les processeurs Intel® Xeon® Scalable offrent aux clients un choix de technologies d'informatique confidentielle répondant à leurs attentes.

Adoptez l'informatique confidentielle avec Intel® SGX et Intel® TDX

Avec Intel® SGX, l'informatique confidentielle favorise l'isolation au niveau de l'application ou de la fonction. Dans le Cloud, en périphérie ou sur site, vos calculs et données sensibles bénéficient d'une protection et d'une sécurisation accrues vis-à-vis du fournisseur de services dans le Cloud, des administrateurs non autorisés, du système d'exploitation et à d'autres applications privilégiées.

Témoignage client : une sécurité au service de l'innovation avec les processeurs Intel® Xeon® Scalable

Dans le secteur des soins de la santé, les processeurs Intel® Xeon® Scalable aident BeeKeeperAI à développer des algorithmes d'apprentissage automatique soucieux de la protection des données sensibles. À l'aide d'Intel® SGX, les gestionnaires de données peuvent vérifier l'intégrité de l'application incorporant de l'IA.

Tout savoir de ce projet ›

La plateforme cloud native Zero Trust Exchange de Zscaler connecte utilisateurs, appareils et applications en sécurité où qu'ils se trouvent. Zscaler isole sa plateforme Zero Trust Exchange et ses machines App Connectors dans des TEE Intel® TDX et utilise Intel® Trust Authority pour vérifier leur authenticité et leur intégrité dans de multiples infrastructures Cloud.

Lire le témoignage ›

Les perspectives de transformation sont nombreuses

- Services et analyses assurés par l'IA
- Économie et échelle de l'informatique dans le Cloud
- Applications distribuées et en périphérie
- Innovation dans les services avec l'emploi de nouvelles sources de données
- Technologies préservant la confidentialité
- Services basés sur la blockchain
- Collaboration à parties multiples autour des données

Intel® SGX est le TEE (Trusted Execution Environment, ou environnement d'exécution de confiance) pour centre de données le plus étudié et le plus actualisé, offrant la plus petite surface d'attaque au sein d'un système[1]. Forts de cet environnement, les processeurs Intel® Xeon® Scalable favorisent des solutions d'informatique confidentielle dans des contextes multiples, à la périphérie et dans le Cloud.

Intel® SGX offre une solution de sécurité matérielle visant la protection les données en cours de traitement, grâce à une technologie d'isolation des applications. En protégeant le code et les données sélectionnés des inspections ou modifications, les développeurs peuvent exécuter des opérations de données sensibles à l'intérieur d'enclaves, dans un souci d'accroître la sécurité applicative et de protéger la confidentialité des données.

En outre, les capacités d'attestation d'Intel® SGX offrent une plus grande confiance dans le fait que le logiciel exécuté dans l'enclave correspond à ce qui est attendu et préalablement convenu par toutes les parties.

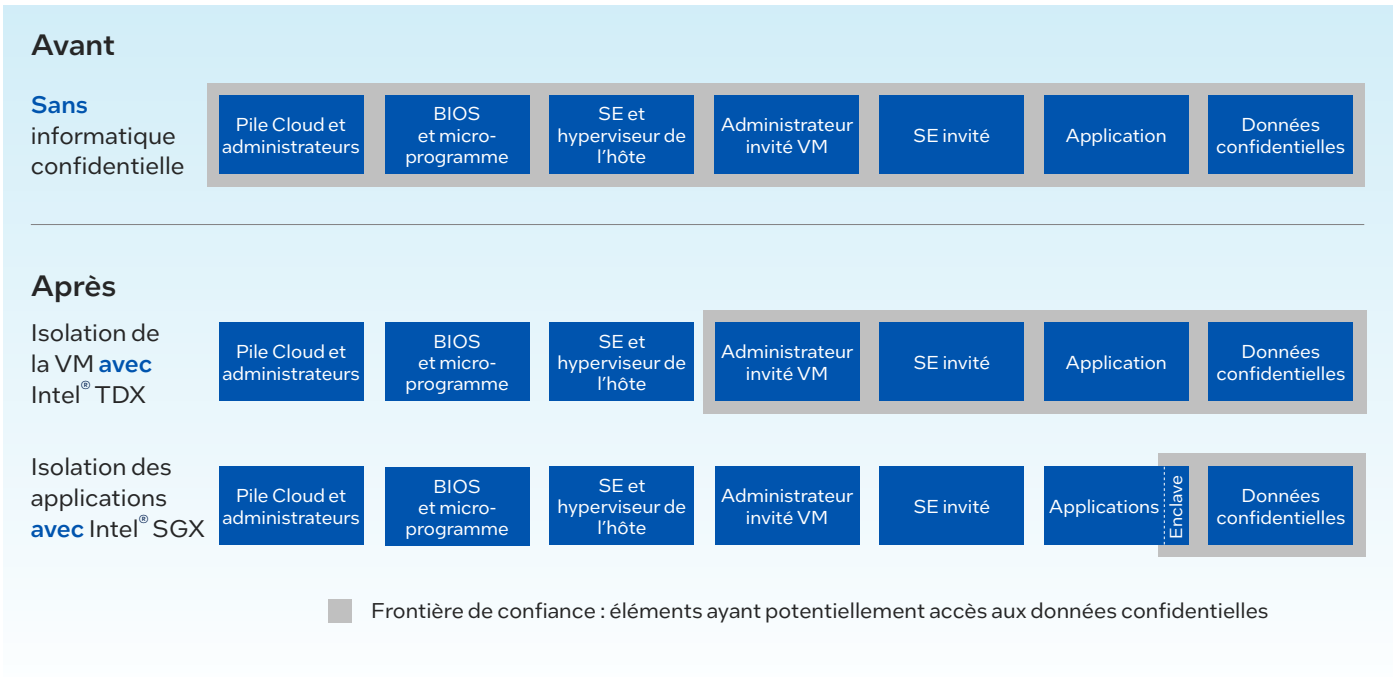
Alors qu'Intel® SGX se destine à l'isolation des applications et des fonctions, Intel® TDX est affecté à l'isolation et la confidentialité au niveau de la VM (Virtual Machine, ou machine virtuelle). Avec cet outil, le système d'exploitation invité et les applications de la VM sont isolés de l'hôte Cloud, de l'hyperviseur et des autres VM de la plateforme. Le périmètre de confiance d'Intel® TDX est plus large que l'isolation des applications d'Intel® SGX, mais Intel® TDX est conçu de manière que les VM confidentielles soient plus faciles à déployer et à gérer à grande échelle que les enclaves d'application. De plus, Intel® TDX simplifie le processus de migration des applications existantes vers un TEE. Les clients constatent jusqu'à 11 % d'augmentation des performances des machines virtuelles sur les plateformes Intel® Xeon® Scalable de 5e génération avec TDX par rapport aux plateformes Intel® Xeon® Scalable de 4e génération sans TDX sur les nombres entiers, la virgule flottante et le modèle BERT-large[2].

Optimiser la conformité réglementaire tout en accélérant l'analyse des données

Les données qui possèdent une valeur pour les entreprises font régulièrement l'objet de réglementations strictes en matière de protection de la vie privée. Leur contrevenir pourrait entraîner des amendes et d'autres pénalités, et ainsi freiner les entreprises dans l'exploitation exhaustive des données sensibles. Certaines solutions palliatives existent pour l'exploitation d'informations personnellement identifiables, mais elles ralentissent souvent de manière significative les processus d'analyse voire entravent leur précision. Avec les processeurs Intel® Xeon® Scalable de 5e génération et le portefeuille pour l'informatique confidentielle d'Intel, les entreprises peuvent créer des enclaves cryptées contribuant à préserver la confidentialité des données et des applications, et optimisant à la fois la conformité et la disponibilité des données.

Lever les obstacles au partage des données sensibles

Le partage de données entre entités peut considérablement accroître la précision et la vitesse des processus métiers, notamment l'entraînement des réseaux neuronaux. Grâce aux processeurs Intel® Xeon® Scalable de 5e génération, le partage des données confidentielles peut s'effectuer en activant des modèles de calcul sollicitant des tiers de confiance comme l'apprentissage fédéré. Dotés des technologies Intel® pour l'informatique confidentielle, ces processeurs permettent à de multiples parties prenantes de mettre en commun des données sensibles pour tirer les fruits d'une analyse collective sans exposer leurs données privées à des utilisateurs non autorisés.



Renforcement de la sécurité : protégez les performances avec Intel® Crypto Acceleration et Intel® QAT (Intel® QuickAssist Technology)

Les centres de données s'emploient à protéger leurs données, tout en s'appuyant sur la cryptographie pour les processus réseau, stockage et compression des données, outre la défense traditionnelle du périmètre. L'essor de la cryptographie s'accompagne d'une explosion du nombre de cycles de cryptage que les processeurs doivent exécuter, ce qui peut rejaillir sur les performances et l'expérience utilisateur.

Intégrées aux processeurs Intel® Xeon® Scalable de 5e génération, les technologies avancées d'accélération cryptographique facilitent la sécurité cryptographique à des niveaux plus élevés, optimisent les performances et offrent une expérience utilisateur plus transparente, sans l'ajout de cœurs et de processeurs supplémentaires au centre de données.

L'accélérateur de compression et de cryptage de données Intel® QAT est intégré à l'accélérateur intégré des processeurs Intel® Xeon® Scalable de 5e génération pour la compression/décompression de données à la volée et les charges de travail cryptographiques. Grâce au déchargement des charges de travail à forte intensité de calcul, Intel® QAT peut récupérer une partie de la capacité des cœurs au profit d'autres charges de travail, tout en contribuant à réduire les coûts et les empreintes de données compressées[4]. Les clients peuvent constater une performance NGINX TLS Handshake par cœur jusqu'à 1,85 fois plus élevée sur la 5e génération Intel® Xeon® Platinum 8592+ avec QAT intégré par rapport à la 4e génération AMD EPYC 9554 OOB[5].

Les instructions Intel® Crypto Acceleration emploient des protocoles de chiffrement plus puissants, comme des tailles de clés plus grandes, des algorithmes plus puissants et davantage de types de données chiffrées, avec un impact minimal sur l'expérience utilisateur. En utilisant des algorithmes cryptographiques plus rapides, les utilisateurs peuvent constater des performances accrues, envisager de meilleurs accords de niveau de service et bénéficier d'une réduction des cycles de calcul généralement consacrés au traitement de la cryptographie.

L'accélération cryptographique améliore les performances dans trois domaines clés du calcul cryptographique au niveau de l'algorithme :

Le cryptage par clé publique : notamment pour le SSL (Secure Sockets Layer), le web front-end et une PKI (infrastructure à clé publique).

Le chiffrement en masse : notamment pour la transmission sécurisée de données, le cryptage de disques et le cryptage de flux vidéo.

Le hachage : notamment pour les signatures numériques, l'authentification et la vérification de l'intégrité comme les algorithmes SHA-1 (Secure Hash Algorithm 1) et SHA-2 (Secure Hash Algorithm 2), également connu sous le nom de SHA-256, utilisés par le SSL.

De nombreux logiciels d'entreprises comme Microsoft, SAP et Oracle sont optimisés pour tirer parti de la technologie Intel® Crypto Acceleration. Intel optimise des logiciels libres pour que l'Intel® Crypto Acceleration soit prise en charge (par exemple dans de nombreuses distributions Linux, NGINX, le moteur d'exécution Java OpenJDK, ou la bibliothèque OpenSSL).

La boîte à outils Crypto API comme d'autres outils de développement peuvent exécuter des opérations cryptographiques de manière plus sécurisée dans une enclave Intel® SGX. Par ailleurs, la bibliothèque Intel® IPP (Intel® Integrated Performance Primitives) tire automatiquement parti des capacités disponibles du processeur, tandis que le moteur Intel® QAT pour OpenSSL permet aux solutions logicielles de sécurité réseau d'exploiter Intel® Crypto Acceleration en toute transparence.

En exploitant les technologies d'accélération cryptographique intégrées des processeurs Intel Xeon, vous pouvez réduire les cycles de calcul consacrés au traitement de la cryptographie et améliorer l'expérience utilisateur dans l'entreprise.

Une protection des données de bout en bout pour Thales

Thales et Intel collaborent pour généraliser l'informatique confidentielle et intégrer des capacités de protection des données en cours de traitement à sa plateforme CipherTrust Data Security Platform. Ensemble, Intel et Thales créent un écosystème harmonisé fiable qui offrent des solutions de protection des données de bout en bout pour les environnements dans le Cloud et sur site, attestant de l'authenticité de l'environnement, avant tout déchiffrement de charges de travail client sensibles.

En recourant aux attestations vérifiables que fournit Intel® Trust Authority, les charges de travail de la plateforme CipherTrust Data Security Platform de Thales ne sont pas déchiffrées à l'extérieur d'un environnement TEE Intel® TDX et Intel® SGX. La plateforme CipherTrust Data Security Platform de Thales est conforme à la norme FIPS 140-2 de niveau[3].

Cette technologie est également employée dans de nombreux autres secteurs. Dans le domaine de la santé, par exemple, l'intégration d'ensembles de données pour l'entraînement de modèles d'apprentissage automatique peut faciliter le diagnostic des maladies et l'élaboration de médicaments. Dans le secteur bancaire, les établissements peuvent s'échanger des données sans exposer d'informations personnelles, dans le but de détecter des opérations de blanchiment d'argent ou d'autres irrégularités.

Une confiance flexible et évolutive pour le Cloud et les centres de données

Sur les processeurs Intel® Xeon® Scalable de 5e génération, les moteurs Intel® Security Engines aident les entreprises à tirer parti de la flexibilité et de l'évolutivité de l'informatique du Cloud, tout en réduisant le risque d'exposition des données sensibles. L'informatique confidentielle recourant aux processeurs Intel® Xeon® Scalable isole vos données sensibles des logiciels du fournisseur de services Cloud, des administrateurs et des autres locataires. L'attestation à distance permet au propriétaire des données de vérifier que son enclave est authentique, à jour et qu'elle n'exécute que les logiciels choisis.

Choisissez les processeurs Intel® Xeon® Scalable pour optimiser l'exploitation de vos données

Les processeurs Intel® Xeon® Scalable avec les moteurs intégrés Intel® Security Engines sont disponibles auprès des fournisseurs de services Cloud et des fabricants de systèmes du monde entier. Ils peuvent aider à alimenter de nouveaux services, amplifier la valeur des transactions, se prémunir contre la criminalité financière, écourter les cycles de R&D et optimiser les applications qui manipulent des données sensibles, précieuses ou réglementées.

L'avenir appartient aux détenteurs de données.
Avec les Intel® Security Engines, cet avenir est à votre portée.

Découvrez en quoi les moteurs intégrés Intel® Security Engines peuvent améliorer la performance et renforcer la sécurité de charges de travail indispensables à votre activité.

Informatique confidentielle ›

Intel® Security Engines ›

1. https://www.intel.fr/content/www/fr/fr/architecture-and-technology/software-guard-extensions-enhanced-data-protection.html
2. Voir [S1] sur intel.com/processorclaims : processeurs Intel® Xeon® Scalable de 5e génération. Vos résultats peuvent varier.
3. Confidential Computing: Hardware-Based Trusted Execution for Applications and Data," The Confidential Computing Consortium November 2022, V1.3, https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC_outreach_whitepaper_updated_November_2022.pdf
4. https://www.intel.com/content/www/us/en/developer/articles/technical/offloading-compression-and-encryption-in-ceph.html
5. Voir [N202] sur intel.com/processorclaims : processeurs Intel® Xeon® Scalable de 5e génération. Vos résultats peuvent varier.