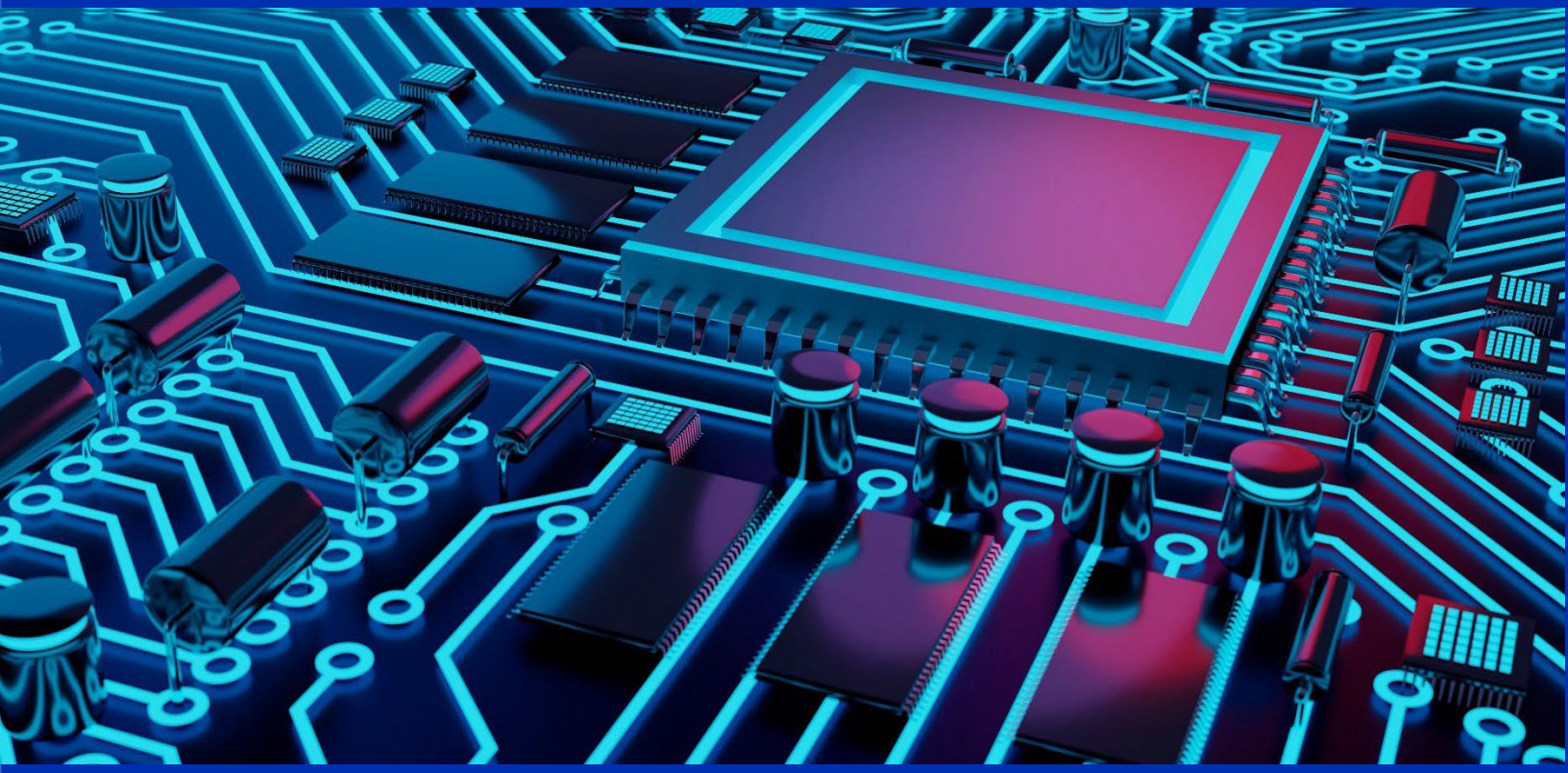
DELL Technologies intel

# Bénéficier d'une sécurité omniprésente sur les couches supérieures et inférieures du système d'exploitation

**Les AI PC professionnels les plus sécurisés au monde*, fournis par Dell et Intel®. Assurez la pérennité de votre parc et restez en avance sur les cybercriminels grâce à plusieurs couches de défense.**

Juillet 2025



## Synthèse

- Assurer la sécurité des données d'entreprise est une tâche difficile. Cette mission est d'autant plus complexe que les vecteurs de menaces évoluent en permanence et que les points de terminaison situés en dehors du réseau de l'organisation prolifèrent.
- L'IA est arrivée sur les appareils, développant ainsi l'innovation et la surface d'attaque. Avec des centaines de modèles et de fonctionnalités d'IA actuellement disponibles, les données sensibles risquent désormais d'être exposées à des applications telles que l'IA générative.
- Dell et Intel se sont engagés à assurer la sécurité des réseaux de leurs clients commerciaux grâce à plusieurs couches de défense.
- Dell combine une sécurité intégrée au matériel et au firmware avec des protections Intel actives au niveau de la puce pour défendre les niveaux les plus profonds d'un appareil contre les attaques fondamentales.
- Nous renforçons ces défenses « sous le système d'exploitation » avec des logiciels intelligents issus de notre écosystème de partenaires pour une protection avancée contre les menaces.
- En plus de cette approche, Dell et Intel ont investi dans des pratiques et des politiques visant à sécuriser continuellement les plates-formes une fois qu'elles sont sur le marché et susceptibles de subir des attaques de la part d'acteurs malveillants.

## Sujets traités dans ce document

### Socle de sécurité

**Cycle de vie du développement sécurisé** Dell et Intel placent la sécurité au cœur de la conception de leurs produits et la testent rigoureusement avant la commercialisation.

**Sécurité de la chaîne logistique** Des protections sont en place tout au long de la chaîne logistique pour garantir la sécurité des appareils une fois qu'ils ont quitté l'usine.

### Cadre de défense complet

**Sécurité intégrée :** des contrôles rigoureux de la chaîne logistique et une assurance facultative garantissent la sécurité des clients dès le premier démarrage.

**Sécurité intégrée :**

- Les fonctionnalités de sécurité basées sur le matériel et les firmwares aident à protéger les appareils contre les menaces qui ciblent leurs couches de base, par exemple, le BIOS.
- Les protections intégrées au niveau de la puce fournissent une couche fondamentale qui sous-tend la fiabilité et la confiance de l'AI PC.

**Sécurité intégrée :** la sécurité logicielle offre une protection avancée pour les points de terminaison, les réseaux et les environnements Cloud, ce qui est essentiel à la sécurité des appareils modernes.

**Support continu :** Dell et Intel s'assurent que leurs produits restent sécurisés, corrigent les failles de sécurité et mettent à jour les protections en silicium dans le système d'exploitation.

## Principales tendances en matière de sécurité

1. Dans le rapport Perspectives du marché de la sécurité des points de terminaison, de Forrester Research, Inc. daté de mars 2025, la société explique que « les points de terminaison sont parmi les principales cibles des attaques externes pour les entreprises qui ont subi une violation au cours des 12 derniers mois. »

2. Selon le Rapport sur les menaces mondiales CrowdStrike 2025 , les attaques sans fichier de logiciels malveillants représentent désormais 79 % des attaques, ce qui signifie que les atteintes sur la mémoire sont plus difficiles à détecter.

3. Selon un rapport de recherche d'Enterprise Strategy Group publié en mai 2023 , plus de 75 % des organisations déclarent avoir subi au moins une cyberattaque causée par un périphérique de terminaison inconnu, non géré ou mal géré.

# Introduction

## Le niveau de sécurité de votre réseau correspond à celui de son point de terminaison le plus faible

**La sécurité commence beaucoup plus tôt que vous ne pourriez le penser.** Pas un mois ne se passe sans qu'une nouvelle grande marque mondiale soit victime d'une faille de sécurité majeure. Or cet écho négatif porte véritablement atteinte à la réputation des marques. Les entreprises et les professionnels de la sécurité appréhendent qu'une faille de sécurité non détectée sur l'un de leurs appareils ou qu'une vulnérabilité logicielle inconnue et exploitable les exposent à leur tour aux attaques. Vous faites peut-être confiance à votre équipe IT pour sécuriser vos réseaux et mettre en œuvre des pratiques de sécurité des données, mais comment faire confiance à tous les points de terminaison et applications sur lesquels vous vous appuyez pour travailler, alors que vous n'avez aucun contrôle sur leur fabrication ou leur développement ?

**La sécurisation logicielle ne suffit pas.** Une approche courante, mais erronée, pour répondre à la question de l'intégrité des appareils, consiste à créer un faux sentiment de sécurité via des solutions logicielles uniquement, sans traiter les failles de sécurité matérielles sous-jacentes. Il est important que les dirigeants d'entreprise comprennent les limites de cette stratégie : en s'appuyant uniquement sur des logiciels pour protéger leurs activités, ils ne protègent pas le matériel sur lequel les logiciels sont installés contre les attaques potentielles. En résumé, si le matériel n'est pas sécurisé, les applications et les technologies de sécurité qui s'y exécutent ne le sont pas non plus.

D'autres fournisseurs tentent de créer un « jardin clos » pour protéger les appareils, avec des règles intégrées aux applications et aux services pour limiter la flexibilité des utilisateurs. Bien que cette stratégie puisse faire sens pour des particuliers, elle bride l'utilisation des appareils, ce qui devient problématique dans un contexte professionnel. Cette approche peut également inciter les auteurs des attaques à viser et à décomposer ces systèmes davantage, afin d'exposer les failles de sécurité dans les configurations courantes.

En d'autres termes, ce qui fonctionne pour les appareils vendus aux particuliers ne fonctionne généralement pas dans un environnement professionnel qui représente une cible plus attractive pour les pirates. C'est pourquoi Dell et Intel adoptent une approche différente et globale de la sécurité. Dell et Intel savent que le seul moyen de sécuriser de manière fiable les appareils et les réseaux professionnels consiste à harmoniser les technologies de sécurité matérielle et logicielle qui fonctionnent ensemble. Nos équipes ont collaboré pour créer une chaîne de fonctionnalités de sécurité matérielle et logicielle étroitement intégrées, mais d'autres fournisseurs n'ont peut-être pas encore fait cet investissement.

## Sécurité matérielle pour les AI PC professionnels

**Chaque PC sera un AI PC.** L'analyste du marché technologique Canalys prédit que les AI PC prendront le dessus sur l'ensemble du marché des PC au cours des six prochaines années. En d'autres termes, les PC ne disposant pas de fonctionnalités d'IA intégrées ne seront plus vendus d'ici 2030. Pour pérenniser votre entreprise, vous devez commencer dès maintenant. Bonne nouvelle : Dell et Intel guident leurs clients dans le paysage IT et l'environnement de la sécurité en constante évolution avec des AI PC professionnels dotés de la sécurité, de la rapidité et de l'efficacité intégrées nécessaires pour lutter contre les menaces modernes.

Mais la tâche n'est pas simple. Les niveaux de complexité et les préoccupations liées à la sécurisation des appareils et des réseaux sont vertigineux. Et les technologies émergentes de l'IA ont rendu ce domaine encore plus complexe. C'est pourquoi nous nous sommes donné pour mission de fournir des appareils avec la sécurité intégrée dès la conception. Ainsi nos clients peuvent se concentrer sur ce qui compte vraiment : faire fonctionner leur entreprise. La relation de co-ingénierie que Dell et Intel entretiennent depuis des décennies se concentre depuis toujours sur la protection des données des clients, en particulier des clients professionnels. Grâce à son partenariat avec Intel, Dell s'est imposé comme le fournisseur incontournable des entreprises de toutes tailles, sur tous les marchés. Qu'est-ce qu'un appareil professionnel Dell basé sur l'IA ? Loin des ensembles de fonctionnalités obsolètes, Intel et Dell intègrent des technologies, des outils et des politiques tout au long du cycle de vie des PC professionnels, afin de fournir une sécurité de bout en bout à leurs clients et leurs entreprises.

### Sécurité intégrée dès la conception

Lorsqu'ils conçoivent les systèmes de demain, Intel et Dell gardent un temps d'avance sur les menaces actuelles, afin de minimiser la surface d'attaque et de garantir la sécurité des appareils professionnels.

### Protection en transit

Nous avons mis en place des technologies et des politiques pour protéger l'intégrité des appareils avant qu'ils ne vous soient livrés, afin de garantir leur sécurité tout au long des phases d'approvisionnement en composants, d'assemblage et de livraison.

### Défense contre des menaces en constante évolution

Nous utilisons la sécurité matérielle par le biais des fonctionnalités de Dell Trusted Devices et Intel vPro® Security pour renforcer les appareils qui traitent les principaux cas d'utilisation de la cybersécurité pour la prévention, la détection, la réponse, la récupération et les mesures correctives. En outre, Dell et Intel disposent d'équipes de sécurité dédiées pour tester leurs produits et rechercher de nouvelles failles de sécurité avant que des pirates ne les trouvent, et pour émettre rapidement des correctifs afin de vous aider à protéger votre équipe et votre entreprise.

Dans ce livre blanc, nous découvrirons comment Dell et Intel ont collaboré pour produire des plates-formes d'AI PC professionnelles avec une sécurité intégrée aux niveaux les plus profonds, afin de protéger les appareils tout au long de leur cycle de vie, notamment grâce à des actualisations régulières.

## Cybersécurité et IA générative : une arme à double tranchant

Tout comme les cyberdéfenseurs utilisent l'IA générative pour faire le bien autour d'eux, les cybercriminels cherchent à poursuivre leurs propres objectifs malveillants, en lançant des attaques plus sophistiquées, plus rapidement et à grande échelle.

Bien que les cas d'utilisation de l'IA générative soient encore à leurs débuts et en constante évolution, il est important de garder à l'esprit quelques concepts clés. Tout d'abord, l'IA générative peut représenter un certain nombre de menaces pour les organisations notamment :

- Des problèmes de confidentialité et d'intégrité des données
- Des problèmes de conformité
- Et une violation de la propriété intellectuelle

De plus, nous observons plusieurs façons dont l'IA générative pourra contribuer à la lutte contre la sécurité, notamment :

- Détection des menaces avancées
- Formation spécialisée et ciblée des employés, et
- Automatisation

Dell et Intel travaillent activement pour permettre une meilleure modélisation des menaces spécifiques à l'IA générative. Cela peut inclure la prévention de la perte de données, la gestion des droits des données, le phishing avancé, la falsification de modèles, la réglementation et la conformité ; le tout avec une application des contrôles appropriés.

Dell peut également vous aider à tester votre environnement d'IA générative en matière de sécurité grâce à des programmes de gestion des failles de sécurité et de tests d'intrusion pour suivre l'évolution des différentes menaces.

## Socle de sécurité

**Cycle de vie de développement sécurisé**

### La sécurisation de nos plates-formes commence avec le tableau blanc

**Planification, évaluation et analyse**

Avant de concevoir nos tout derniers chipsets et plates-formes, les experts Dell et Intel ont défini des paramètres stricts répertoriant ce qu'une plate-forme sécurisée doit inclure pour répondre aux futurs besoins de sécurité et aux réglementations applicables en la matière. Ce processus a commencé par une table ronde pour déterminer les futurs risques probables en matière de sécurité et de confidentialité, ainsi que les activités à mettre en œuvre pour y remédier. Cette évaluation permet de définir les objectifs de sécurité qui serviront à évaluer nos architectures. Avec ces informations, les équipes de sécurité de Dell et Intel développent des modèles de menaces en adoptant une approche de l'architecture conceptuelle partant du point de vue de l'adversaire, et en recherchant les failles de sécurité et les exploits potentiels qui devront être traités. Cette méthode a permis d'apporter des améliorations significatives dans la détection et l'atténuation des failles de sécurité potentielles lors de la conception du BIOS, du firmware et du matériel.

**Conception axée sur la sécurité**

Une fois l'évaluation des menaces terminée et les modèles créés pour définir la surface de menace et la cible des tests, les ingénieurs commencent à développer le code produit. Les objectifs de sécurité définis à l'étape précédente permettent de guider les ingénieurs dans cette phase de développement et servent de critères afin de déterminer si le produit est sur la bonne voie pour répondre aux besoins de nos clients.

**Vérification et tests**

Une fois le code affiné pour répondre aux objectifs de sécurité définis au début du cycle de développement, le produit passe par un processus de tests rigoureux. Ces tests commencent généralement par des révisions de code sécurisées et une analyse statique du code, un processus automatisé qui utilise des outils spéciaux pour rechercher et corriger les défauts. Certains produits présentant un code plus complexe nécessitent un processus de révision manuel, durant lequel les experts en sécurité vérifient le code ligne par ligne pour détecter des erreurs passées inaperçues et s'assurer que le code a été conçu de façon sécurisée. Enfin, des équipes de pirates informatiques chevronnés sont chargées d'effectuer des tests de pénétration et d'autres exercices « d'équipe rouge » pour détecter les failles de sécurité potentielles qui sont passées inaperçues au cours des phases précédentes. Ces failles de sécurité sont à nouveau atténuées en fonction du risque, de sorte que toute exposition supplémentaire identifiée est documentée et corrigée.

**Commercialisation et post-commercialisation**

Une fois que le produit a été rigoureusement testé et que les objectifs de sécurité initialement définis ont été atteints ou dépassés, la phase de commercialisation peut être lancée. Toutefois, ces étapes ne représentent qu'une partie du cycle de vie du développement sécurisé. Pour Dell et Intel, la sécurité des plateformes représente un effort continu. Nos équipes travaillent à la détection des failles de sécurité avant qu'elles ne puissent être exploitées par les pirates, puis développent et transmettent des mises à jour de sécurité pour les corriger. L'engagement de Dell et Intel en matière de sécurité de bout en bout se reflète dans notre investissement dans la chaîne logistique, sécurisée de l'assemblage à la livraison des appareils, un des vecteurs d'attaque à la croissance la plus rapide. Dans la section suivante, nous découvrirons comment Dell et Intel atténuent les risques tout au long de leur chaîne logistique afin de garantir que l'appareil livré à votre domicile est sécurisé dès le premier démarrage.

**Sécurisation de la chaîne logistique**

### La sécurité de la chaîne logistique est essentielle pour la sécurité des appareils

Bien des choses peuvent arriver entre le moment où un composant ou un appareil quitte l'usine et le moment où il arrive à destination. Chaque étape de la chaîne logistique représente un nouveau vecteur d'attaque potentielle, qui expose vos collaborateurs, votre entreprise et vos clients. Dell et Intel ont développé des outils, des technologies et des processus pour garantir la sécurité de nos produits avant leur arrivée dans les entreprises des clients, et pour permettre l'autovérification de l'authenticité des appareils avant leur distribution aux collaborateurs.

**Source**
Dell utilise un processus rigoureux de filtrage des partenaires pour garantir la qualité et la sécurité des appareils et de leurs composants. Ces partenaires sont également régulièrement soumis à des audits afin de garantir la conformité avec l'ensemble des normes de sécurité de la chaîne logistique de Dell.

**Fabrication**
Outre le respect des normes de sécurité de la chaîne logistique de Dell, les fabricants d'appareils Dell testent fréquemment les pièces lors de leur fabrication, afin de s'assurer qu'aucun produit de contrefaçon ne se glisse dans la chaîne logistique. Pour limiter ce risque, les étiquettes PPID (Unique Piece Part Identification Number) sont apposées sur certains composants à haut risque, et comprennent des informations sur le fournisseur, le numéro de référence, le pays d'origine et la date de fabrication, afin que Dell puisse identifier, authentifier, suivre et valider ces composants, pour garantir que le client reçoit exactement ce qui a été expédié.

**Livraison**
Le transport Dell est protégé par des couches de sécurité physique, des sceaux inviolables jusqu'aux mécanismes de verrouillage des portes, en passant par divers systèmes de suivi des appareils, qui détectent si les appareils Dell transportés ont été altérés durant le transit.

Les appareils Dell sont également dotés de technologies de détection des altérations. Les solutions Dell SafeSupply Chain couvrent les contrôles de sécurité et d'intégrité de la chaîne logistique, tels que les sceaux inviolables et les nettoyages de disque dur selon la norme NIST, afin de garantir une base propre pour votre image d'entreprise.

**Vérifier**
Les appareils professionnels Dell basés sur l'IA sont livrés avec des certificats de plate-forme signés sous forme chiffrée, qui capturent les attributs de snapshot des plates-formes lors de la fabrication, de l'assemblage, des tests et de l'intégration. Ces attributs de plate-forme sont ensuite liés, sous forme chiffrée également, à l'appareil concerné à l'aide du module TPM (Trusted Platform Module) en tant que racine de confiance matérielle.

En savoir plus sur les efforts conjoints de Dell et Intel pour sécuriser la chaîne logistique. Visionnez l'entretien ***avec SiliconANGLE***

Dell a mis en œuvre des certificats de plate-forme Trusted Computing Group (TCG) dans la solution Dell Secured Component Verification (SCV) pour les AI PC professionnels équipés de processeurs Intel (certificat disponible à la fois sur les appareils pour les organisations fédérales et sur le Cloud pour les clients professionnels). SCV fournit des certificats d'inventaire signés sous forme chiffrée au département IT pour les appareils Dell pris en charge. Grâce à des outils d'autovérification sécurisés, la solution SCV* exclusivement proposée par Dell garantit l'intégrité complète du matériel lors du transit vers les environnements IT, et permet aux clients de vérifier que les AI PC professionnels et les composants clés Dell livrés sont conformes à ce qui a été fabriqué et commandé.

## Cadre de défense complet

**Sécurité sous le système d'exploitation**

### Les technologies de sécurité intégrées aident à prévenir, détecter et agir contre les menaces et à reprendre le dessus sur elles

La sécurité globale implique d'aller au-delà du modèle existant de logiciels de protection logicielle pour faire face aux nouvelles catégories de menaces contre la sécurité, la sûreté et la confidentialité numériques. En l'associant à une technologie de sécurité matérielle « sous le système d'exploitation », vous protégez chaque couche de la pile informatique, et prévenez et détectez les attaques de base, y compris les variantes de menaces qui concernent le plus souvent la chaîne logistique. La relation de co-ingénierie entre Dell et Intel s'est concentrée sur la couverture de cette surface d'attaque via un ensemble complexe de technologies au niveau des composants et de la plate-forme.

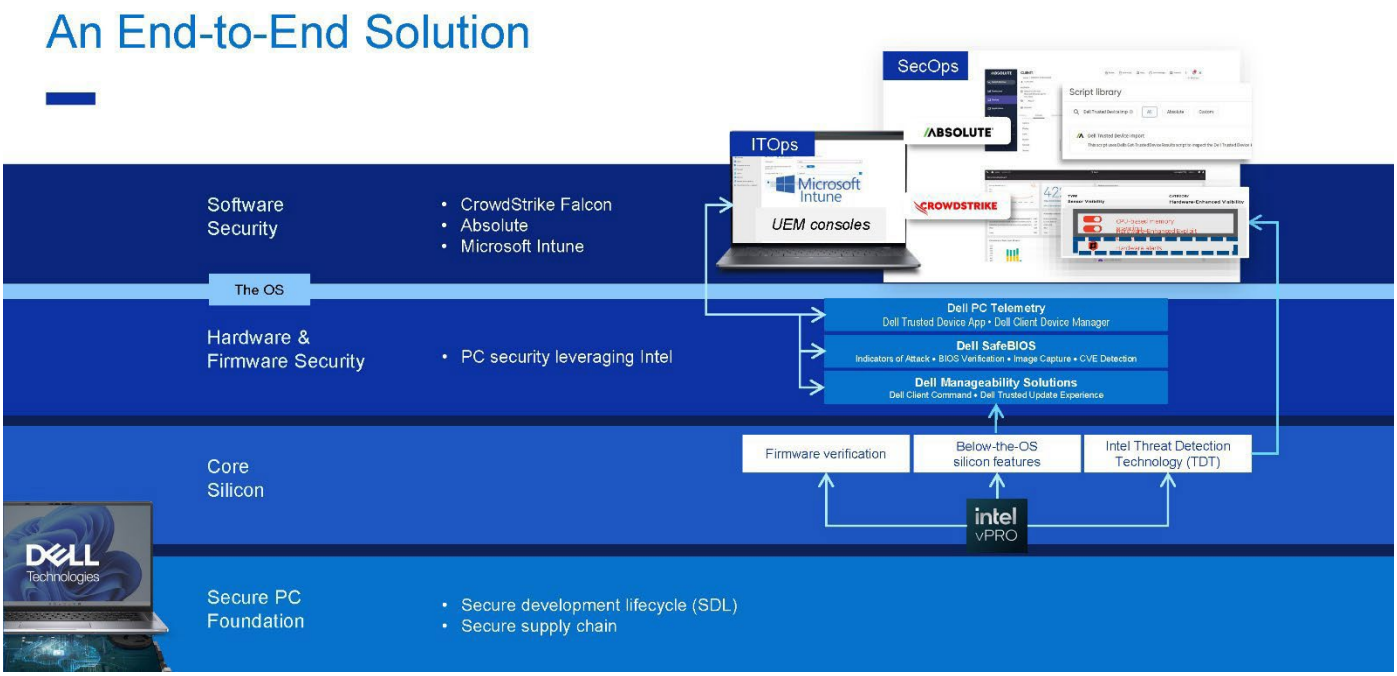



Figure 1 : aujourd'hui, une sécurité efficace nécessite plusieurs couches de contre-mesures. Dell et Intel collaborent avec des partenaires logiciels pour fournir une défense en profondeur.

Nous avons abordé la chaîne logistique et la base sécurisée des AI PC proposés par Dell et Intel. Examinons à présent les couches intermédiaires.

### Intel vPro® Security

Intel vPro Security est inclus avec chaque appareil professionnel Dell s'exécutant sur la plate-forme Intel vPro® et offre des fonctions de sécurité optimisées par le matériel qui aident à protéger toutes les couches de la pile informatique. Cet ensemble de technologies de sécurité permet de se défendre contre les menaces modernes à chaque couche : matériel, BIOS/firmware, hyperviseur, machines virtuelles, système d'exploitation et applications.

### Sécurité Dell intégrée du matériel et du firmware

La protection du BIOS (Basic Input Output System) est cruciale pour la sécurité des appareils. Étant donné que le BIOS occupe une position unique et privilégiée au sein de l'architecture de l'appareil, un pirate qui parviendrait à s'introduire dans le BIOS pourrait prendre le contrôle total de l'appareil. Pour protéger cette couche critique, les appareils IA professionnels Dell sont livrés avec SafeBIOS, une suite de sécurité multicouche au niveau du firmware. Les fonctionnalités sous-jacentes qui constituent SafeBIOS améliorent la protection, la détection et la récupération au niveau du BIOS.


Figure 2 : selon Principled Technologies, Dell et Intel proposent les AI PC professionnels les plus sécurisés au monde*

Il est également important de noter qu'une sécurité efficace inclut une visibilité sur la posture de sécurité actuelle. Dell rend ces événements SafeBIOS se produisant sous le système d'exploitation visibles au niveau du système d'exploitation pour que les administrateurs et les utilisateurs finaux puissent les consulter et prendre des décisions avec l'application Dell Trusted Device (application DTD).
L'application DTD détecte si le BIOS a été compromis en comparant les mesures de l'image du BIOS en cours d'exécution à celle de la copie de référence sécurisée dans l'environnement Dell, ce qui permet de fournir une vérification du BIOS hors hôte sans précédent sur le marché. En outre, la vérification du firmware Intel Management Engine (ME), disponible exclusivement sur les PC professionnels Dell, protège contre les accès non autorisés et la falsification du firmware hautement privilégié.

Cette télémétrie PC unique à Dell (disponible via le Dell Client Device Manager (DCDM) pour les environnements IT gérés ou la console d'applications DTD pour les environnements non gérés) est le paramètre secret de l'équation de sécurité. Cette télémétrie permet l'intégration avec des consoles tierces, telles que CrowdStrike et Absolute pour la sécurité et Microsoft Intune pour la gestion (voir Figure 1). En fait, Dell est le seul fabricant de PC à fournir une intégration et une visibilité de la détection des menaces au niveau du firmware via des consoles de sécurité tierces*

Dell limite également le risque croissant de compromission des identités et d'accès non autorisé aux charges applicatives sensibles. Certains appareils professionnels Dell incluent également Dell SafeID avec ControlVault 3+, une puce de sécurité unique certifiée FIPS 140-3 de niveau 3* qui stocke les informations d'identification des utilisateurs finaux, les isole du système d'exploitation et les rend beaucoup moins vulnérables aux attaques.

### La sécurité sous le système d'exploitation n'est qu'une partie de l'approche globale adoptée par Dell pour sécuriser les appareils

Pour sécuriser davantage les appareils professionnels Dell basés sur l'IA, Dell et Intel ont également investi massivement dans la sélection et la mise en place d'un écosystème de solutions de sécurité logicielle leaders sur le marché. Ces fonctionnalités fournissent une protection contre les menaces avancées des pirates sophistiqués, en offrant une couche de sécurité supplémentaire au niveau des données et des applications.

Encore une fois, Dell et Intel peuvent enrichir les technologies logicielles avec des télémétries informatiques en dessous du système d'exploitation pour améliorer la détection et la réponse aux menaces.

**Sécurité au-dessus du système d'exploitation**

## La sécurité logicielle intégrée offre une protection avancée contre les menaces

Étant donné les gains potentiels liés à une seule violation réussie, les cybercriminels sont très motivés : ils effectuent souvent des dizaines de tentatives sur un seul appareil au cours de sa durée de vie. Cette situation, qui s'applique à l'ensemble du parc informatique d'une entreprise, suscite de sérieuses préoccupations. Pouvez-vous permettre à une attaque de réussir ? À ce stade, une chose est certaine : aucune solution ne peut bloquer la totalité des attaques, aussi bien aux points de terminaison de votre parc que sur les réseaux et environnements Cloud dans lesquels ils opèrent.
Les solutions logicielles intelligentes peuvent vous aider à prévenir les menaces, à les détecter, à y répondre et à reprendre le dessus sur elles, où qu'elles se produisent. À cette fin, la gamme de solutions de sécurité des points de terminaison Dell Trusted Workspace inclut des logiciels leaders sur le marché pour simplifier les achats et fournir aux dirigeants d'entreprise tout ce dont ils ont besoin pour défendre leurs points de terminaison. Les fonctionnalités comprennent les suivantes :

- Prévention, détection, réponse et mesures correctives sur les points de terminaison, le réseau et les environnements Cloud, en tirant parti de l'IA et de l'apprentissage automatique
- Géolocalisation des points de terminaison, geofencing, effacement des données à distance et autoréparation pour les applications stratégiques, sur ou hors réseau
- Les solutions de sécurité Edge de Secure Service pour une approche centrée sur les données de la sécurité et de l'accès au Cloud, protégeant les données et les utilisateurs partout

Les fonctionnalités de sécurité Intel, intégrées en profondeur au niveau de la puce, telles que la technologie Intel Control-flow Enforcement, protègent contre les attaques ciblant le système d'exploitation, tandis que d'autres fonctionnalités dans Intel vPro® Security protègent les couches sous le système d'exploitation, sécurisent les applications et les données, et fournissent des protections avancées contre les menaces.

**Sécurité assistée par matériel**

## Sécurité intégrée

Les pirates ciblent de plus en plus l'ensemble de l'infrastructure informatique de l'entreprise, qui manquait traditionnellement de visibilité et de contrôle. Ces menaces en constante évolution contournent les outils de sécurité logiciels existants de détection et de réponse des points de terminaison (EDR), c'est pourquoi la sécurité des PC est si essentielle. Pour rester en avance sur les menaces modernes et en constante évolution, une collaboration approfondie de l'écosystème est nécessaire pour connecter de manière adéquate les protections de surface d'attaque entre fournisseurs dans une solution cohérente.

Ce travail d'intégration back-end est toutefois complexe et nécessite beaucoup de temps et de ressources. Pour résoudre ce problème, Dell et Intel ont tiré parti de notre connaissance approfondie des problématiques des concurrents et des clients pour travailler avec nos partenaires afin de développer une solution matérielle et logicielle intégrée appelée « sécurité assistée par matériel ». Dell propose non seulement des AI PC sécurisés et s'associe avec les principaux fournisseurs de logiciels, mais notre télémétrie unique des appareils* enrichit tout l'écosystème de sécurité, offrant ainsi une meilleure visibilité au niveau du BIOS à votre parc. Cette fonctionnalité d'intégration est essentielle pour combler le fossé de sécurité IT auquel de nombreuses organisations sont confrontées aujourd'hui. Avec Dell, Intel et notre écosystème de partenaires, le matériel et les logiciels communiquent entre eux, ce qui améliore la sécurité et la facilité de gestion à l'échelle du parc.


Figure 3 : les cybermenaces en constante évolution déjouent les défenses exclusivement logicielles. Réduisez la surface d'attaque des points de terminaison grâce à des protections assistées par matériel.

**Focus sur la sécurité assistée par matériel avec Dell, Intel et CrowdStrike**

Conjointement, Dell, Intel et CrowdStrike ont mis au point des fonctionnalités de détection et de réponse aux menaces qui associent la puissance de Dell Trusted Devices, les AI PC professionnels les plus sécurisés au monde*, aux fonctionnalités d'Intel intégrées au niveau de la puce et au Gartner Magic Quadrant 2024 de CrowdStrike. En travaillant ensemble, CrowdStrike, Dell et Intel ont développé une solution de sécurité multicouche qui va au-delà des protections logicielles pour offrir une sécurité assistée par matériel, adaptée aux besoins de votre entreprise.

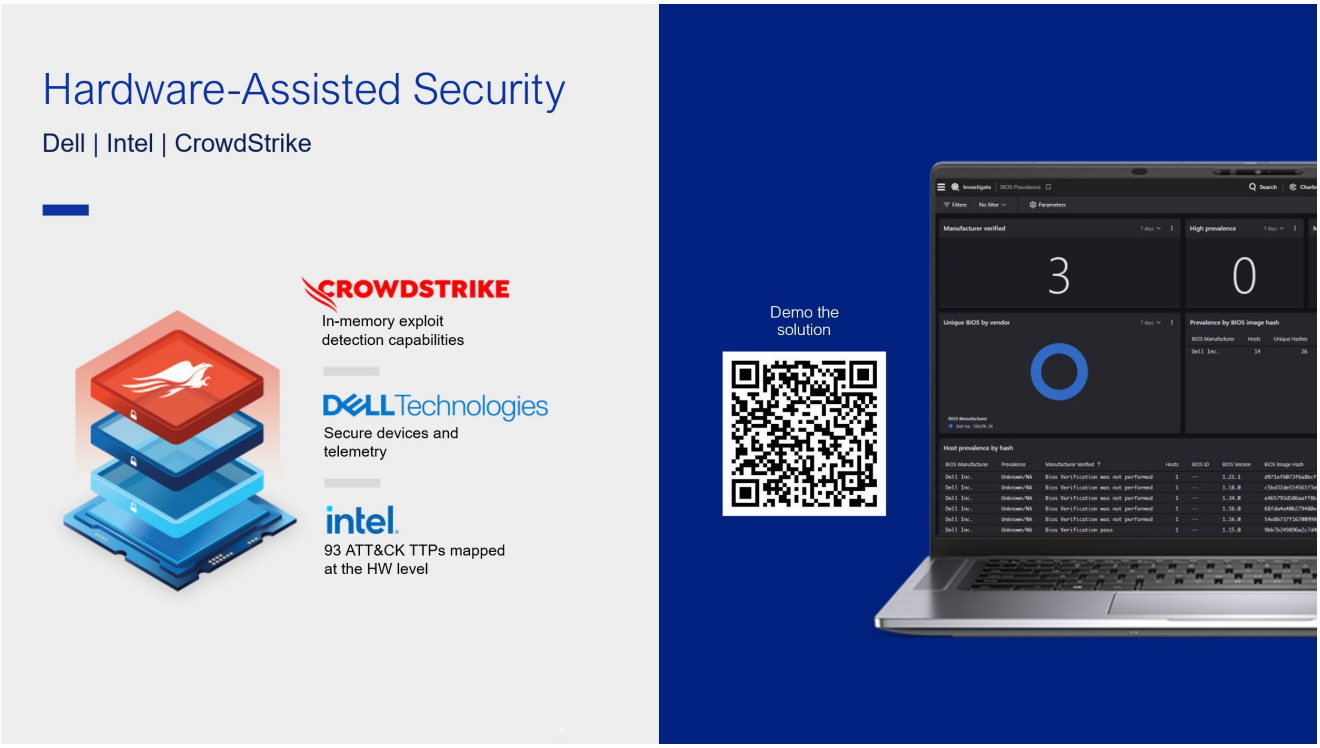



Figure 4 : sécurité multicouche sur les AI PC professionnels Dell, intégrée à CrowdStrike et Intel.

## Valeur ajoutée de l'intégration d'Intel et CrowdStrike sur les AI PC Dell

Amélioration de la sécurité des points de terminaison grâce à l'IA et à l'accélération du GPU/NPU **:** les cybermenaces deviennent de plus en plus sophistiquées, et les AI PC sont conçus pour garder une longueur d'avance en utilisant l'IA sur le périphérique pour une détection de menaces plus rapide et en temps réel tout en réduisant la dépendance aux services Cloud. Des outils tels que CrowdStrike peuvent décharger la détection des logiciels malveillants des unités de traitement neuronal (NPU) intégrées, détectant ainsi les menaces plus rapidement avec un impact minimal sur les performances du processeur. Grâce au traitement local des données et aux fonctionnalités anti-hameçonnage avancées des AI PC d'architecture Intel, les informations sensibles restent sécurisées, ce qui réduit l'exposition aux risques externes.

Exemples de travaux réalisés par Intel et CrowdStrike (actuellement en phase de validation de concept, mais disponibles pour le public dans les prochains mois) pour améliorer la sécurité des points de terminaison grâce à l'accélération de l'IA et des NPU :

- Détection d'exploitation renforcée par le matériel (HEED) : utilise la télémétrie du processeur Intel pour suivre le flux de contrôle des applications et identifier les attaques ciblant la mémoire.
- Analyse accélérée de la mémoire : utilise Intel Threat Detection Technology pour décharger le processus d'analyse de la mémoire gourmand en ressources vers le processeur graphique Intel intégré, pour une capacité d'analyse de la mémoire jusqu'à 7 fois plus élevée.

Avec ces deux fonctionnalités, Intel contribue à alimenter les indicateurs de capacités d'attaque basés sur l'IA de CrowdStrike présents sur le point de terminaison et le Cloud de sécurité CrowdStrike. Ces fonctionnalités fournissent également une nouvelle vision dans la couche mémoire pour CrowdStrike afin de proposer de nouveaux modèles de détection à l'avenir, améliorant ainsi la sécurité au fil du temps.

**Défense validée par le secteur de la sécurité des AI PC :** de nouvelles recherches du MITRE prouvent que votre choix de matériel informatique joue un rôle essentiel dans la mise en place de logiciels de sécurité et de fonctionnalités de système d'exploitation pour protéger efficacement vos actifs.

Les équipes SecOps (Security Operations) déploient des agents puissants sur les parcs informatique de points de terminaison pour inspecter chaque processus afin d'identifier les signes de logiciels malveillants. Les fournisseurs de logiciels de sécurité ont mis en correspondance leurs capacités avec le cadre MITRE ATT&CK pour montrer où ils fournissent des solutions. Les fournisseurs de sécurité gérée aident les entreprises à trier les alertes quotidiennes dans les outils de sécurité XDR, SIEM et co-pilot. C'est assez complexe, mais l'applicabilité de la sécurité matérielle aux attaques réelles visant les PC que vous possédez déjà est restée un mystère... jusqu'à récemment.

Fin 2024, le Center for Informed Defense du MITRE® (CTID) a collaboré avec plus d'une trentaine d'experts d'Intel, Microsoft, CrowdStrike et ATTACK IQ afin de comparer et de classer l'importance des fonctionnalités logicielles de sécurité optimisées pour le matériel par rapport aux tactiques et (sous-)techniques du cadre d'attaques MITRE. Ensemble, le groupe a mis en correspondance les fonctionnalités de sécurité Intel vPro® avec 150 tactiques de menaces, (sous-)techniques et procédures (TTP) cumulatives et uniques dans lesquelles le matériel informatique fournit des protections prêtes à l'emploi avec un logiciel de sécurité optimisé.

Pour la validation des tests de correspondance et d'émulation, le MITRE a utilisé un système Dell Pro équipé d'un processeur Intel Core Ultra (notamment l'ensemble complet des protections de sécurité Intel vPro activées sur une pile logicielle de sécurité standard de niveau entreprise), ce qui enrichit les défenses « sous le système d'exploitation » intégrées uniques de Dell.

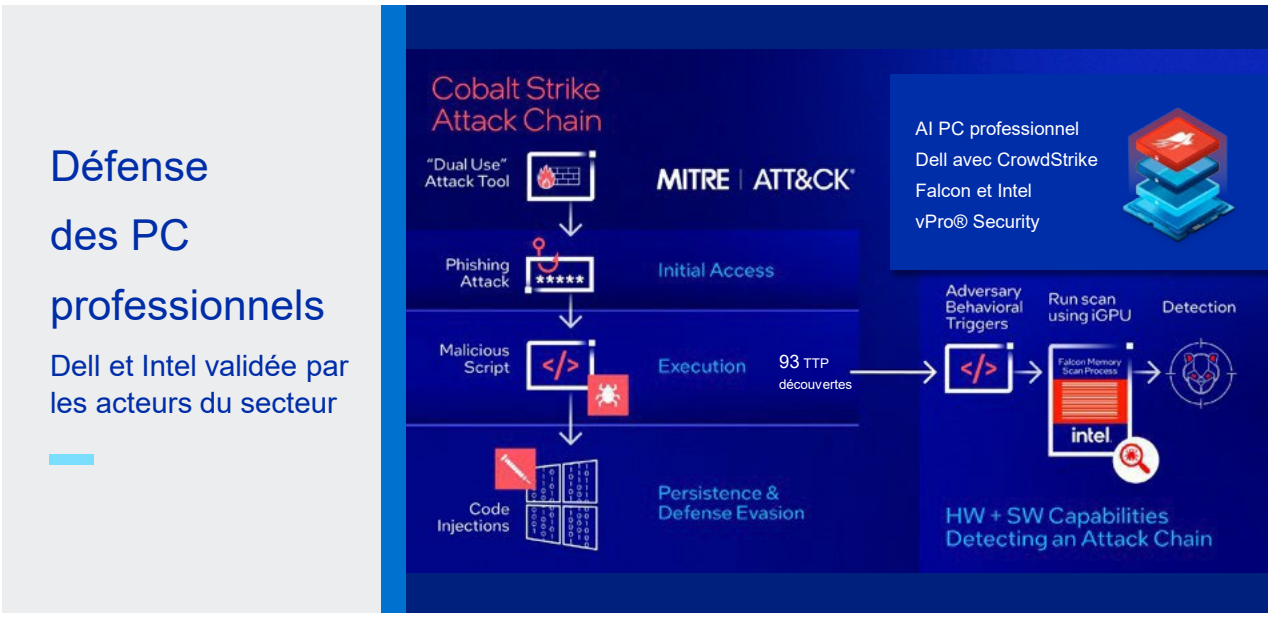



Figure 5 : la sécurité assistée par matériel fonctionne.

Dans l'exemple de scénario (scénario Cobalt Strike Attack Chain), nous montrons une attaque Cobalt Strike sans fichier vers la mémoire et la façon dont CrowdStrike Falcon permet de fournir des mesures préventives en utilisant le matériel. Comme mentionné précédemment, les attaques de logiciels malveillants sans fichier sont devenues populaires parmi les cybercriminels. Près de 75 % de tous les types d'attaque utilisent des processus système valides, comme l'exécution en mémoire, où ils peuvent échapper aux défenses de détection et de réponse des points de terminaison (EDR) traditionnelles. Cette illustration montre bien comment le matériel de votre PC contribue à fournir la puissance de calcul supplémentaire nécessaire pour analyser la mémoire sans perturber l'expérience informatique de l'utilisateur. **CrowdStrike utilise les algorithmes d'analyse accélérée de la mémoire de la technologie Intel Threat Detection (Intel TDT) et sa capacité à décharger le traitement vers le processeur graphique intégré à la technologie Intel Graphics Technology. Cela permet d'obtenir des performances jusqu'à 7 fois plus rapides, ce qui garantit une bonne expérience utilisateur tout en offrant la capacité d'analyser plus en profondeur et de découvrir plus de 93 TTP.** (Remarque : La fonctionnalité d'analyse de la mémoire de CrowdStrike, conçue dans son logiciel, fonctionne uniquement sur les PC Intel vPro.)

Avoir des informations sur les mesures de sécurité logicielles et matérielles peut aider les entreprises à exploiter tout le potentiel disponible sur les AI PC modernes. Les résultats prouvent que le choix du matériel informatique a un impact significatif sur la capacité des logiciels de sécurité et des fonctions du système d'exploitation à contrer des menaces spécifiques et à protéger les actifs de l'entreprise contre les cybercriminels avancés.

Les cadres de sécurité sous et au-dessus du système d'exploitation de Dell et Intel offrent une approche globale de la protection des appareils professionnels, mais en tant qu'experts en sécurité, nous savons qu'aucun appareil n'est sécurisé à 100 %. C'est pourquoi nous sommes leaders du secteur pour les investissements en matière de sécurité post-commercialisation. Nous garantissons que nos appareils restent sécurisés pendant des années après leur commercialisation.

**Support continu**

## Dell et Intel investissent dans la sécurité continue de leurs plates-formes, après leur commercialisation

Dell et Intel ont réalisé des investissements importants et durables pour garantir la sécurité tout au long du cycle de vie des produits. Une fois qu'un appareil ou une plateforme est sur le marché, les équipes Dell et Intel continuent de tester activement leurs produits pour détecter toute faille de sécurité. Pour Intel, ce processus inclut une collaboration avec des chercheurs et des universités, de façon à détecter les failles possibles avant que des acteurs malveillants ne les trouvent, corriger rapidement toutes les menaces de sécurité identifiées, puis les consigner dans un rapport.

L'assurance de sécurité proactive des produits inclut des efforts visant à détecter les failles de sécurité en interne et des mesures incitatives destinées à la communauté des chercheurs en sécurité extérieure via des programmes de primes aux bogues. En 2024, les investissements d'Intel dans l'assurance proactive de la sécurité des produits ont mené à 96 % des vulnérabilités découvertes et atténuées. Les 4 % restants de failles de sécurité corrigées par Intel n'ont pas été soumis via le programme de primes aux bogues d'Intel ou ont été soumises par des partenaires ou d'autres organisations qui ne cherchent pas à obtenir de primes. Dans tous les cas, Intel a collaboré avec des chercheurs pour coordonner la divulgation publique de ces problèmes, ce qui signifie que les clients pouvaient bénéficier de mesures d'atténuation à la date de divulgation publique.

Pour gérer les failles de sécurités et expositions courantes (CVE) identifiées via ses programmes étendus, Intel publie régulièrement des mises à jour de plate-forme Intel, pour tous les systèmes fonctionnant avec ses produits. Ce processus trimestriel comprend des mises à jour de sécurité, fonctionnelles et de fonctionnalités dans le microcode, le firmware et le BIOS du système. Des mises à jour régulières permettent aux partenaires Intel de valider et d'intégrer les mises à jour de matériel et firmware dans leurs plates-formes selon un calendrier trimestriel prévisible, menant à une divulgation publique coordonnée dans l'ensemble de l'écosystème.

La coordination de la publication des failles de sécurité identifiées sur les produits et de la réponse apportée est gérée par les équipes dédiées de réponse aux incidents de sécurité des produits de Dell et Intel. Ensemble, elles s'assurent que les CVE sont gérées rapidement et en toute sécurité, ce qui permet d'atténuer efficacement les risques qu'elles représentent.

Dell et Intel ont réalisé ces investissements pour fournir un support continu aux clients et alléger la charge de travail de leurs équipes IT. Nous avons recruté des chercheurs, des architectes de sécurité et des analystes en informatique légale pour assurer la sécurité de votre entreprise et permettre à vos équipes de se concentrer sur l'équipement de vos collaborateurs, afin qu'ils puissent donner le meilleur d'eux-mêmes.

## Les investissements d'Intel ont permis de traiter 96 % des failles de sécurité trouvées en 2024

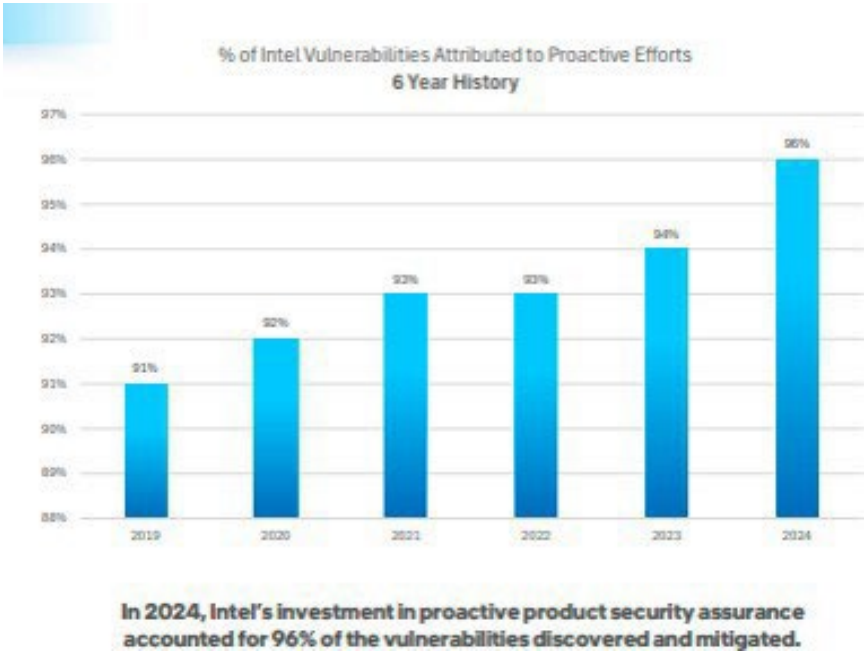
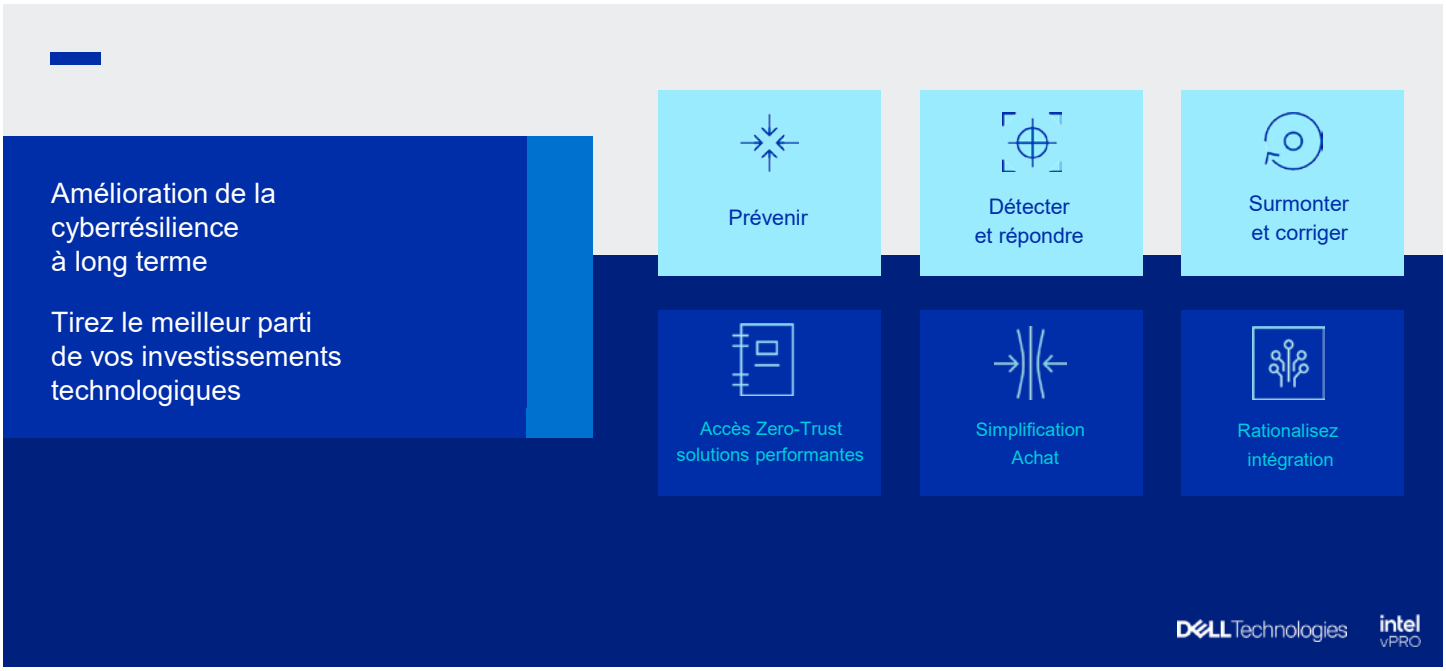



Figure 6 : pourcentage de failles de sécurité Intel attribuées aux efforts proactifs (source : Rapport sur la sécurité des produits Intel 2024)

# Conclusion

## Résultats de la collaboration avec Dell et Intel



L'objectif de Dell et Intel est de mettre au point des solutions basées sur un état d'esprit conflictuel. Un des objectifs clés des cybercriminels : l'argent qu'ils gagnent en volant des données et en les vendant ou en les retenant en otage. Par conséquent, bien que leur méthode d'action varie (le cadre MITRE ATT&CK® suit neuf méthodes d'accès initiales globales), les « kill chain » des cyberattaques sont très similaires : reconnaissance, accès initial (en exploitant une vulnérabilité = faiblesse ou exposition = erreur qu'ils ont trouvée), infiltration d'un réseau, déplacement latéral/obtention d'un accès privilégié plus important, espionnage et développement des connaissances, exfiltration de données.

Nous pouvons vous aider à sécuriser n'importe quelle charge applicative grâce à des produits, des solutions et des services intelligents conçus pour contrer les menaces potentielles. Au lieu d'essayer de bloquer 100 % des attaques (ce qui est impossible), nous acceptons la situation en supposant qu'une attaque est inévitable et en nous basant sur les défenses dans le pire des cas. Nous mettons l'accent sur la visibilité et la facilité d'action sur l'ensemble d'un parc informatique. Nos clients peuvent ainsi garder une longueur d'avance sur les vecteurs d'attaque émergents.

En mettant en place les solutions de sécurité des terminaux Dell et Intel, les organisations **obtiennent des résultats clés en matière de sécurité** :

- **Amélioration de la cyberrésilience à long terme**
- **Tirez le meilleur parti de vos investissements technologiques**

Cas d'utilisation de la cybersécurité... :

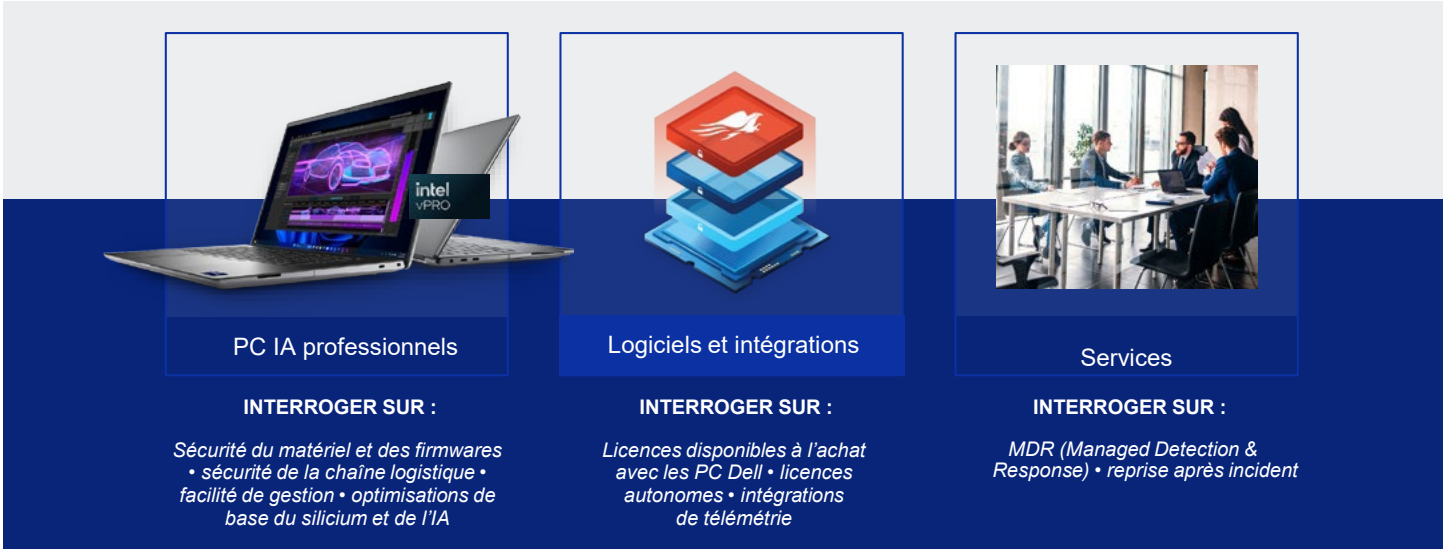
- **Réduction de la surface d'attaque** : limiter le risque de propagation d'une attaque ; minimiser les failles de sécurité et les points d'entrée susceptibles d'être exploités pour compromettre l'environnement.
- **Amélioration de la détection et la réponse aux menaces** : identifiez et gérez activement les incidents de sécurité potentiels et les activités malveillantes grâce à des couches de défense intégrées qui accélèrent la détection et la réponse.
- **Activation de la récupération et mesures correctives** : capturer les données de violation à des fins d'analyse afin de vous prémunir contre les menaces futures et restaurer les points de terminaison vers un état sécurisé et opérationnel antérieur après un incident de sécurité.

…ainsi que la réduction de la charge opérationnelle de la sécurité :

- Maintenez la confiance des appareils et des identités grâce à **des offres compatibles avec le concept Zero-Trust**
- **Simplifiez les achats** en regroupant les fournisseurs et en obtenant un accès au matériel, aux logiciels et aux services dans un emplacement unique
- Économisez du temps et des ressources grâce à **une intégration rationalisée**

C'est votre capacité à collecter et à analyser les informations sur les menaces, et à y répondre, qui détermine si vous gagnez ou perdez la bataille de la cybersécurité. Les pirates d'aujourd'hui ne sont jamais à court d'innovation. Sachant que la plupart des solutions de sécurité se concentrent uniquement sur ce qui se passe « au-dessus du système d'exploitation », les cybercriminels recherchent des surfaces d'attaque moins dures : les couches situées « sous le système d'exploitation » et la chaîne logistique. Pour devancer les acteurs malveillants et garantir la sécurité de leur entreprise, les leaders d'aujourd'hui doivent savoir que les technologies de sécurité matérielle intégrées sont cruciales lors du déploiement des appareils professionnels utilisés par leurs collaborateurs.

## Découvrir les solutions adaptées à vos besoins




Dell, Microsoft et Intel offrent un niveau de sécurité de la chaîne logistique, des protections matérielles, des logiciels de protection contre les menaces avancées, des services managés et un support continu de classe mondiale, pour fournir à votre entreprise des appareils professionnels efficaces et qui tiennent aussi vos données métier à distance du Dark Web.

*AI PC professionnels les plus sécurisés : d'après une analyse tierce réalisée par Principled Technologies comparant les AI PC professionnels Dell avec processeurs Intel avec HP et Lenovo, juillet 2025. Basé sur une analyse interne menée par Dell sur le marché mondial des PC, octobre 2024. S'applique aux PC équipés de processeurs Intel. Toutes les fonctionnalités ne sont pas disponibles sur tous les PC. Certaines fonctionnalités sont vendues séparément.

---

En savoir plus sur les solutions Dell

Contacter un expert Dell Technologies

Consulter d'autres ressources

Rejoindre la discussion