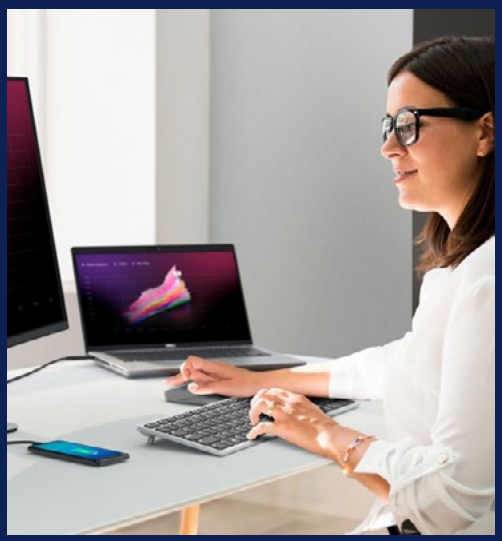
DELL Technologies

Oubliez les concessions

Comment protéger vos équipes boostées par l'IA avec Dell Technologies, Microsoft et Intel



Windows 11

intel

Synthèse

La transition vers le travail hybride a engendré une plus grande complexité et de nouveaux vecteurs d'attaque, tandis que les points de terminaison, les réseaux et les Clouds élargissent les surfaces d'attaque. Par ailleurs, la course à l'adoption de l'IA générative ne fait qu'accentuer les enjeux en introduisant de nouvelles problématiques de sécurité, comme la fuite de données et de propriété intellectuelle, ou les attaques contextuelles éclair.

De plus, les cybercriminels ont désormais recours à des techniques sophistiquées qui visent différentes couches de la pile informatique, en se dissimulant dans des processus système valides. Certaines méthodes leur permettent même d'obtenir un accès privilégié et de désactiver des protections logicielles sans être détectés.

L'union fait la force…

Aucun fournisseur ne peut répondre seul à tous ces enjeux. C'est pourquoi Dell, Intel et Microsoft travaillent ensemble stratégiquement afin d'éliminer ce fardeau pour les organisations.

Notre approche globale de la sécurité intègre des fonctionnalités matérielles « sous le système d'exploitation » qui aident à contrer les attaques grâce à des protections Intel intégrées au niveau de la puce qui préservent les appareils en profondeur.

Nous veillons ensuite à ce que Windows 11, les appareils modernes Dell et les logiciels fonctionnent ensemble pour réduire la surface d'attaque, protéger l'intégrité du système, les utilisateurs et les données de valeur

Plus forts ensemble. Plus forts pour vous.

La sécurité intégrée et intrinsèque unique de Dell Technologies réunit toutes les innovations de nos partenaires Intel et Microsoft en matière de sécurité afin que vous puissiez protéger le personnel hybride contre les menaces en constante évolution.

Seuls 33 % des décideurs informatiques utilisent une stratégie de sécurité globale de bout en bout intégrant à la fois des protections matérielles et logicielles.

Source : Dell Innovation Index, 2023

Sujets abordés dans ce document

Socle de sécurité

Cycle de vie du développement sécurisé

Dell Technologies, Intel et Microsoft travaillent en étroite collaboration pour intégrer la sécurité de la puce au Cloud avec, par exemple, les appareils Dell Trusted Devices, les PC professionnels les plus sécurisés du secteur*.

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.

* D'après une analyse interne réalisée par Dell en septembre 2022. Toutes les fonctionnalités ne sont pas disponibles sur tous les PC. Certaines fonctionnalités sont vendues séparément.

Cadre de défense complet : application de la sécurité Zero-Trust

Sécurité pilotée par l'IA

Utilisation de l'IA pour automatiser la protection des utilisateurs, offrant des solutions de sécurité révolutionnaires prêtes à l'emploi.

Sécurité sous le système d'exploitation

Les fonctionnalités de sécurité matérielle aident à protéger les appareils contre les menaces visant leurs couches de base.

Sécurité au-dessus du système d'exploitation

Les technologies de sécurité logicielles et les protections au niveau de la puce sont essentielles pour assurer la sécurité globale des appareils.

Sécurité Windows 11

Protection prête à l'emploi avec des couches logicielles et matérielles étroitement intégrées entre système d'exploitation, applications, système de gestion des identités et Cloud.

Support continu

Dell, Intel et Microsoft s'assurent que leurs solutions restent sécurisées en corrigeant les failles de sécurité et en mettant à jour la sécurité au niveau de la puce dans le système d'exploitation.

Le niveau de sécurité de votre réseau d'entreprise correspond à celui de son point de terminaison le plus faible

Pas un mois ne se passe sans qu'une nouvelle grande marque mondiale ne soit victime d'une violation 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 les expose 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 que vous utilisez pour travailler, alors que vous n'avez aucun contrôle sur leur cycle de fabrication ou de développement ?

Dell, Microsoft et Intel savent que le seul moyen de sécuriser les appareils et les réseaux professionnels de manière fiable consiste à harmoniser les technologies de sécurité matérielle et logicielle. 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.

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 préserver leurs activités, ils ne protègent pas le matériel sur lequel les logiciels sont installés, le laissant vulnérable face aux 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.

Autrement dit, ce qui fonctionne pour les appareils destinés aux particuliers ne fonctionne généralement pas dans un environnement professionnel, qui représente une cible plus attractive pour les pirates.

C'est pourquoi Dell, Microsoft et Intel adoptent une approche différente et globale de la sécurité.

Le niveau de sécurité de votre réseau d'entreprise correspond à celui de son point de terminaison le plus faible

Dell, Microsoft et Intel proposent une sécurité matérielle intégrée

Les niveaux de complexité et les préoccupations liées à la sécurisation des appareils et des réseaux sont vertigineux. 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 prospérer leur entreprise.

La relation de codéveloppement que Dell, Microsoft et Intel entretiennent depuis des décennies se concentre depuis toujours sur la protection des données, en particulier celles des clients professionnels. Grâce à son partenariat avec Microsoft et 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 ? Bien plus qu'un simple assemblage de fonctionnalités : nous intégrons étroitement technologies, outils et règles tout au long du cycle de vie des PC professionnels, afin de fournir une sécurité de bout en bout à nos clients et à leurs entreprises.

Sécurité intégrée dès la conception
Lorsqu'ils conçoivent les systèmes de demain, Microsoft, Intel et Dell gardent un temps d'avance sur les menaces actuelles, afin de limiter 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 des technologies Dell Trusted Device et Intel® Hardware Shield pour renforcer les défenses des appareils via un cadre de prévention, de détection et de réponse. En outre, Dell, Microsoft et Intel disposent d'équipes de sécurité dédiées pour tester les produits et rechercher de nouvelles failles de sécurité avant que des pirates ne les trouvent, et pour déployer rapidement des correctifs afin de vous aider à protéger votre équipe et votre entreprise.

Dans ce livre blanc, nous découvrirons comment Dell, Microsoft et Intel ont collaboré pour produire des plateformes PC professionnelles avec une sécurité intégrée en profondeur, afin de protéger vos appareils tout au long de leur cycle de vie, notamment grâce à des actualisations régulières.

La sécurisation de nos plateformes commence sur le tableau blanc

Planification, évaluation et analyse

Avant de concevoir leurs tout derniers chipsets, plateformes et logiciels, les experts Dell, Microsoft et Intel définissent des paramètres stricts répertoriant ce qu'une plateforme sécurisée doit inclure pour répondre aux futurs besoins de sécurité et respecter les réglementations applicables en la matière.

Ce processus commence 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 les atténuer. Cette évaluation permet de définir les objectifs de sécurité qui serviront à évaluer nos architectures.

Avec ces informations, les équipes de sécurité Dell, Microsoft et Intel développent des modèles de menaces en adoptant une approche de l'architecture conceptuelle du point de vue de l'adversaire, et en recherchant les failles de sécurité et les vulnérabilités potentielles à neutraliser. 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.

La sécurisation de nos plateformes commence sur le tableau blanc

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 du code sécurisé et une analyse du code statique, un processus automatisé qui utilise des outils spéciaux pour rechercher et corriger les défauts. Certains produits présentant un code plus complexe passent ensuite par 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 d'experts en piratage sont chargées d'effectuer des tests de pénétration et d'intrusion pour détecter les failles de sécurité potentielles passées inaperçues au cours des phases précédentes. Ces failles de sécurité sont de 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.

De l'assemblage à la livraison des appareils, notre investissement dans la sécurisation de la chaîne logistique, un des vecteurs d'attaque de plus en plus utilisé par les acteurs malveillants, reflète notre engagement envers la sécurité de bout en bout. 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.

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 son arrivée 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 leurs produits avant qu'ils n'arrivent chez les clients, et pour permettre une autovérification de l'authenticité des appareils avant leur distribution aux collaborateurs.

Source

Dell utilise un processus rigoureux de contrôle des partenaires pour garantir la qualité et la sécurité des appareils et de leurs composants. En outre, ces partenaires sont régulièrement soumis à des audits afin de garantir qu'ils respectent l'ensemble des normes de sécurité de la chaîne logistique Dell.

Fabrication

Outre le respect des normes de sécurité de la chaîne logistique Dell, les fabricants d'appareils Dell testent fréquemment les pièces pendant la fabrication, afin de s'assurer qu'aucun produit de contrefaçon ne se glisse dans la chaîne logistique. Pour atténuer encore 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 que le client reçoive exactement ce qui a été expédié.

Livraison

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

Les appareils Dell sont également équipés de technologies de détection des altérations. Les solutions Dell Technologies Safe SupplyChain 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.

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

Vérification

Les appareils professionnels Dell sont livrés avec des certificats de plateforme signés de manière chiffrée, qui capturent les attributs de snapshot des plateformes lors de la fabrication, de l'assemblage, des tests et de l'intégration. Ces attributs de plateforme sont ensuite liés de manière chiffrée à l'appareil spécifique à l'aide du module TPM (Trusted Platform Module) en tant que racine de confiance matérielle.

Dell a implémenté des certificats de plateforme Trusted Computing Group dans la solution Dell Secured Component Verification (SCV) pour les ordinateurs professionnels équipés de processeurs Intel. 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, SCV garantit l'intégrité complète du matériel lors du transit vers les environnements IT, et permet aux clients de vérifier que les PC professionnels et les composants clés Dell livrés sont conformes à ce qui a été fabriqué et commandé.

De même, Intel permet aux fournisseurs de garantir la transparence et la traçabilité de la chaîne logistique numérique de base depuis de nombreuses années. Intel® Transparent Supply Chain (Intel® TSC) fournit des certificats de plateforme TCG et des données de composants pour la prise en charge des plateformes basées sur Intel, à l'aide d'une API Cloud disponible pour le département IT via le portail Web Intel® TSC. Bien que Dell et Intel aient choisi d'implémenter des solutions indépendantes, les certificats de plateforme TCG sont communs à Intel® TSC et Dell SCV. Ce point commun offre une compatibilité et une interopérabilité qui permettent aux acheteurs des entreprises et du secteur public de déployer des certificats de plateforme TCG pour mieux garantir la sécurité de la chaîne logistique numérique sur les appareils basés sur Intel.

Cadre de défense complet : application de la sécurité Zero-Trust

Les organisations qui progressent en matière de cybersécurité conçoivent une feuille de route exploitable afin d'identifier des moyens de réduire la surface d'attaque, de détecter et de contrer les cybermenaces, et de récupérer après une cyberattaque. Le tout avec des fonctionnalités permettant d'adopter une approche Zero-Trust.

Pour faire face à des cybermenaces toujours plus sophistiquées, Dell s'appuie sur les fonctionnalités de sécurité intégrées dans ses solutions et celles de ses partenaires, dont Microsoft et Intel, pour aider ses clients à atteindre une approche Zero-Trust qui s'aligne sur leurs objectifs métier.

77 %

n'ont pas encore exploré ni construit une architecture Zero-Trust*

* Dell Technologies, Innovation Index, 2023 : https://www.dell.com/en-us/dt/perspectives/innovation-index.htm

Avec une architecture entièrement intégrée, simplifiez radicalement l'adoption d'une approche Zero-Trust pour votre personnel

Dell, Microsoft et Intel collaborent pour favoriser un environnement de travail hybride fluide et sécurisé, permettant aux clients de respecter les trois principes du Zero-Trust :

1. Vérifier de manière explicite

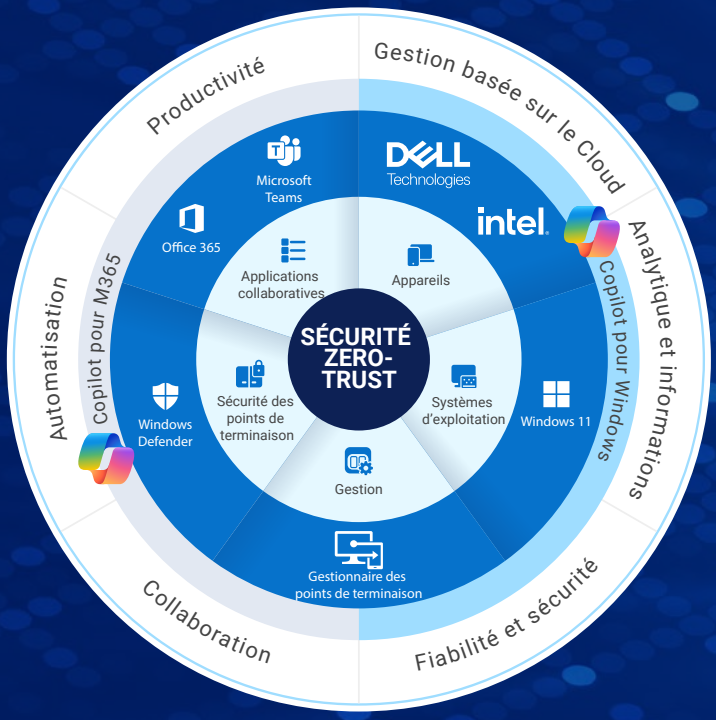
Exigez systématiquement une authentification et accordez toujours les autorisations en fonction de tous les points de données disponibles, y compris l'identité de l'utilisateur, son emplacement, l'intégrité de l'appareil, le service ou la charge applicative, la classification des données et les anomalies.

2. Utiliser l'accès basé sur le principe du moindre privilège

Limitez l'accès des utilisateurs avec un modèle juste-à-temps (JIT) avec accès juste suffisant (JEA), des règles évolutives basées sur le risque et une protection des données afin de sécuriser les données et la productivité.

3. Anticiper une violation

Opérez d'une manière qui réduit le périmètre impacté et l'accès aux segments. Vérifiez le chiffrement de bout en bout et utilisez l'analytique pour gagner en visibilité, détecter les menaces et améliorer les défenses.



Nos solutions conjointes aident les organisations à mettre en œuvre un modèle de sécurité Zero-Trust en vérifiant chaque tentative d'accès et en appliquant des règles de sécurité strictes basées sur l'identité, l'intégrité de l'appareil, l'emplacement et le niveau de risque. Cela réduit le risque d'accès non autorisé et atténue l'impact des violations de sécurité.

Nécessite les intégrations suivantes :

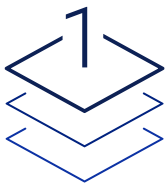
Sécurité du BIOS/firmware des PC professionnels Dell, sécurité matérielle, assurance de la chaîne logistique, logiciels de gestion des menaces (EDR, XDR, VDR), logiciels de protection des données réseau et Cloud combinés avec Intel® Hardware Shield exclusivement sur la plateforme Intel vPro®.

Offre Microsoft complète d'outils et de technologies pour la gestion des identités et des accès, la sécurité des points de terminaison, la sécurité du réseau, la protection des données, l'intelligence sur les menaces, l'analyse de la sécurité, l'application des règles, ainsi que la surveillance et la réponse en continu. Ceci comprend Azure Active Directory, Microsoft Defender for Endpoint, le Pare-feu Azure, Azure Information Protection, Microsoft Threat Intelligence, Azure Sentinel, Microsoft Endpoint Manager et Microsoft Security Center.

Sécurité pilotée par l'IA

Sécurité révolutionnaire pilotée par l'IA, prête à l'emploi

Dell, Intel et Microsoft utilisent l'IA pour automatiser la protection des utilisateurs, en offrant collectivement des solutions de sécurité révolutionnaires prêtes à l'emploi. Ces mesures innovantes sont conçues pour prévenir et détecter les attaques actuelles, plus sophistiquées, en intégrant une sécurité matérielle, un chiffrement avancé et une protection contre les logiciels malveillants, le tout optimisé par des processeurs Intel® Core™ Ultra sur Intel vPro® et des systèmes d'exploitation Windows 11 Professionnel, intégrés de façon fluide dans les appareils Dell modernes. Ces efforts de collaboration réduisent considérablement la surface d'attaque en mettant en œuvre plusieurs couches de défense, visant principalement trois domaines clés :



1. En dessous du système d'exploitation :

- Dell et Intel ont étroitement collaboré sur Dell SafeBIOS, un mécanisme de défense robuste contre les attaques visant le BIOS et le firmware, avec vérification hors hôte pour garantir l'intégrité du BIOS en utilisant un firmware sur Intel vPro®.
- La toute dernière plateforme Intel vPro® réduit la surface d'attaque physique jusqu'à 70 % par rapport à des appareils datant d'il y a quatre ans*
- Les appareils Dell avec Intel vPro® obtiennent la certification Windows 11 Secured-Core PC Niveau 3, intégrant une suite de protections étroitement intégrées.
- Par exemple, le rapport de sécurité du système d'Intel garantit au système d'exploitation que le processus de démarrage a été exécuté en toute sécurité, assurant son intégrité dès le départ.
- Ces protections sont intrinsèques et opérationnelles de façon fluide dès la première utilisation.

2. Protection des applications et des données :

- Des fonctionnalités avancées intégrées permettent de protéger les informations d'identification des utilisateurs, comme l'isolation de ces dernières avec Windows Hello via les technologies de virtualisation d'Intel.
- Le chiffrement multiclé total de la mémoire dote les machines virtuelles Windows 11 d'une mémoire chiffrée, isolant efficacement les processus et les données qui leur sont associées.
- Ces mesures de protection sont préconfigurées pour une utilisation immédiate ou peuvent être ajustées facilement via le centre de sécurité Windows.

3. Détection des menaces avancées :

- La technologie Intel® Threat Detection Technology se démarque comme étant la seule solution de détection des menaces par l'IA au niveau de la puce capable de contrer les attaques de rançongiciel et de cryptojacking.
- Étant donné que les rançongiciels visent principalement le processeur pour chiffrer le contenu stratégique de l'entreprise, Intel TDT utilise une détection des menaces pilotée par l'IA pour analyser la télémétrie du processeur à la recherche d'indicateurs d'attaque et signale rapidement les processus malveillants. Les logiciels de sécurité comme Microsoft Defender peuvent alors intervenir pour les mettre en quarantaine ou les supprimer plus facilement.

*13th Gen Intel® Core™ Processor Attack Study Report

Sécurité pilotée par l'IA

Notre collaboration s'étend à l'analyse accélérée de la mémoire pour la détection précoce des logiciels malveillants sans fichier, ce qui offre un niveau de sécurité supplémentaire pour contrer les attaques de logiciels malveillants. Grâce à notre partenariat avec Microsoft Defender et Intel Threat Detection Technology, nous optimisons les processus d'analyse gourmands en ressources de calcul en les déchargeant sur le processeur graphique, libérant ainsi le processeur pour une productivité ininterrompue. En cas d'attaque potentielle, le processeur graphique communique proactivement avec MSFT Defender, ce qui permet une approche d'analyse plus complète.

Cette fonctionnalité offre aux **organisations trois avantages :**

Réduction du volume d'attaques sans fichier, qui sont devenues la principale méthode d'entrée pour diverses cybermenaces.

Détection précoce des rançongiciels et autres menaces malveillantes au stade de l'accès initial à la mémoire

Maintien d'une expérience utilisateur hautes performances pendant les analyses de protection de la sécurité.

En utilisant l'analyse accélérée de la mémoire, les organisations peuvent renforcer leur défense contre l'évolution des cybermenaces tout en garantissant une efficacité opérationnelle et une productivité optimales des utilisateurs.

En substance, la collaboration entre Dell, Microsoft et Intel offrent des solutions de sécurité complètes qui englobent la protection matérielle, les processus Secure Boot, la sécurité des applications et des données, ainsi que des capacités de détection des menaces avancées, toutes méticuleusement conçues pour répondre aux cybermenaces actuelles en constante évolution.

Les technologies de sécurité intégrées aident à prévenir, à détecter et à contrer les menaces

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 codéveloppement entre Dell, Microsoft 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 plateforme. En plus de la protection offerte par d'autres outils et technologies Dell et Intel, Intel® Hardware Shield et le cadre Dell SafeBIOS fournissent aux utilisateurs d'appareils professionnels Dell une protection matérielle intégrée.

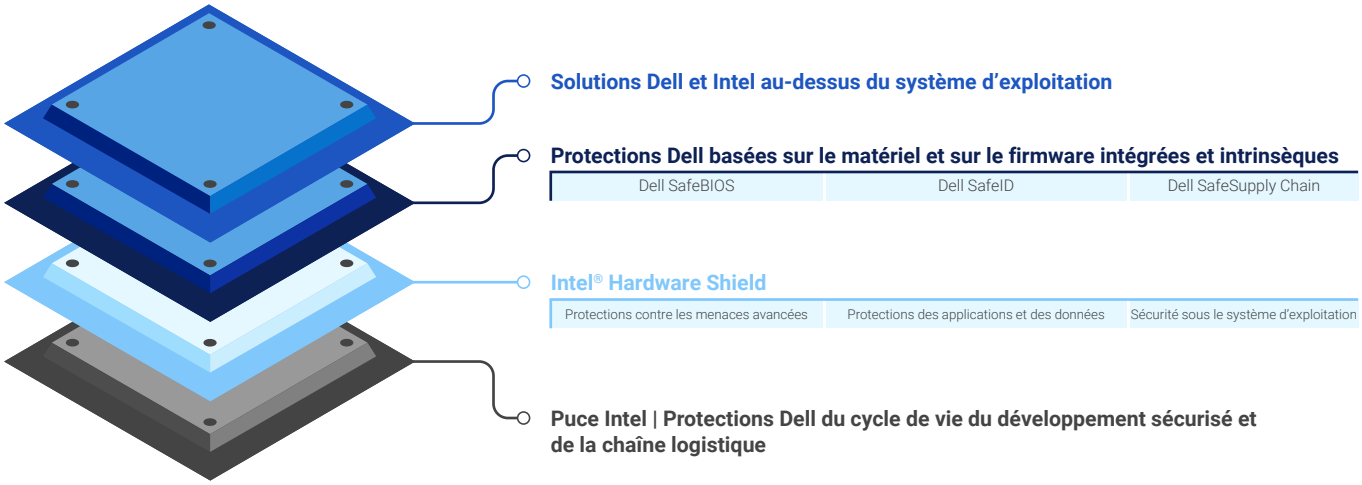


Figure 1 : Intel® Hardware Shield et les protections matérielles de Dell constituent des couches de sécurité qui protègent contre les attaques de base

Intel® Hardware Shield

Intel Hardware Shield est inclus avec chaque appareil professionnel Dell s'exécutant sur la plateforme Intel vPro® et offre des fonctions de sécurité optimisées par le matériel qui aident à protéger toutes les couches de la pile informatique.

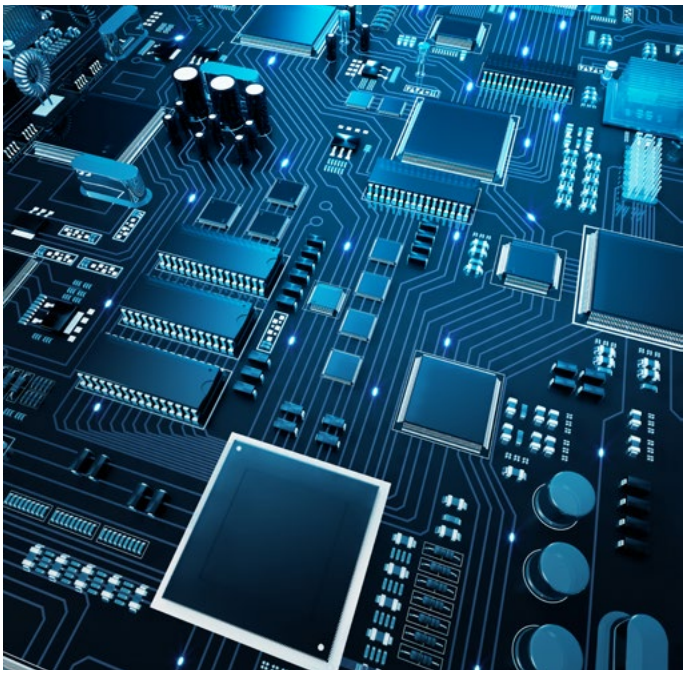
Intel Hardware Shield comporte des protections avancées contre les menaces, des protections pour les applications et les données, et une sécurité sous le système d'exploitation comprenant plus de vingt technologies de sécurité innovantes. Dell tire parti de presque toutes ces fonctionnalités pour développer des solutions de sécurité axées sur les fonctionnalités de base, de façon à fournir aux clients les appareils professionnels parmi les plus sécurisés du marché. Ces solutions comprennent le cadre Dell SafeBIOS, Dell SafeID et Dell SafeSupply Chain, afin d'offrir un niveau encore plus élevé de sécurité contre les menaces actuelles et futures.

Les technologies de sécurité intégrées aident à prévenir, à détecter et à contrer les menaces

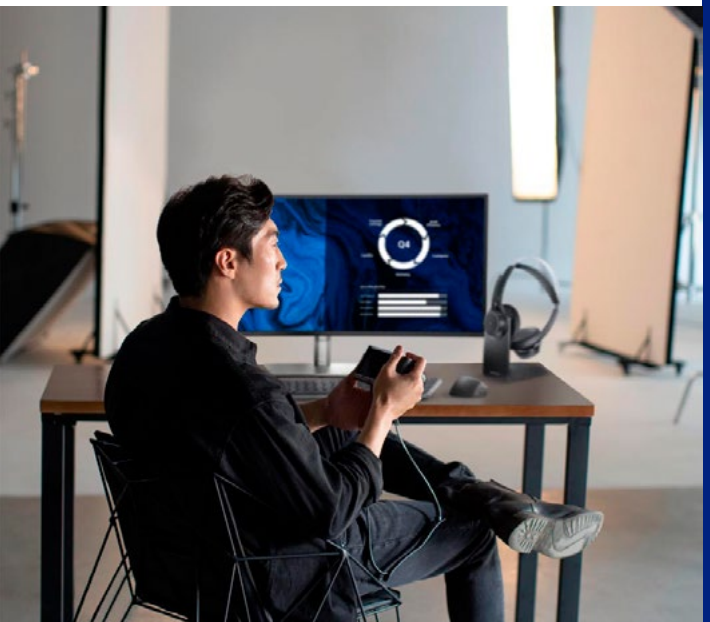
Cadre Dell SafeBIOS, Dell SafeID et Dell SafeSupply Chain

La protection du BIOS 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 stratégique, les appareils professionnels Dell sont livrés avec SafeBIOS, une suite d'outils qui aident à prévenir les attaques contre le BIOS, à détecter si le BIOS a été compromis et à avertir le département IT en cas d'anomalie.

Certains appareils professionnels Dell incluent également Dell SafeID, qui sécurise les informations d'identification de l'utilisateur final dans une puce de sécurité dédiée, afin de les protéger contre les logiciels malveillants qui recherchent et volent les informations d'identification d'accès, compromettant de ce fait l'ensemble du réseau de l'entreprise. Pour renforcer encore la sécurité des produits, Dell propose des fonctionnalités complémentaires en option comme Secured Component Verification et les emballages inviolables via Dell SafeSupply Chain.



Les solutions Dell et Intel pour les couches situées au-dessus du système d'exploitation aident à sécuriser les points de terminaison



Malgré la menace croissante des attaques sous le système d'exploitation, la protection des couches situées au-dessus est plus importante que jamais. Le nombre d'utilisateurs finaux travaillant à distance et en déplacement augmente de manière exponentielle, et vous avez besoin de solutions intelligentes qui bloquent, détectent et neutralisent les menaces, où qu'elles se produisent. La gamme de solutions de sécurité des points de terminaison Dell Trusted Workspace comprend des logiciels en option comme Dell SafeGuard and Response et Dell SafeData pour fournir aux dirigeants d'entreprise ce dont ils ont besoin pour protéger leurs points de terminaison. Les fonctionnalités de sécurité Intel, intégrées en profondeur au niveau de la puce, telles que la technologie Intel® Control-flow Enforcement, assurent une protection contre les attaques visant le système d'exploitation, tandis que d'autres fonctionnalités dans Intel Hardware Shield protègent les couches sous le système d'exploitation, sécurisent les applications et les données, et fournissent des protections contre les menaces avancées.

Nous ajoutons ensuite une couche de sécurité logicielle de Microsoft qui s'étend du socle de sécurité jusqu'au Cloud. Sous Windows 11, matériel et logiciels fonctionnent ensemble pour protéger les données sensibles depuis le cœur de votre PC jusqu'au Cloud. Une protection complète permet à votre organisation de rester sécurisée, quel que soit le lieu de travail des collaborateurs. La page suivante présente les couches de protection de Windows 11.

Les solutions Dell, Microsoft et Intel pour les couches situées au-dessus du système d'exploitation aident à sécuriser les points de terminaison

Intel intègre ensuite les protections matérielles supplémentaires dans chaque couche de sécurité imaginée par Microsoft. Ces protections sont ensuite intégrées dans les solutions clientes Dell.

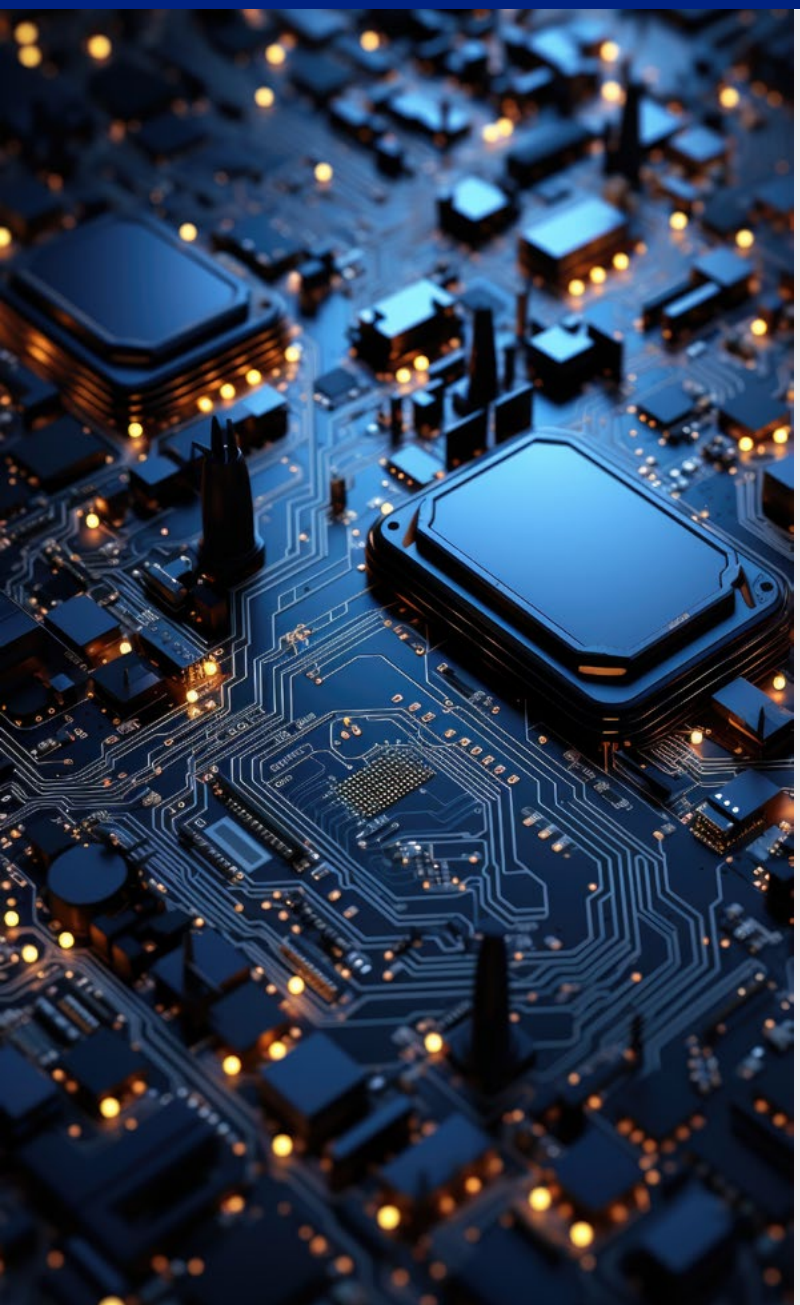
Travailler en partenariat pour offrir une protection puissante par défaut

La sécurité intégrée et intrinsèque unique de Dell Technologies réunit toutes les innovations de nos partenaires Intel et Microsoft en matière de sécurité, afin que vous puissiez protéger le personnel hybride contre les menaces en constante évolution.

Sécurité Windows 11

Une protection de bout en bout avec une gestion moderne.

Windows 11 est le système d'exploitation Windows le plus sûr jamais conçu, car la plupart des fonctions de sécurité sont activées dès la première utilisation. Matériel et logiciels fonctionnent ensemble pour protéger les données sensibles depuis le cœur de votre PC jusqu'au Cloud, avec des couches de protection à chaque niveau du matériel, du système d'exploitation, des applications, de la gestion des identités et du Cloud, le tout en améliorant la productivité, la sécurité et la résilience en tout lieu.



Matériel (puce)

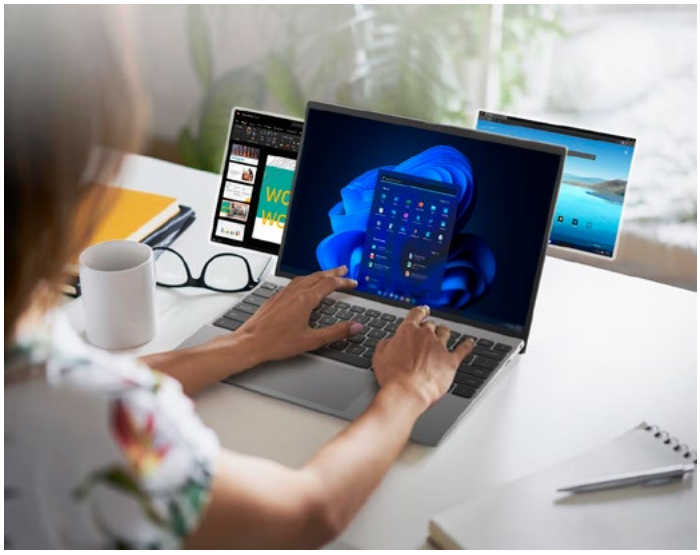
Racine de confiance matérielle

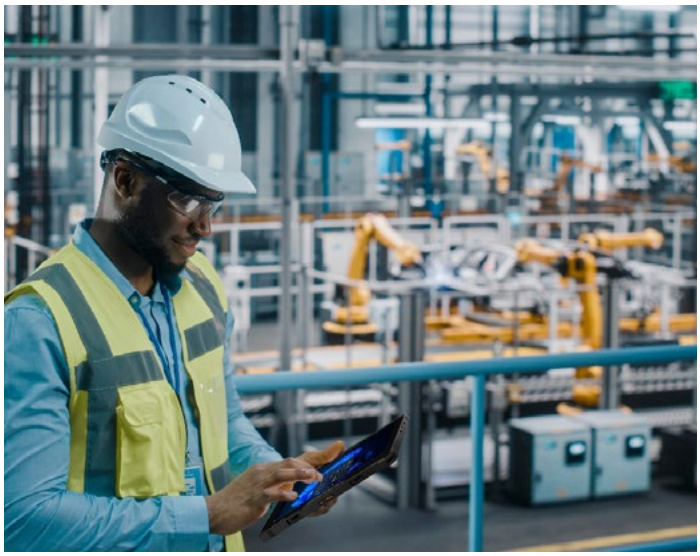
Une racine de confiance matérielle permet de protéger et de maintenir l'intégrité du système lorsque l'appareil s'allume, charge le firmware, puis lance le système d'exploitation, ce qui permet d'atteindre d'importants objectifs en matière de sécurité du système.

Module TPM (Trusted Platform Module)

La technologie TPM est conçue pour fournir des fonctions matérielles liées à la sécurité. Les modules TPM offrent des avantages en matière de sécurité et de protection de la vie privée pour le matériel du système, les propriétaires de plateformes et les utilisateurs. Windows Hello, BitLocker, System Guard (anciennement appelé Windows Defender System Guard) et d'autres fonctionnalités de Windows reposent sur le module TPM, entre autres pour des fonctions de génération de clés, de stockage sécurisé, de chiffrement, de mesures de l'intégrité au démarrage et d'attestation.

Sécurité Windows 11





Système d'exploitation

Sécurité du système

Trusted Boot (Secure Boot + Measured Boot)
Windows 11 exige que tous les PC utilisent la fonction Secure Boot de l'interface UEFI (Unified Extensible Firmware Interface). Lorsqu'un appareil Windows 11 démarre, Secure Boot et Trusted Boot fonctionnent ensemble pour empêcher le chargement de logiciels malveillants et de composants corrompus.

Chiffrement et protection des données

Le **chiffrement de disque BitLocker** est une fonction de protection des données qui s'intègre dans le système d'exploitation et neutralise les menaces de vol ou d'exposition des données provenant d'ordinateurs perdus, volés ou mis hors service de manière inadéquate.

Secured-Core PCs

Microsoft a collaboré avec Dell pour proposer une catégorie spéciale d'appareils appelés Secured-Core PCs (SCPC). Ces appareils sont livrés avec des mesures de sécurité supplémentaires activées au niveau de la couche de firmware (au cœur de l'appareil) qui sous-tend Windows.

Sécurité du réseau

Pour réduire la surface d'attaque d'une organisation, la protection du réseau dans Windows empêche les personnes d'accéder aux adresses IP et aux domaines dangereux susceptibles d'héberger des arnaques par hameçonnage, des codes d'exploitation et d'autres contenus malveillants. À l'aide de services basés sur la réputation, la protection du réseau bloque l'accès aux domaines et adresses IP potentiellement dangereux et à faible réputation.

Protection contre les virus et les menaces

Microsoft Defender SmartScreen Microsoft Defender SmartScreen assure une protection contre le hameçonnage, les applications et les sites Web malveillants et le téléchargement de fichiers potentiellement dangereux.

Sécurité Windows 11

Application

Smart App Control
Smart App Control empêche les utilisateurs d'exécuter des applications malveillantes sur des appareils Windows en bloquant les applications non approuvées ou non signées. Cette application va au-delà des précédentes protections de navigateur intégrées en ajoutant une couche de sécurité supplémentaire qui est directement introduite au cœur du système d'exploitation, au niveau du processus.

Isolation d'application
L'isolation des applications Win32 est une nouvelle fonction de sécurité en préversion publique, conçue pour devenir la norme d'isolation par défaut sur les clients Windows. Elle repose sur AppContainer et offre plusieurs fonctions de sécurité supplémentaires pour aider la plateforme Windows à se défendre contre les attaques qui exploitent les vulnérabilités des applications ou des bibliothèques tierces.

Identité

Authentification sans mot de passe
Windows Hello peut permettre l'authentification sans mot de passe à l'aide d'une vérification biométrique ou par code PIN, et intègre la prise en charge de la norme du secteur FIDO2. Windows Hello Entreprise étend Windows Hello aux comptes ActiveDirectory et Microsoft Entra ID d'une organisation. Cette technologie offre un accès par authentification unique aux ressources professionnelles ou scolaires comme OneDrive Entreprise, la messagerie professionnelle et d'autres applications métier.

Protection renforcée des informations d'identification
En plus d'adopter l'authentification sans mot de passe, les organisations peuvent renforcer la sécurité des informations d'identification des utilisateurs et des domaines dans Windows 11 avec Credential Guard et Remote Credential Guard.

Transparence et contrôles de la confidentialité
Des icônes bien visibles dans la barre système indiquent aux utilisateurs quand des ressources et des applications telles que les microphones et la localisation sont en cours d'utilisation. Une description de l'application et de son activité est présentée dans une info-bulle simple qui s'affiche lorsque vous passez le curseur de la souris sur une icône. Les applications peuvent également utiliser de nouvelles API Windows pour prendre en charge la fonctionnalité permettant de couper le son rapidement.

Sécurité Windows 11

Cloud

Microsoft Entra ID

Microsoft Entra ID (anciennement Azure Active Directory) est une solution complète de gestion des identités basée sur le Cloud qui permet de sécuriser l'accès aux applications, aux réseaux et aux autres ressources, et de se protéger contre les menaces.

Microsoft Intune

Microsoft Intune est une solution complète de gestion des points de terminaison qui permet de sécuriser, de déployer et de gérer les utilisateurs, les applications et les appareils. Intune regroupe des technologies telles que Microsoft Configuration Manager et Windows Autopilot pour simplifier le provisionnement, la gestion des configurations et les mises à jour logicielles à l'échelle de l'organisation.

Service Microsoft Azure Attestation

L'attestation à distance permet de s'assurer que les appareils sont conformes aux règles de sécurité et fonctionnent dans un état fiable avant d'être autorisés à accéder aux ressources. Microsoft Intune s'intègre au service Microsoft Azure Attestation pour vérifier de manière exhaustive l'intégrité des appareils Windows et connecte ces informations à l'accès conditionnel Microsoft Entra ID.

Dell, Microsoft et Intel investissent dans la sécurité continue des plateformes après leur commercialisation

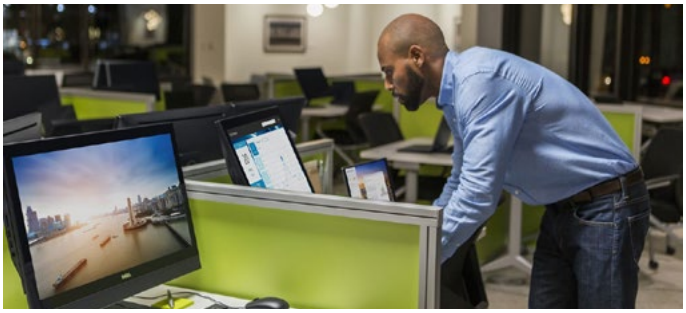
46,4 Mds $

de dépenses combinées de R&D en 2023*

* Macrotrends.net : dépenses de R&D en 2023 : 2,88 milliards de dollars pour Dell Technologies, 16,046 milliards de dollars pour Intel, 27,524 milliards de dollars pour Microsoft

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

Dans ce cadre, Intel finance l'un des meilleurs programmes de prime aux bugs du secteur, ayant permis de détecter 86 % des failles de sécurité externes en 2021. Les CVE (Common Vulnerabilities and Exposures) détectées via ce programme et par les chercheurs internes ou externes sont consignées dans une base de données publique. La société Intel est fière de sa position de leader ainsi que de ses capacités de surveillance et de création de rapports sur les failles de sécurité post-commercialisation. L'entreprise a consigné et corrigé plus de failles de sécurité potentielles que la plupart de ses concurrents, gardant une longueur d'avance sur les autres fabricants de puces, aucun n'égalant cet engagement envers la transparence et la sécurité des appareils.

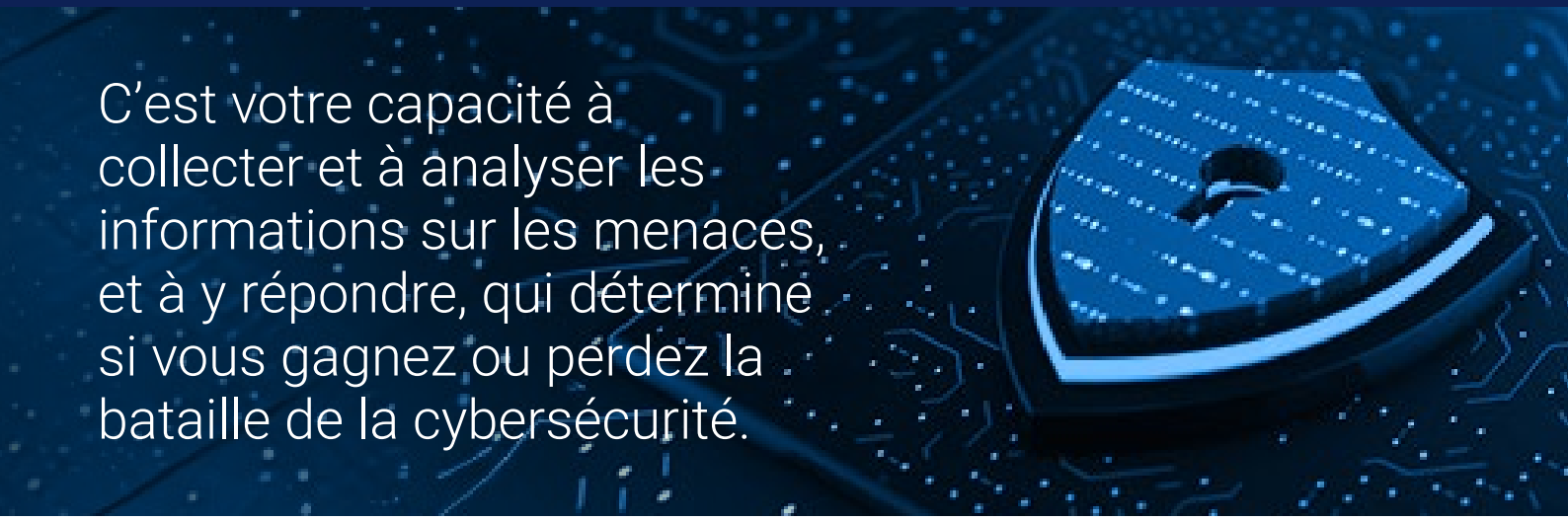


Pour gérer les CVE identifiées via ses programmes étendus, Intel publie régulièrement des mises à jour de plateforme Intel, pour tous les systèmes fonctionnant avec ses produits. Ce déploiement est un processus complet qui nécessite la validation de l'écosystème de partenaires Intel, y compris des CSP, des ISV, des OEM/ODM et des SI.

La coordination de la divulgation des failles de sécurité identifiées sur les produits et des réponses apportées est gérée par les équipes dédiées de réponse aux incidents de sécurité des produits de Dell et d'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, Microsoft 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.

Dell, Microsoft et Intel s'engagent à vous aider à sécuriser votre entreprise en pleine croissance



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. Ils savent que la plupart des solutions de sécurité se concentrent uniquement sur la sécurisation des logiciels. C'est pourquoi ils cherchent à compromettre la sécurité et à exploiter les failles des entreprises en se focalisant sur la chaîne logistique et sur les couches situées sous le système d'exploitation.

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.

Forts d'une collaboration de plusieurs décennies dans ce domaine, Dell, Microsoft et Intel ont gagné la confiance des clients en proposant des appareils professionnels parmi les plus sécurisés du secteur. Notre expertise commune et notre relation de codéveloppement nous permettent de garder une longueur d'avance sur les pirates grâce à nos recherches, à notre diligence et à nos innovations constantes. Leaders du marché des appareils professionnels depuis de nombreuses années, nous détectons et bloquons de plus en plus de menaces, en agissant sans cesse sur une énorme quantité de données et de télémesures, pour aider continuellement nos clients communs à activer et améliorer la sécurité de leurs appareils. Grands visionnaires, nos dirigeants se rencontrent régulièrement pour discuter de la sécurité globale actuelle et future, et des investissements nécessaires pour garantir que nos produits restent à la pointe de la cybersécurité professionnelle.

Dell, Microsoft et Intel offrent un niveau de sécurité de la chaîne logistique, des protections matérielles, des logiciels de protection contre les menaces avancées et un support continu de classe mondiale, pour fournir à votre entreprise des appareils professionnels non seulement efficaces, mais qui tiennent aussi vos données métier à distance du Dark Web. Contactez votre agent commercial Dell dès aujourd'hui pour en savoir plus sur nos programmes d'appareils professionnels et sur la façon dont nous pouvons vous aider à atteindre vos objectifs métier.

Cliquez ici pour

oublier les concessions

DELL Technologies

Windows 11

intel