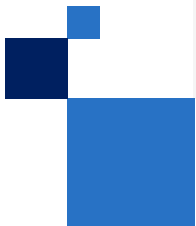


# Package d'habilitation de l'informatique confidentielle pour les intégrateurs de systèmes

Comment les intégrateurs de systèmes peuvent résoudre les difficultés opérationnelles des clients avec des solutions basées sur la technologie Intel



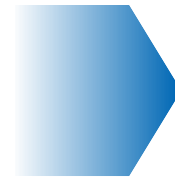


**Qu'est-ce que  
l'informatique confidentielle ?**

# Qu'est-ce que l'informatique confidentielle ?

L'informatique confidentielle permet d'extraire des informations ou de former des modèles d'IA avec des données sensibles sans exposer ces données à d'autres logiciels, à des collaborateurs ou à votre fournisseur de services Cloud  
Cela ouvre aux entreprises de grandes possibilités d'exploiter des données qui étaient auparavant trop sensibles ou réglementées pour être utilisées dans le cadre d'analyses ou à d'autres fins

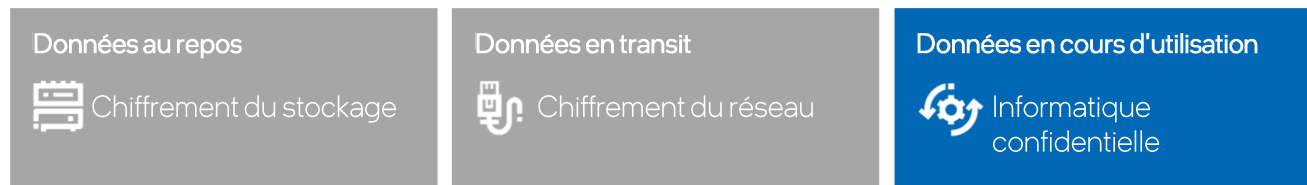
Le segment des logiciels d'informatique confidentielle devrait devenir le segment de marché le plus important et dont la croissance est la plus rapide, suivi des segments du matériel et des services



En quelques années seulement, l'informatique confidentielle a attiré l'attention et a pris de l'élan comme nouveau moyen puissant de protéger de bout en bout le code et les données en cours d'utilisation

## La nécessité de l'informatique confidentielle

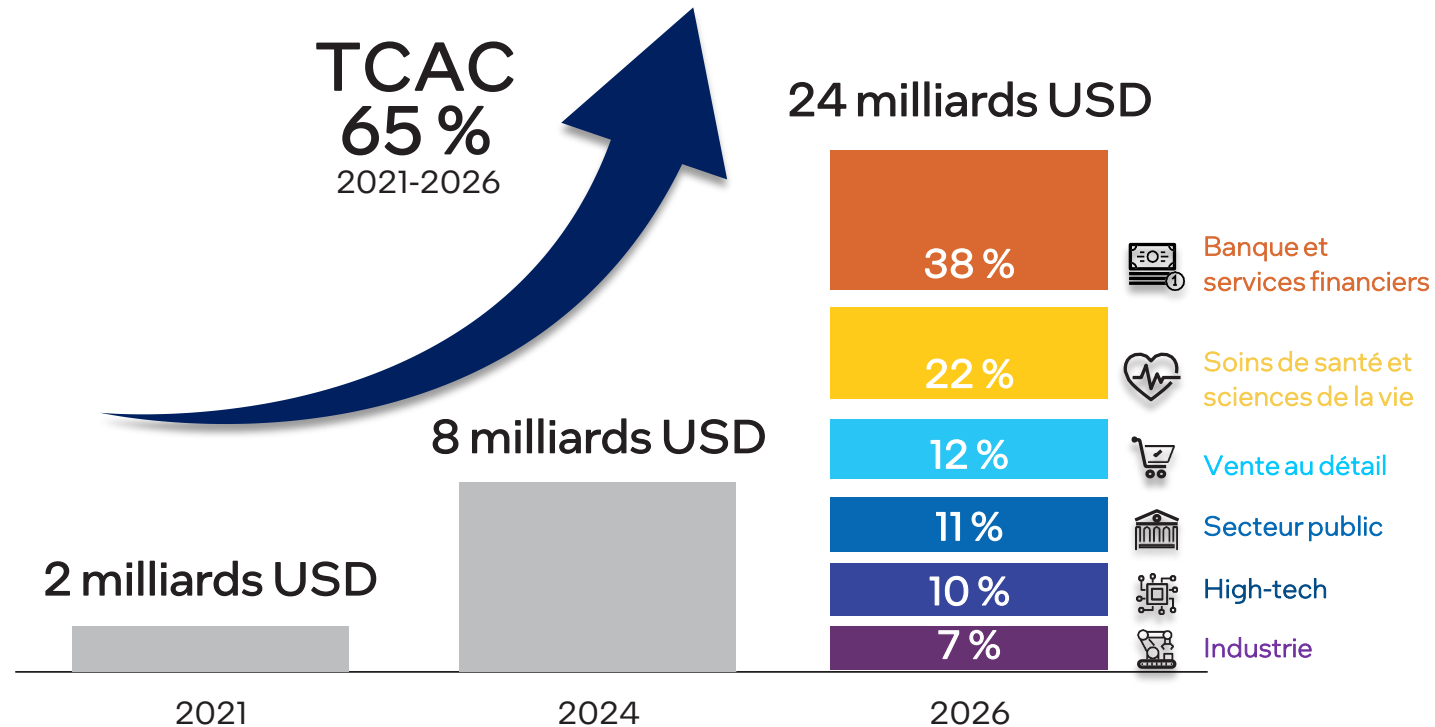
Comble une lacune majeure dans la chaîne de protection des données



 Everest Group®  
D'après Everest Group, cette « nouvelle frontière en matière de sécurité des données... est en passe de connaître une croissance exponentielle. »  
Le marché mondial, qui s'élève à 1,9 milliard de dollars en 2021, devrait connaître un taux de croissance composé annuel de 40 % à 95 % d'ici à 2026, grâce aux projets liés au Cloud et à la sécurité.

# Prévisions sur le marché de l'informatique confidentielle

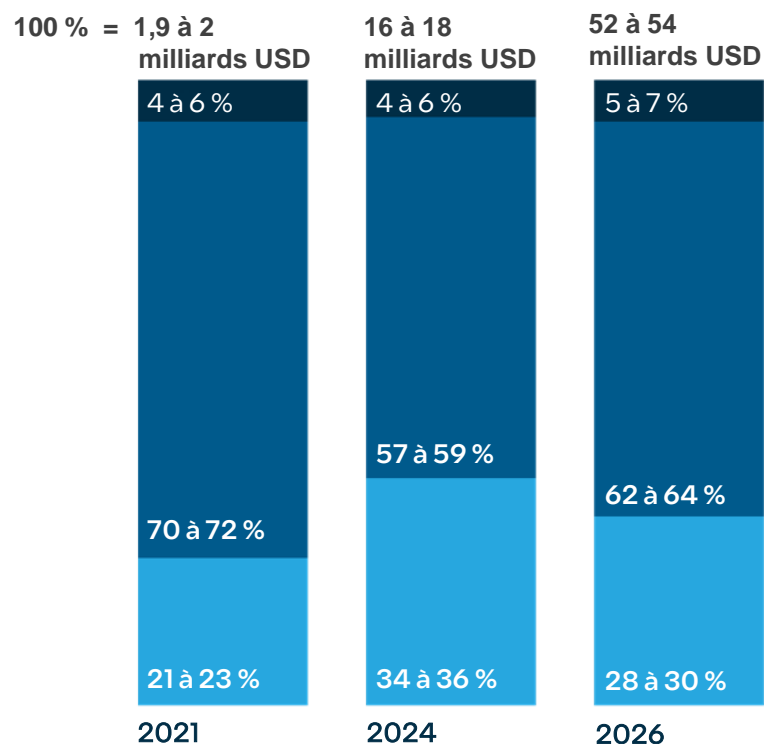
Devrait croître de manière exponentielle, stimulé par la sécurité du Cloud et le traitement multipartite préservant la confidentialité des données



# Marché de l'informatique confidentielle

Le segment des logiciels d'informatique confidentielle devrait devenir le segment de marché le plus important et dont la croissance est la plus rapide, suivi des segments du matériel et des services

Marché total accessible de l'informatique confidentielle,  
par segment technologique  
Pourcentage, AC 2021-26



Matériel Logiciels Service

## SOUS-SEGMENTS DE SERVICES

TCAC = 100-105 %

Intégrateurs de systèmes mondiaux (% de contribution)	Services internes des ISV (% de contribution)
8 à 10 %	90 à 92 %
<ul style="list-style-type: none"> <li>Les services restent limités aux validations de concept précoces avec très peu de solutions ou d'offres de services</li> <li>La majorité de la demande de services sera probablement satisfaite par les services internes des ISV</li> </ul>	

## SOUS-SEGMENTS LOGICIELS

TCAC = 90-95 %

Fournisseurs de services Cloud (% de contribution)	ISV de logiciels d'habilitation (% de contribution)
83 à 85 %	15 à 17 %
<ul style="list-style-type: none"> <li>Le segment des logiciels d'habilitation comprend les technologies utilisées pour adopter et gérer les TEE et les applications basées sur les TEE</li> <li>Alors que le marché arrivera à maturité, la contribution des logiciels d'habilitation devrait s'accroître</li> <li>Suppose une tarification de 1,5 à 2 fois supérieure à l'informatique standard pour les CSP en 2021, avec une normalisation au fil du temps</li> </ul>	

## SOUS-SEGMENTS MATÉRIELS

TCAC = 100-105 %

OEM de chipsets silicium (% de contribution)	OEM de serveurs assemblés (% de contribution)
51 à 53 %	47 à 49 %
<ul style="list-style-type: none"> <li>La différence de tarification limitée ou inexistante du matériel informatique pour l'IC par rapport à la normale continuera de stimuler la demande</li> <li>La contribution du secteur des chipsets devrait dépasser le marché des serveurs assemblés après 2024 en raison de l'adoption accrue des environnements Cloud</li> </ul>	

# Résultats de l'informatique confidentielle

Migrez vers le Cloud et exploitez vos données en sachant que vous gardez le contrôle

Même avec des données confidentielles ou réglementées

RBC Bank / Microsoft Azure

Collaborez avec plusieurs parties sur des analyses partagées bénéfiques

Tout en maintenant la confidentialité et la conformité

Novartis / BeeKeeperAI

Renforcez les programmes de conformité et de souveraineté des données

Avec des protections technologiques

Cloud souverain Deutsche Telekom

Renforcez la sécurité des applications et la protection de la PI

Isolation et contrôle d'accès basés sur le matériel

« Réseaux sociaux et géants de la publicité »

# Informatique confidentielle

## Secteurs & Cas d'utilisation

### Secteurs



### Cas d'utilisation



# Étude de cas de clients

## Santé

Informatique collaborative avec données réglementées



BeeKeeperAI™



NOVARTIS

### Situation

Novartis Biome développe des modèles de diagnostic et des thérapies pour les maladies rares. Les informations sur les maladies rares sont rares et éparpillées dans de nombreux hôpitaux et établissements de recherche

### Difficulté

Les informations des patients sont privées et hautement réglementées. Les hôpitaux ne veulent pas transférer les données hors site ni divulguer les dossiers privés à BeeKeeperAI ou Novartis

### Solution

Un nœud BeeKeeperAI équipé d'Intel® Software Guard Extensions (Intel® SGX) installé sur site dans chaque hôpital examine les données privées et met à jour la pondération du modèle de référence dans le Cloud. Ni Novartis ni le personnel de BeeKeeperAI ne voient ni ne stockent les dossiers médicaux réglementés



BeeKeeperAI™

« [Les plateformes d'informatique confidentielle] nous permettent de réduire de moitié les délais de validation d'un algorithme. Elles réduisent également les coûts presque de moitié. Ces économies nous permettent de former, de valider et de commercialiser beaucoup plus rapidement des algorithmes généralisables. Et, cela ne fera que s'accélérer pour un moindre coût à mesure que la technologie et les processus qui sous-tendent les plateformes d'informatique confidentielle (CCP) arriveront à maturité. »  
MaryBeth Chalk, cofondatrice et directrice commerciale, BeeKeeperAI, Inc



Livre blanc

[Accelerating Development of Clinical AI Algorithms](#)



# Étude de cas de clients

## Protection des clés de haute sécurité



### Situation

La prolifération rapide des clés et des certificats nécessite une protection renforcée et une gestion centralisée. Les solutions HSM sont chères et les solutions Cloud s'appuient sur la sécurité et la conformité des PSC

### Difficulté

Établir un système de gestion des clés évolutif basé sur logiciels, doté d'une sécurité de type HSM isolée technologiquement de son hôte dans le Cloud

### Solution

Fortanix fonde son logiciel KMS d'autodéfense sur Intel® SGX pour protéger les clés et les certificats des adversaires externes et du fournisseur de services Cloud et contribue à assurer que les secrets du propriétaire restent sous son contrôle



Les performances restent élevées lorsque Intel® SGX est activé

La mise en œuvre d'une configuration multi-instance offre des gains de débit importants. Ces améliorations de performances sont affectées de manière minimale par l'activation d'Intel® SGX, ce qui signifie que les entreprises peuvent simultanément accroître la sécurité et les performances.



Aperçu de la solution

[Données confidentielles d'IA Solution de sécurité Intel - Fortanix](#)

# Étude de cas de clients de la RPC

## Extraction de la valeur des données



### Chuanglin Technology

#### Situation

La protection de la sécurité et de la confidentialité des données des entreprises est un problème auquel sont confrontés tous les fabricants de bases de données et de matériel

#### Difficulté

Les technologies de chiffrement de données traditionnelles chiffrent uniquement le stockage sur disque dur et la transmission en réseau, et leur efficacité repose sur l'hypothèse que l'autorité de contrôle du serveur n'a pas été divulguée. Si le contrôle du serveur est intercepté, les données en cours d'utilisation peuvent être volées ou modifiées par un tiers

#### Solution

Chuanglin Technology et Intel ont lancé conjointement une solution de chiffrement de données de base de données graphiques, en utilisant le chiffrement en mémoire Intel® SGX. Cela garantit que Galaxybase bénéficie de performances optimales pour créer une base de données graphique sécurisée en mémoire



Nous pensons qu'à l'aide de la technologie de chiffrement en mémoire Intel® SGX, la base de données graphique de nouvelle génération Galaxybase créée par Chuanglin Technology peut fournir aux clients des services de données de haute qualité et plus sécurisés, effectuer efficacement des interconnexions entre les données et permettre aux entreprises d'extraire de manière stable de la valeur de leurs ressources de données.



[Communiqué de presse](#)

# Activation de zones d'atterrissage souveraines grâce à l'informatique confidentielle





## Informatique confidentielle avec les processeurs Intel® Xeon® Scalable

Le vaste portefeuille de technologies d'informatique confidentielle d'Intel permet aux organisations de choisir le niveau de sécurité dont elles ont besoin pour répondre à leurs besoins opérationnels et aux exigences réglementaires

Intel est la seule entreprise qui offre des solutions d'informatique confidentielle au niveau des applications et des MV

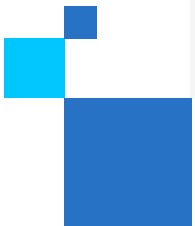


La puissance d'Intel, d'Accenture, de Scone et des fournisseurs de services Cloud permet ce qui suit :

-  Transformations des opérations : conception de solutions adaptées par les centres d'excellence
-  Conformité, intégrité, cohérence, évolutivité et résilience améliorées
-  Instanciations extrêmement sécurisées des zones d'atterrissage, notamment de Scone CAS et des mesures de sécurité
-  Automatisation du pipeline de déploiement pour affecter les charges de travail à leur zone d'atterrissage respective

 [Livre blanc](#)

# Ce qu'offre Intel pour l'informatique confidentielle



# 4 faits : Intel à la base de l'informatique confidentielle



2018

Intel® Software Guard Extensions (Intel® SGX) sur les processeurs Intel® Xeon® est la première solution d'informatique confidentielle introduite dans le centre de données



+ de 300

organisations on fait appel à Intel pour développer et déployer des services d'informatique confidentielle



300M \$

est la valeur estimée de l'infrastructure déployée avec Intel® SGX sur les processeurs Intel® Xeon®



4

fournisseurs de services Cloud mondiaux se sont engagés à offrir Intel® Trust Domain Extensions (Intel® TDX) sur les processeurs Intel® Xeon® de 4<sup>e</sup> génération en 2023



IBM Cloud



Google Cloud



Alibaba Cloud

Regarder la vidéo : [ici](#)

# Intel offre le portefeuille de sécurité le plus complet

Intel® Software Guard  
Extensions (Intel® SGX)



Isolation des applications

Intel® Trust Domain  
Extensions (Intel® TDX)



Isolation des machines  
virtuelles

Intel® Trust Authority



Services de vérification de  
confiance indépendants pour le  
multicloud et le Cloud hybride

Écosystème de solutions logicielles, Cloud, OEM et d'intégrateurs de systèmes

Assistance Intel pour le développement et le cycle de vie axée sur la sécurité

\*Intel® TDX disponible auprès de certains fournisseurs Cloud

# Intel® Trust Authority

Rendez le Zero Trust accessible et bénéficiez de la flexibilité du Cloud public grâce à la sécurité du Cloud privé

Intel® Trust Authority est un nouveau portefeuille de logiciels et de services qui offre davantage de sécurité et de garanties pour l'informatique confidentielle avec des principes de Zero Trust  
La première génération d'Intel® Trust Authority propose un service d'attestation indépendant pour des environnements d'exécution de confiance (TEE) basés sur (Intel® SGX) et (Intel® TDX)

Mettez en œuvre les principes de Zero Trust sans les coûts et la complexité associés à la création de votre propre service d'attestation



Indépendant



Évolutif



Facile à déployer

En savoir plus

[Package d'habilitation de l'informatique confidentielle](#)



[Fiche produit](#)



[Étude de cas Noname](#)



[Étude de cas Thales](#)

**THALES**



[Étude de cas Zscaler](#)



[Vidéo « What That Means »](#)

# Informatique confidentielle

## Écosystème de logiciels et de solutions pour Intel® SGX

Solutions prises en charge au niveau commercial

Développement en interne

### Fournisseurs de solutions commerciales

anJUNA

cosmian

decentriq

EDGELESS  
SYSTEMS

CYBERNETICA

Fortanix®

Mithril Security

Opaque

enclave

SCONTAIN

HUB  
SECURITY

secretarium

### Sélection de conteneurs prêts à être déployés (lors du T1 2023)\*

PyTorch

redis

scikit  
learn

Spark

TensorFlow

### Outils pour développeurs

GRAMINE

SCONE

Mystikos

Occlum  
Empowering everyone to run every app in enclave

Open Enclave SDK

Teaclave

intel  
Intel SGX SDK

### Intégrateurs de systèmes

accenture

KPMG

Capgemini

IBM

Atos

leidos

avanade

### Hyperviseurs (SGX)

KVM  
v. 5.13 et  
ultérieures

vmware®  
vSphere 8

\* Disponibles sur [Azure Marketplace](#)



# Disponibilité d'Intel® TDX

Intel® TDX est disponible sur les instances Intel® Xeon® Scalable de 4<sup>e</sup> génération en présentation publique auprès de trois grands fournisseurs de Cloud

Cliquez sur les logos ci-dessous pour obtenir plus d'informations sur l'offre de chaque fournisseur de Cloud



Intel® TDX est compatible avec les SE invités des fournisseurs suivants



# Comparaison avec la concurrence

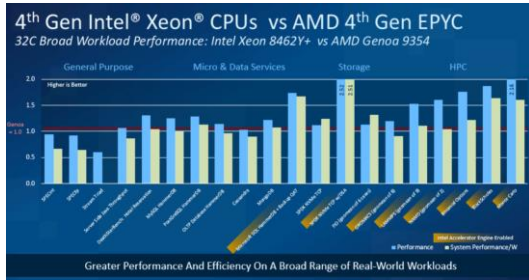
	Intel® SGX	Intel® TDX	AMD SEV-SNP	AWS Nitro Enclaves	Conf. Comp sur le GPU NVIDIA H100
Le matériel et les microprogrammes, l'hyperviseur et la pile de gestion du Cloud des fournisseurs d'infrastructure Cloud sont exclus de la zone de confiance	●	●	●		●
Disponible auprès de plusieurs fournisseurs de services Cloud pour faciliter l'approvisionnement chez différents fournisseurs	●	● <sup>1</sup>	●		●
Conçu pour prendre en charge les applications existantes avec peu ou pas de portage, de reconception ou de repackaging		●	●		● <sup>2</sup>
Attestation d'authenticité du matériel et de lancement correct du TEE	●	●	●	●	●
Attestation d'intégrité de l'image logicielle chargée dans le TEE	●	● <sup>3</sup>	● <sup>3</sup>	●	
Données confidentielles accessibles uniquement avec le code d'application désigné ; les administrateurs de MV, les systèmes d'exploitation invités et les autres applications et piles Cloud sont exclus de l'accès	●				
Déployable sur des serveurs « métal nu » sans virtualisation	●				●
Option d'intégrité de la mémoire cryptographique basée sur le matériel pour une protection supplémentaire contre les attaques Rowhammer	●				
Compatible avec le service de confiance indépendant d'Intel portant le nom de code Project Amber	●	●			
<i>Sources de données sur la concurrence au mois de mars 2023</i>			<a href="#">Lien</a> , <a href="#">lien</a>	<a href="#">Lien</a> , <a href="#">lien</a> , <a href="#">lien</a>	<a href="#">Lien</a>

<sup>1</sup> Les instances Intel® TDX seront mises en ligne chez certains fournisseurs de services Cloud en 2023 ; les délais de disponibilité varient.

<sup>2</sup> Pas ou peu de changements pour le code existant exécuté sur le GPU. Les portions de la charge de travail qui utilisent le processeur devront intégrer un TEE basé sur le processeur et un moyen de protéger les communications PCIe.

<sup>3</sup> Il ne s'agit pas d'une capacité inhérente à la technologie matérielle disponible, mais il est possible de l'incorporer en tant que capacité à valeur ajoutée fournie par le fournisseur de services Cloud ou d'attestations.

# Analyse concurrentielle des processeurs Intel® Xeon® de 4<sup>e</sup> génération



Les processeurs Intel® Xeon® Scalable de 4<sup>e</sup> génération surpassent la concurrence sur les charges de travail réelles



VS



Les processeurs Intel® Xeon® Scalable de 4<sup>e</sup> génération sur logiciel optimisé pour les processeurs fonctionnent jusqu'à 2,5 fois plus vite que les GPU NVIDIA A100



VS



Performances de centre de données de pointe avec les processeurs Intel® Xeon® Scalable de 4<sup>e</sup> génération



VS





**Pourquoi choisir Intel pour  
l'informatique confidentielle ?**

# Pourquoi choisir Intel pour l'informatique confidentielle ?

## Options technologiques qui répondent aux différents besoins de sécurité



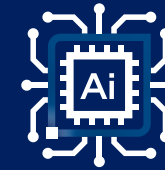
Seule Intel offre à la fois l'isolation des applications (Intel® SGX) et l'isolation des MV (Intel® TDX) afin que les clients puissent ajuster précisément la solution pour différents niveaux de sécurité

## Large écosystème de solutions



Intel collabore avec des dizaines d'ISV et de fournisseurs de services Cloud pour offrir des services d'hébergement et des solutions logicielles, notamment en matière d'IA confidentielle, d'analytique, de blockchain, de bases de données et bien plus encore

## Accès aux experts chez Intel et chez nos partenaires de solutions



Les experts Intel sont prêts à assister les clients en matière d'architecture de solutions, de mise en correspondance des partenaires, de ressources de POC et de dépannage de déploiement

Prenez contact avec votre PSAM pour plus d'informations

# Étapes suivantes

## Formation



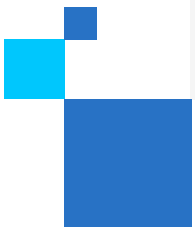
Comprendre la valeur de l'informatique confidentielle et pourquoi il est nécessaire que de nombreuses applications d'utilisateurs finaux en tirent parti pour s'assurer que leur environnement est sécurisé et pour autoriser un traitement multipartite

## Engagement



Prenez contact avec votre Intel PSAM pour mieux comprendre la place du portefeuille technique d'informatique confidentielle Intel dans l'écosystème

**Comment l'Alliance partenaire Intel®  
peut aider**



# Démarrer avec l'Alliance partenaire Intel®

L'adhésion à l'Alliance partenaire Intel® vous offre des opportunités commerciales exclusives, comme l'accès à notre plateforme mondiale, des formations avancées et une assistance promotionnelle, le tout adapté à vos besoins

## Formation et compétences



L'admission à l'Université partenaire Intel® vous offre des formations spécialisées sur les technologies de pointe, des programmes de compétences et des récompenses pour l'apprentissage

## Ressources marketing



L'accès à la Plateforme de solutions Intel et au Studio marketing Intel vous permet de générer une plus grande demande pour vos produits et services

## Récompenses avantageuses



Gagnez des points pour vos activités éligibles, faites progresser votre statut de membre et accédez à des ressources supplémentaires pour développer votre entreprise

**Si vous n'êtes pas déjà membre**  
**Rejoignez-nous dès maintenant**



# Avantages de l'adhésion

## Gagner des points



L'un des avantages les plus populaires et les plus spécifiques à l'Alliance partenaire Intel® est que nous attribuons des points aux partenaires pour récompenser leurs résultats commerciaux avec Intel et leur engagement dans des activités hautement prioritaires.

Il existe plus de 1 000 moyens de gagner des points dans l'Alliance partenaire Intel® et des centaines de possibilités d'échange.

## Communauté Cloud Insider



La communauté Intel® Cloud Insider offre un contenu et des outils de classe mondiale sur le cloud qui sont actualisés en permanence. Les membres ont la possibilité d'entrer en contact avec d'autres membres et avec l'écosystème pour mettre sur le marché des solutions Cloud conjointes et innovantes

[En savoir plus](#)

## Informations sur le secteur



Les membres Gold et Titanium peuvent accéder à des informations trimestrielles spécifiquement organisées pour alimenter leur croissance

[En savoir plus](#)

## Incitations financières



L'adhésion débloque de puissants fonds de développement marketing et des programmes d'incitation pour accélérer le succès de votre marketing de produit

Discutez avec votre PSAM pour en savoir plus sur les initiatives d'accélération de l'Alliance partenaire Intel® et sur les autres incitations financières

## Comment accéder à l'assistance clientèle

### Intel Virtual Assistant

Ce chat bot, situé dans l'angle inférieur droit de chaque page Web de l'Alliance partenaire, fournit des réponses à la plupart des questions ou un lien rapide vers un agent d'assistance en direct.



### Lame « Get Help »

Soumettez une [demande d'assistance en ligne](#).  
Ce lien se trouve en bas de la plupart des pages du site Web de l'Alliance partenaire.

#### Get Help

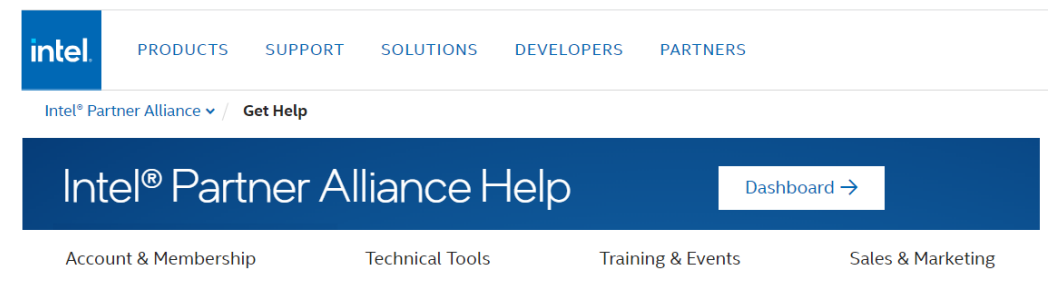
---

##### Request Support

Contact us anytime to create a support request.  
[Submit request >](#)

### Page « Get Help » de l'Alliance partenaire

La page [Get Help](#) fournit une assistance détaillée en libre-service sur la plupart des outils et sur les avantages disponibles aux membres de l'Alliance partenaire.





# Ressources

# Cloud TV

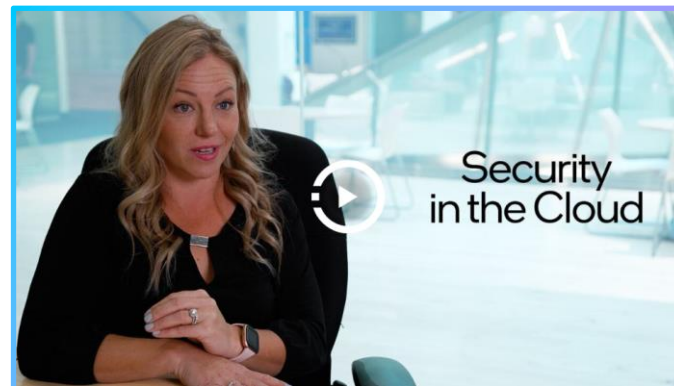
Intel® Cloud TV explore l'actualité, les tendances et les stratégies du cloud computing pour favoriser votre réussite



Sapphire Rapids dans le Cloud



Découvrez comment protéger vos ressources Cloud



Sécurité dans le Cloud



Problèmes de sécurité dans le Cloud

# Informatique confidentielle

## Informations et ressources



### 30-3-30

[Informatique confidentielle 30-3-30](#)



### Vidéos

[Présentation de l'informatique confidentielle](#)

[La sécurité est un défi](#)

Nouveau



### Infographie

[Comment contrer les menaces de sécurité dans le Cloud](#)



### Rapport de recherche

[Protéger les données et les modèles au sein des flux de travail d'IA émergents](#)



### Articles technologiques

[L'état de l'informatique confidentielle](#)

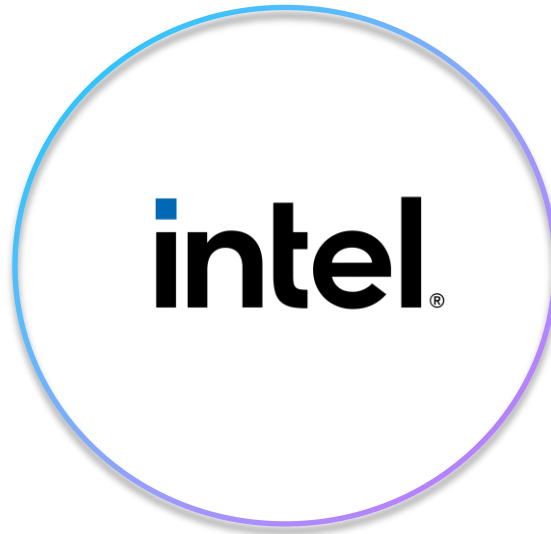
[Introduction à la sécurité du Cloud](#)



### Blogs

[Un nouveau paradigme en matière de performances et de cybersécurité](#)

[La sécurité commence avec Intel](#)



# Autres ressources



## Indice de performances

Processeurs Intel® Xeon® Scalable de 4<sup>e</sup> génération



## Webinaires en direct

Tech Talk Cloud Solution Architect (CSA): réduire le TCO et améliorer l'efficacité avec les processeurs Intel® Xeon® Scalable de 4<sup>e</sup> génération



## Webinaires à la demande

Tech Talk Cloud Solution Architect (CSA): accélérer les charges de travail critiques avec les processeurs Intel® Xeon® Scalable de 4<sup>e</sup> génération



## Formations supplémentaires

Compétences et certifications



# Liens de formation sur l'informatique confidentielle

# Liens de formation sur la sécurité

## Cours / formations

Sujet - Public visé
<a href="#">3 technologies clés pour accroître votre résilience en matière de cybersécurité</a> DevOps, architectes Cloud – Informatique confidentielle
<a href="#">Sécurité de bout en bout pour solutions IOT</a> DevOps
<a href="#">Sécurité Edge to Cloud</a> DevOps, architectes Cloud
<a href="#">Cloud privé virtuel, mise en réseau du Cloud et sécurité du Cloud</a> DevOps
<a href="#">La valeur de la sécurité dans les produits et solutions Intel®</a> Tous
<a href="#">Sécuriser les applications dans le Cloud</a> DevOps
<a href="#">Sécurité et Cloud Computing</a> DevOps, architectes Cloud

Sujet - Public visé
<a href="#">Cloud privé virtuel, mise en réseau du Cloud et sécurité du Cloud</a> DevOps, architectes Cloud
<a href="#">Conversation sur la sécurité dans les entreprises</a> Architectes Cloud, C-Suite
<a href="#">Une introduction au chiffrement pour l'architecture Intel</a> DevOps
<a href="#">La valeur de la sécurité dans les produits et solutions Intel®</a> DevOps, architectes Cloud



intel®

# Sauvegarde



# Informatique confidentielle

## Cas d'utilisation clés de l'IA

### Machine Learning multipartite

Tirez parti de la puissance du Machine Learning sans compromettre la confidentialité des données sensibles des clients

 [Fiche stratégie](#)

Le Machine Learning multipartite avec informatique confidentielle peut s'avérer particulièrement utile pour ces domaines :



#### La santé

peut tirer parti de la puissance des données pour faire avancer la recherche sans exposer les informations confidentielles des patients



#### Les services financiers

peuvent prévoir plus précisément les activités potentiellement frauduleuses tout en combattant le blanchiment d'argent et le financement du terrorisme

# Engagement d'Intel en matière de sécurité

« La sécurité de nos produits fait partie de nos plus grandes priorités. Nous nous efforçons de concevoir, de fabriquer et de vendre les produits technologiques les plus sécurisés au monde, et nous innovons et améliorons continuellement les capacités de sécurité de notre produit. »

Pat Gelsinger, PDG



**93 %**

des vulnérabilités traitées en 2022 résultaient directement des investissements effectués par Intel dans l'assurance de sécurité de ses produits

**56 %**

des 243 CVE publiées en 2022 ont été découvertes en interne par des employés d'Intel

**93 %**

Depuis le premier rapport sur la sécurité des produits pour l'année civile 2019, 93 % en moyenne de toutes les CVE publiées ont été le résultat direct d'investissements d'Intel dans l'assurance de sécurité de ses produits

**85 %**

Parmi les 106 vulnérabilités signalées par des chercheurs externes en 2022, 90 vulnérabilités, soit 85 %, ont été signalées dans le cadre du Bug Bounty program d'Intel

Consultez le rapport complet : [ici](#)

# Analyse concurrentielle des processeurs Intel® Xeon® Scalable de 4<sup>e</sup> génération

## Leadership en informatique grand public

75 %

Performances  
supérieures

50 %

Performances/watt  
supérieures

20 %

Moins d'émissions de Co2 et  
économies sur le TCO global

## Leadership dans l'IA

80 %

Débit d'inférence  
supérieur

## Leadership dans le HPC

40 %

Performances  
supérieures sur toutes les  
charges de travail

[Cliquez pour obtenir des faits sur le Cloud](#)