Fournissez aux télétravailleurs une sécurité des terminaux assistée par le matériel avec Intel vPro®

La nouvelle plateforme Intel vPro® améliore l’expérience des employés en télétravail grâce à un environnement de sécurité renforcé.

Les principaux problèmes de sécurité liés au télétravail

Alors que le retour au bureau se poursuit, de nombreux collaborateurs préfèrent encore travailler à distance. Dans la mesure où le télétravail estompe la frontière entre l'informatique personnelle et professionnelle, en l'absence de directives claires et de garde-fous technologiques, les risques en matière de sécurité peuvent se multiplier :

- **Réseaux Wi-Fi non sécurisés.** Les personnes qui travaillent à partir de leur domicile, d'un hall d'hôtel ou d'un café peuvent télécharger des fichiers ou consulter des sites web non sécurisés, ce qui peut exposer le réseau de l'entreprise à toutes sortes d'attaques et d'acteurs malveillants. En outre, les réseaux Wi-Fi domestiques relient souvent plusieurs appareils (tels que des routeurs, des objets connectés [IoT] et des appareils électroménagers intelligents) qui peuvent être facilement piratés.

- **Absence de pare-feu.** Lorsque les collaborateurs sont en télétravail, leurs appareils ne sont pas toujours protégés par les dispositifs de sécurité réseau traditionnels tels que les VPN et les pare-feux, ce qui conduit de nombreuses entreprises à adopter des principes de sécurité de type « Zero Trust ».

- **Les attaques par hameçonnage.** Les e-mails ou les messages textuels peuvent facilement imiter les informations d'identification, dupant les télétravailleurs qui ne sont pas en mesure de vérifier la source de ces communications, ce qui peut conduire à des attaques par ransomware.

- **Appareils non sécurisés.** Les fuites de données et les violations de la confidentialité peuvent se produire lorsque les collaborateurs se trouvent dans des lieux publics, où les passants peuvent voir l'écran de leur ordinateur portable, ou lorsqu'ils laissent leur ordinateur portable sans surveillance ou dans leur voiture.

Afin de limiter ces risques, les entreprises doivent mettre en œuvre un ensemble de bonnes pratiques et de technologies, notamment des logiciels de sécurité. Mais les logiciels de sécurité peuvent ralentir les performances des ordinateurs portables actuels. Comment les entreprises peuvent-elles s'assurer que leurs ordinateurs sont dotés des fonctions de sécurité les plus récentes et qu'ils sont continuellement mis à jour pour faire face aux nouvelles menaces, sans compromettre l'expérience télétravail et la performance de l'ordinateur de leurs collaborateurs ?

Sommaire :

Intel vPro® : donner aux services IT les moyens de sécuriser et de gérer l'informatique à l'ère du travail hybride

Partout dans le monde, les entreprises ont besoin de PC spécialement conçus pour contrer les cybermenaces, stimuler la productivité des utilisateurs et même faire gagner du temps et de l'argent au service informatique. Intel vPro® est une base informatique professionnelle qui intègre des technologies matérielles et logicielles afin de permettre aux services IT de mieux contrôler les PC tout en maintenant la productivité de leurs utilisateurs. La plateforme Intel vPro® permet de sécuriser les PC et les données grâce à des protections matérielles améliorées, dès la mise en service.

De plus, grâce aux capacités de gestion à distance intégrées, les services informatiques peuvent aider les collaborateurs à travailler n'importe où, sans avoir à toucher à leur PC.[1] Intel vPro® contribue à maintenir les performances en télétravail, tout en offrant des protections matérielles multicouches exclusives.

Intel vPro® contribue à renforcer la sécurité à tous les niveaux de la pile, en prenant en charge les solutions d'identité fédérée telles que la sécurité de connexion renforcée Windows Hello et Microsoft Active Directory pour Windows Server. Il prend également en charge la couche de protection supérieure, à savoir les solutions de détection et de réponse des terminaux (EDR), telles que Microsoft Defender for Business et les intégrations de logiciels de sécurité OEM sous le système d'exploitation (OS).

91 % des centaines de personnes interrogées ont déclaré que les ordinateurs portables et de bureau équipés d'Intel vPro® fonctionnaient plus rapidement et mieux qu'auparavant.[2]

Renforcez la sécurité de vos parcs de PC

Intel vPro® aide à protéger les PC en tout lieu grâce à des fonctions de sécurité complètes, conçues pour des effectifs dispersés travaillant à distance. Avec Intel vPro®, les entreprises peuvent maintenir les appareils distants patchés et mis à jour avec les dispositifs de sécurité les plus récents. Intel travaille avec les solutions EDR leaders du marché afin que leurs capacités de sécurité soient plus efficaces, tout en offrant de meilleures performances et en préservant l'expérience utilisateur (UX).

Mieux encore, de nombreuses fonctionnalités sont prêtes à l'emploi, sans configuration nécessaire, ce qui simplifie la mise en œuvre pour les services informatiques.

Tableau 1. La plupart des fonctionnalités de sécurité de la plateforme Intel vPro® sont déjà mises en œuvre et ne nécessitent aucune configuration.

Technologie de sécurité Intel vPro®	Fonctionnalité prête à l'emploi
Intel® Hardware Shield	✓
Intel® Control-Flow Enforcement Technology (Intel® CET)	✓
Intel® Threat Detection Technology (Intel® TDT)	✓

Intel® Hardware Shield

Intel® Hardware Shield est une suite de technologies qui aide à protéger l'ensemble de la pile informatique. Contrairement aux logiciels de sécurité, Intel® Hardware Shield fournit des dispositifs de sécurité sous le système d'exploitation contre les attaques au niveau du firmware et du matériel. Il fournit également des mécanismes de protection des applications et des données avec un chiffrement de virtualisation accéléré par le matériel pour maintenir un niveau de performance optimal avec une détection et une protection avancées contre les menaces.

Quelle est l'importance de la sécurité sous le système d'exploitation ?

Les fonctions de sécurité sous le système d'exploitation permettent d'identifier les modifications non autorisées apportées au matériel et au firmware, empêchant ainsi l'injection de code malveillant grâce à la protection et à la visibilité de l'interface UEFI (Unified Extensible Firmware Interface). De nombreuses fonctionnalités Intel vPro® sont utilisées par les OEM dans leurs packages de sécurité sous le système d'exploitation.

Figure 1. Intel® Hardware Shield est intégré à la plateforme Intel vPro® pour aider à protéger les PC à chaque couche, y compris sous le système d'exploitation.

Intel® Threat Detection Technology (Intel® TDT)

Intel® TDT aide à prévenir les ransomwares, le cryptomining et même les attaques par analyse de la mémoire en recourant à la surveillance matérielle pour détecter et prévenir les activités malveillantes.

Intel® TDT est un ensemble de technologies qui exploite les capacités de télémétrie et d'accélération du matériel. Il recueille et analyse des données brutes pour permettre d'identifier les logiciels malveillants polymorphes, le cryptomining, les scripts sans fichier et d'autres attaques ciblées en temps réel, avec un impact minime sur l'utilisateur final.

Intel® TDT utilise l'heuristique de l'apprentissage automatique (ML) afin de réduire le nombre de faux positifs. Intel® TDT permet également d'améliorer les performances des solutions de détection et de réponse (EDR) qui surveillent en permanence les terminaux, telles que Microsoft Defender for Endpoint, CrowdStrike et Fidelis. Cela se fait en délestant les fonctions d'analyse de la mémoire du CPU vers un processeur graphique auxiliaire (GPU), ce qui rend les solutions logicielles de sécurité moins gourmandes en ressources et offre une meilleure UX globale aux collaborateurs.

Les solutions EDR peuvent accroître de 4 à 7 fois les performances d'analyse de la mémoire par rapport au processeur, ce qui permet une utilisation plus large de l'analyse en cas de besoin.[3] CrowdStrike a récemment introduit l'analyse accélérée de la mémoire Intel® TDT dans le capteur CrowdStrike Falcon pour Windows afin d'accroître la visibilité et de détecter les menaces en mémoire,[4] ajoutant ainsi une nouvelle couche de protection contre les menaces sans fichier, qui constituaient 71 % de l'ensemble des attaques détectées en 2022.[5]

Intel® TDT associé aux solutions EDR a permis de détecter jusqu'à 97 % des attaques connues et inconnues.[6]

Intel® Control-Flow Enforcement Technology (Intel® CET)

Intel® CET est une technologie d'atténuation avancée qui aide à se protéger contre les attaques par programmation orientée retour (return-oriented programming, ROP), programmation orientée saut (jump-oriented programming, JOP) et programmation orientée appel (call-oriented programming, COP). Ces attaques, qui sont courantes dans les applications connectées telles que les navigateurs et les outils de réunion, exploitent les vulnérabilités en matière de sécurité de la mémoire.

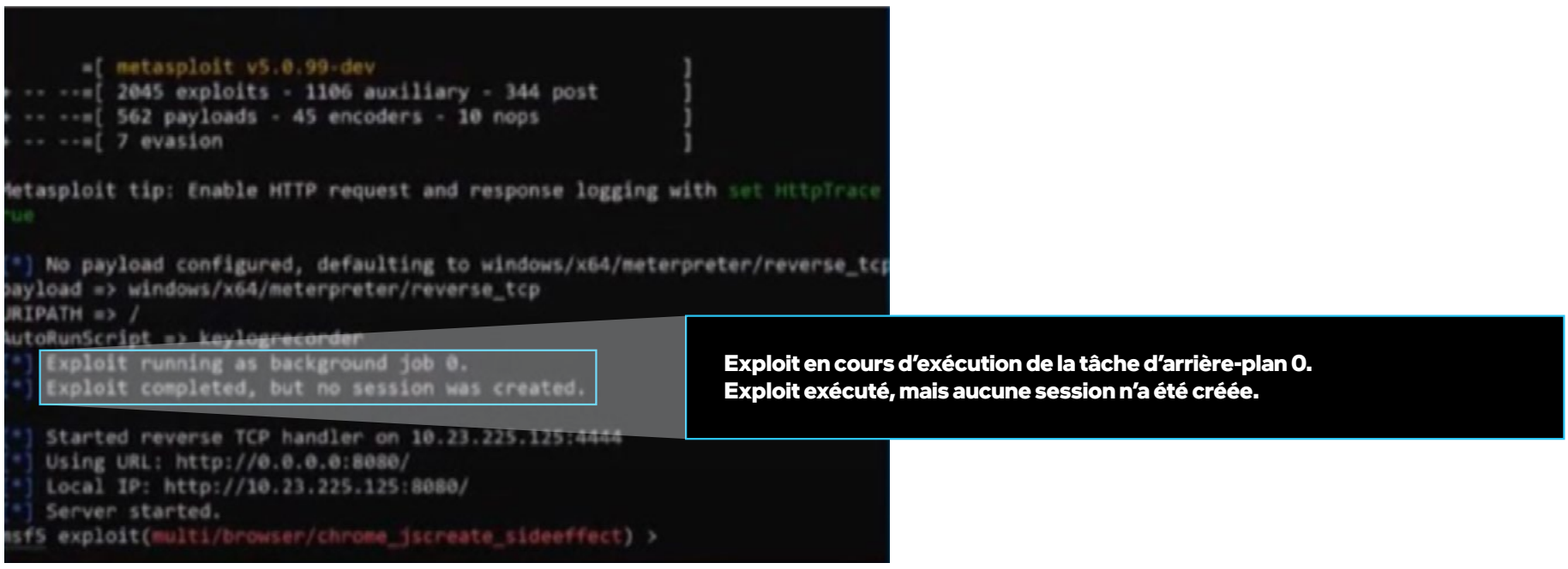


Figure 2. Intel® CET atténue les attaques qui peuvent être difficiles à détecter et faciles à exécuter, par exemple en cliquant sur un lien dans un navigateur

Les cyberattaquants peuvent utiliser des éléments de code existant s'exécutant sur la mémoire exécutable pour modifier les composants du système. Ces attaques sont particulièrement menaçantes parce qu'elles sont difficiles à détecter et qu'elles ont longtemps échappé aux solutions de sécurité purement logicielles.

Intel® CET complète les fonctions de sécurité logicielle pour contrer les attaques ROP/JOP/COP et offrir un niveau de sécurité plus élevé.[7] Selon un rapport, la mise en œuvre d'Intel® CET constitue « un grand pas en avant vers l'élimination de l'utilisation de ROP et d'autres techniques de détournement de flux de contrôle ».[7] Intel® CET a été adopté par Microsoft dans le système d'exploitation Windows, et il est inclus dans la version 20H1 de Windows 10 et les versions ultérieures. Il est également en cours de développement en vue de prendre en charge le noyau Linux, et il est activé pour les processus de navigation critiques en matière de sécurité pour Google Chrome et les navigateurs apparentés.[7]

Technologie de virtualisation Intel® (Intel® VT)

Le télétravail a favorisé l'essor de la sécurité basée sur la virtualisation (VBS). Les équipes informatiques peuvent activer les fonctions de sécurité Intel vPro® à l'aide de stratégies disponibles pour Windows 10 et 11. Intel® VT, disponible sur les PC dotés de la plateforme Intel vPro®, permet aux PC de prendre en charge les usages de partitionnement des activités, d'isolation de la charge de travail, de gestion intégrée, de migration des logiciels existants et de reprise après sinistre. La virtualisation permet aux entreprises d'exécuter plusieurs systèmes d'exploitation et applications dans des partitions indépendantes sur un seul serveur, ce qui permet d'isoler les charges de travail et de réduire les possibilités de propagation des logiciels malveillants. L'isolation est particulièrement importante dans le cadre du travail hybride, lorsque les collaborateurs utilisent leur PC à la fois pour un usage professionnel et personnel.

Isoler l'usage professionnel de l'usage personnel

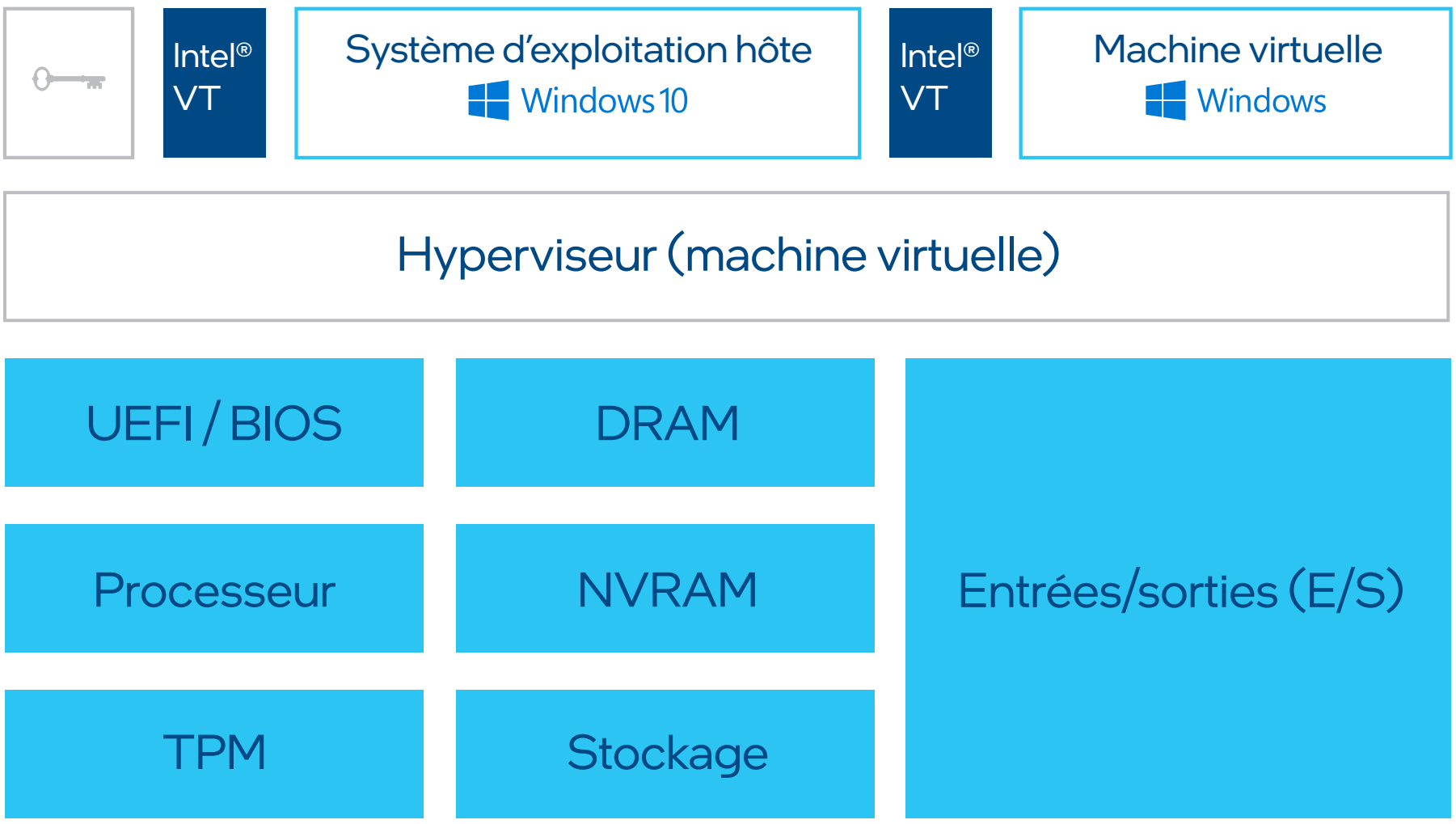


Figure 3. L'isolation des charges de travail, que permet Intel® VT sur la plateforme Intel vPro®, réduit la surface d'attaque et la capacité des logiciels malveillants à persister et à se propager à travers les ressources en prenant en charge la création de machines virtuelles (VM) isolées

Intel® Total Memory Encryption–Multi-Key (Intel® TME-MK)

Intel® TME-MK chiffre des portions de la mémoire système dans la DRAM, y compris les données du système d'exploitation et des applications, afin de renforcer la protection contre les attaques physiques par démarrage à froid. Cette technologie permet aux conteneurs/machines virtuelles d'utiliser plusieurs clés pour chiffrer différentes régions de la mémoire, ce qui renforce la sécurité en isolant les données.

Intel® Wi-Fi Proximity Sensing

Intel® Wi-Fi Proximity Sensing est une technologie qui contribue à simplifier la sécurité lorsque les collaborateurs à distance se trouvent dans des lieux publics ou des bureaux partagés. Cette technologie détecte les mouvements ambiants à proximité immédiate à l'aide de signaux sans fil. Lorsqu'un utilisateur s'éloigne de son ordinateur portable, la technologie détecte son mouvement et verrouille automatiquement l'appareil. Lorsque la personne revient travailler, la fonction « réveille » l'ordinateur et le rend prêt à l'emploi.

La technologie Intel® Wi-Fi Proximity Sensing peut détecter intelligemment quand il convient de verrouiller ou de réveiller l'ordinateur portable de l'utilisateur

Walk-away lock[8]

Le Wi-Fi détecte votre départ et verrouille l'ordinateur en quelques secondes

Sécuritaire

L'utilisateur oublie de verrouiller son PC → Vérification de la présence humaine → Verrouillage automatique du PC

Wake on approach[8]

Le Wi-Fi détecte votre retour et réveille l'ordinateur en quelques secondes

Pratique

Présence humaine détectée → Réveil automatique du PC → L'écran de connexion s'affiche

Intel® Remote Secure Erase (Intel® RSE)

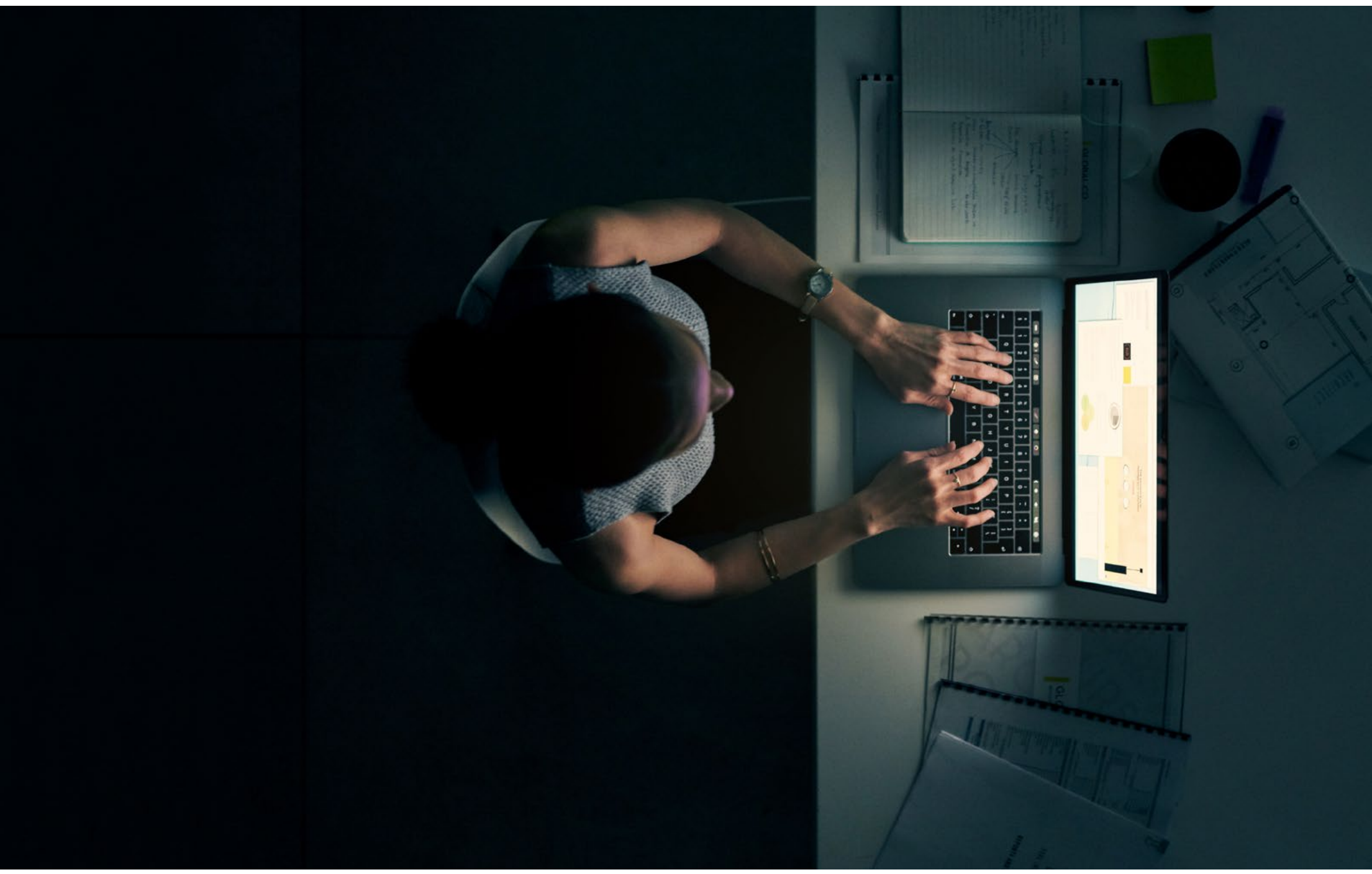
Lorsqu'un PC est mis hors service, réaffecté, renvoyé pour réparation ou perdu, les politiques de sécurité de l'information exigent souvent que les données soient « effacées » du disque. L'effacement peut être difficile et chronophage lorsqu'on travaille sur place, mais cela peut être pratiquement impossible à distance. Intel® RSE permet d'effacer les disques durs à distance en toute sécurité, grâce à la technologie d'administration active Intel® (Intel® AMT).[9]

Des mesures « Zero Trust » qui protègent les collaborateurs, où qu'ils travaillent

Les dispositifs de sécurité combinés de la plateforme Intel vPro® peuvent contribuer à réduire la surface d'attaque des PC grâce à plusieurs contre-mesures anti-attaque matérielle. Intel vPro® est conçu pour prendre en charge le travail à distance grâce à des principes de sécurité « Zero Trust », garantissant l'authentification des utilisateurs et l'évaluation de l'état de chaque appareil et de l'accès aux applications.

L'efficacité des fonctions de sécurité renforcées d'Intel vPro® est attestée par des études. Les entreprises de plus de 5 000 employés qui utilisent principalement des appareils basés sur la plateforme Intel vPro® ont signalé moins de violations de sécurité par an, en moyenne, par rapport à leurs homologues ne disposant pas d'Intel vPro®.[10]

- Les entreprises n'utilisant pas les technologies Intel® ont signalé en moyenne 3,9 violations matérielles par an, contre 2,8 violations matérielles annuelles pour les entreprises utilisant les technologies Intel®.[11]
- Les entreprises utilisant les technologies Intel® étaient moins susceptibles de subir des violations dues à des attaques externes, des incidents internes, des attaques ou des incidents impliquant des fournisseurs tiers, et des actifs perdus ou volés.[12]
- 92 % des professionnels de l'informatique interrogés ont constaté que leurs ordinateurs portables et de bureau étaient plus sécurisés qu'auparavant après avoir adopté Intel vPro®.[2]
- L'utilisation exhaustive de toutes les fonctionnalités de sécurité matérielle d'Intel vPro® peut réduire la surface d'attaque jusqu'à 70 %.[7]



Optimisez la sécurité et les performances

Les appareils basés sur la plateforme Intel vPro® sont spécialement conçus pour répondre aux besoins du télétravail et des charges de travail de sécurité. À chaque nouvelle génération, Intel vPro® continue de mettre l'accent sur l'innovation en matière de sécurité, en s'efforçant constamment de permettre aux entreprises d'avoir une longueur d'avance sur les acteurs malveillants. Ce qui a commencé par une protection de pointe sous le système d'exploitation a évolué vers les processeurs Intel® Core™ de 13e génération actuels, qui peuvent renforcer la sécurité au-dessus du système d'exploitation, évitant ainsi aux entreprises de subir des violations et leur permettant de récupérer de précieuses heures de travail informatique.

En optimisant les capacités et les fonctions de sécurité qui résident habituellement derrière les pare-feu de l'entreprise, Intel vPro® offre la sécurité la plus complète pour votre entreprise.[13]

Améliorez l'expérience employé et la sécurité pour l'informatique d'entreprise d'aujourd'hui

Apprenez-en davantage sur les nouveaux PC équipés de la technologie Intel vPro® et découvrez les avantages considérables dont vos collaborateurs et votre entreprise peuvent bénéficier en matière de sécurité.

[1] Intel® Standard Manageability et Intel® AMT prennent en charge les capacités hors bande à distance sur les PC Windows fournis, mais seule la plateforme Intel vPro® Enterprise pour Windows avec Intel® AMT prend en charge le contrôle du clavier, de l'écran et de la souris (KVM) à distance.

[2] Sur la base d'une enquête menée auprès de 416 ITDM dans des entreprises du monde entier utilisant des plateformes Intel vPro® aux États-Unis, au Royaume-Uni, en Allemagne, au Japon et en Chine. 92 % des répondants ont répondu « d'accord » ou « tout à fait d'accord ». Vos résultats peuvent varier. Source : Forrester Consulting. « Total Economic Impact™ et retour sur investissement de la plateforme Intel vPro® ». Commanditée par Intel. Janvier 2021. intel.fr/content/www/fr/fr/business/enterprise-computers/resources/vpro-platform-tei-case-study-2021.html.

[3] Estimation basée sur le délestage de l'analyse de la mémoire vers le processeur graphique intégré via l'API Intel® TDT, qui se traduit par une accélération de 3 à 7 fois par rapport aux méthodes d'analyse du processeur, comme décrit dans le blog de CrowdStrike. Reportez-vous à intel.com/Performance-vPro pour plus de détails.

[4] CrowdStrike. « CrowdStrike Falcon® améliore la détection des attaques sans fichier grâce à la fonction d'analyse accélérée de la mémoire d'Intel » (« CrowdStrike Falcon® Enhances Fileless Attack Detection with Intel® Accelerated Memory Scanning Feature »). Mars 2022. crowdstrike.com/blog/falcon-enhances-fileless-attack-detection-with-accelerated-memory-scanning/.

[5] CrowdStrike. « Rapport sur les menaces mondiales 2023 » (« 2023 Global Threat Report »). 2023. https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf.

[6] SE Labs. « Sécurité avancée de l'entreprise (Ransomware) : Intel » (« Enterprise Advanced Security (Ransomware): Intel ». Février 2023 https://selabs.uk/reports/enterprise-advanced-security-ransomware-intel-threat-detection-technology-2023-02/.

[7] IOActive. « Étude sur la surface d'attaque des processeurs Intel® Core™ de 13e génération » (« 13th Generation Intel® Core™ Attack Surface Study »). Commanditée par Intel. Mars 2023. intel.com/content/dam/www/central-libraries/us/en/documents/2023-03/ioactive-intel-13th-generation-attack-surface-study-summary-report.pdf.

[8] Les fonctions « Walk-away lock » et « Wake on approach » sont prises en charge par Windows 11. La technologie Intel® Wi-Fi-Proximity Sensing n'est actuellement disponible que sur les modèles Intel® Evo™ et Intel vPro® éligibles sur les PC Windows.

[9] Vérifiez auprès de votre fabricant OEM qu'Intel® RSE est pris en charge par vos appareils.

[10] Forrester Consulting. « Total Economic Impact™ des fonctionnalités de sécurité matérielles d'Intel vPro® ». Commanditée par Intel. Septembre 2022. intel.fr/content/www/fr/fr/business/enterprise-computers/resources/impact-of-vpro-hardware-enabled-security-paper.html.

[11] Sur la base de 719 décideurs informatiques (ITDM) du monde entier ayant une responsabilité dans la gestion des terminaux et ayant répondu à la question « Combien de violations de sécurité se sont produites pour [tel appareil] avec [tel processeur] dans votre entreprise au cours de l'année écoulée ? » Source : Étude commandée par Intel et conduite par Forrester Consulting en 2021.

[12] Sur la base de 239 ITDM du monde entier ayant une responsabilité dans la gestion des terminaux et ayant répondu à la question « Vous avez indiqué précédemment que votre entreprise a été confrontée à une violation au cours des 12 derniers mois. Comment cette violation a-t-elle pu se produire au sein de votre entreprise ? » Source : Étude commandée par Intel et conduite par Forrester Consulting en septembre 2022.

[13] Selon les données disponibles en mars 2023, sur la base de la combinaison inégalée de dispositifs de sécurité en amont et en aval du système d'exploitation, de protections des applications et des données et de protections avancées contre les menaces qu'offre Intel vPro® aux entreprises de toutes tailles, ainsi que l'approche orientée sécurité d'Intel en matière de conception, de fabrication et de support des produits. Tous les PC professionnels conçus sur la plateforme Intel vPro® ont fait l'objet d'une validation selon des critères rigoureux, notamment des fonctions de sécurité matérielle uniques. Plus de détails sur intel.com/Performance-vPro. Vos résultats peuvent varier.

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

Les résultats de performances s'appuient sur des tests à la date telle que décrit dans les configurations et peuvent ne pas refléter la totalité des mises à jour disponibles publiquement. Pour obtenir plus de détails, veuillez lire les informations de configuration.

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

Aucun produit ou composant ne peut être totalement sécurisé en toutes circonstances.
Vos coûts et résultats peuvent varier.

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

Imprimé aux États-Unis 0823/RR/PRW/PDF Pensez à recycler 356510-001US