

► EXPLORATION

Dell Trusted Workspace



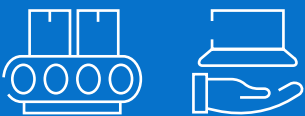
Protégez le travail en tout lieu

avec des solutions de défense matérielles et logicielles conçues pour l'ère du Cloud actuelle.

Le travail hybride a exposé les organisations à de nouveaux vecteurs d'attaque. Face aux techniques de cybercriminalité toujours plus sophistiquées, plusieurs couches de défense protégeant l'appareil, le réseau et le Cloud sont nécessaires pour sécuriser efficacement les points de terminaison.

Réduisez la surface d'attaque et gardez une longueur d'avance sur les menaces modernes avec une gamme complète de solutions de protection matérielles et logicielles.

[En savoir plus sur la gamme →](#)



[Les ordinateurs tout-en-un parmi les plus sécurisés au monde¹ →](#)



[Logiciels pour améliorer la sécurité de tous les parcs →](#)

Plusieurs couches de défense



Sécurité logicielle

complémentaire

Couche sur la protection contre les menaces avancées avec des logiciels d'un écosystème de partenaires sélectionnés avec soin. Tirez parti des avantages et économies associés au regroupement des achats de solutions de sécurité.

Sécurité matérielle et des firmwares

intégrée

Prévenez et détectez les attaques de base avec les PC professionnels les plus sécurisés du marché¹. Des défenses renforcées au niveau du BIOS/firmware et du matériel protègent l'appareil pendant son utilisation.

Seule la société Dell intègre les données de télémétrie des PC avec des logiciels leaders sur le marché pour améliorer la sécurité à l'échelle du parc informatique¹

Sécurité intrinsèque

de la chaîne logistique

Travaillez sereinement en sachant que votre appareil est sécurisé dès le premier démarrage. Une conception, un développement et des tests de PC sécurisés contribuent à réduire le risque de failles de sécurité produit. Des contrôles rigoureux de la chaîne logistique réduisent le risque de falsification des produits.



Prévenez et détectez les menaces, puis répondez-y, où qu'elles se produisent

Dell SafeGuard and Response

Dell SafeData



Protégez-vous contre l'évolution des menaces

Dell SafeBIOS

Dell SafeID

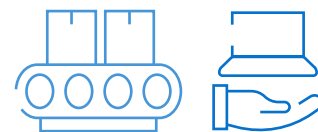


Intégrité physique du matériel assurée lors de la livraison

Dell SafeSupply Chain

Dell Trusted Workspace : sécurité intrinsèque et intégrée

PC professionnels les plus sécurisés au monde¹



Protection assurée dès le premier démarrage

Des contrôles rigoureux et de pointe de la chaîne logistique et des modules complémentaires en option, comme **Secured Component Verification**, une exclusivité Dell, garantissent l'intégrité du PC. [En savoir plus](#) →

Vérification de l'intégrité du firmware

La **vérification du firmware**, une fonctionnalité de sécurité matérielle proposée en exclusivité par Dell sur les processeurs Intel, protège les systèmes contre les accès non autorisés et la falsification de firmware avec un niveau de privilège élevé. [En savoir plus](#) →

Sécurisez les informations d'identification des utilisateurs finaux

Vérifiez l'accès des utilisateurs avec la solution **SafeID**, exclusive de Dell, une puce de sécurité dédiée qui rend les informations d'identification de l'utilisateur indétectables par les logiciels malveillants. [En savoir plus](#) →

Maintien de l'intégrité du BIOS

Détectez et neutralisez les menaces avec **SafeBIOS**, l'outil Dell de vérification du BIOS. Évaluez un BIOS corrompu, réparez-le et obtenez des informations pour réduire l'exposition aux menaces futures. [En savoir plus](#) →

Repérez les bombes à retardement

Les **indicateurs d'attaque**, une fonctionnalité d'alerte précoce proposée uniquement par Dell, analyse les menaces basées sur le comportement avant qu'elles ne puissent causer des dommages. [En savoir plus](#) →

Détectez les failles de sécurité connues

La fonction de **détection des CVE** (Common Vulnerabilities and Exposures) exclusive à Dell surveille les failles de sécurité du BIOS signalées publiquement et recommande des mises à jour pour atténuer les risques. [En savoir plus](#) →



Leadership dans le secteur validé par Principled Technologies

Amélioration de la sécurité avec les données de télémétrie des PC

Comblez les failles de sécurité IT avec l'**application Dell Trusted Device**. Seule la société Dell intègre les données de télémétrie des PC avec des logiciels leaders sur le marché pour améliorer la sécurité à l'échelle du parc informatique¹. [En savoir plus](#) →

Explorer les appareils Dell Trusted Device



[Latitude](#) →



[OptiPlex](#) →



[Precision](#) →

Dell Trusted Workspace Sécurité complémentaire

Logiciels pour améliorer la sécurité de tous les parcs



Contrearez les cyberattaques avancées avec [Dell SafeGuard and Response](#)

Prévenez, détectez et contrez les menaces, où qu'elles se produisent. L'intelligence artificielle et l'apprentissage automatique détectent et bloquent proactivement les attaques sur les points de terminaison, tandis que les experts de la sécurité aident à traquer et corriger les menaces identifiées sur le point de terminaison, sur le réseau et dans le Cloud.

Partenaires

[CrowdStrike Falcon®](#) →

[Secureworks® Taegis™ XDR](#) →

Protégez les données sur les appareils et dans le Cloud avec [Dell SafeData](#)

Sécurisez la collaboration entre utilisateurs, où qu'ils soient. Netskope adopte une approche de la sécurité et des accès au Cloud centrée sur les données, protégeant les données et les utilisateurs où qu'ils soient, tandis que la solution Absolute offre visibilité, protection et persistance à l'équipe IT au-delà du pare-feu de l'entreprise.

Partenaires

Réparation automatique des points de terminaison, applications et réseaux avec [Absolute](#) →

Explorez les solutions Security Service Edge avec [Netskope](#) →

Explorer Dell Security Services

Avec Dell, les clients peuvent autogérer la sécurité ou confier à des experts le soin de la gérer pour eux. Adoptez notre solution SecOps à 360° entièrement gérée pour prévenir les menaces de sécurité dans l'environnement IT, y répondre et restaurer les systèmes en cas de violation.

[En savoir plus sur Managed Detection and Response Pro Plus](#) →



Dell Trusted Workspace : sécurité assistée par matériel

Sécurité intégrée

Les cybermenaces en constante évolution déjouent les défenses exclusivement logicielles. Contribuez à réduire la surface d'attaque des points de terminaison avec des **protections assistées par matériel**.

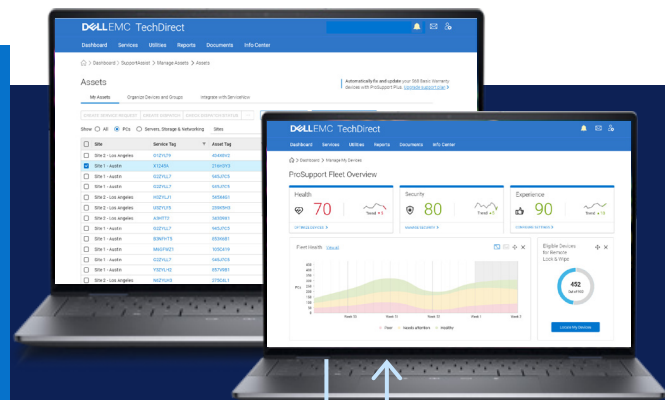
Pour se protéger des menaces actuelles, les défenses matérielles et logicielles doivent s'unir. C'est là que Dell entre en jeu. Nous travaillons avec des partenaires de sécurité leaders sur le marché, combinant une télémétrie riche au niveau des appareils et une détection des menaces de pointe afin d'améliorer la sécurité de votre flotte.

- ✓ Réduction de la surface d'attaque
- ✓ Amélioration de la détection des menaces
- ✓ Maintien de la confiance dans les appareils
- ✓ Consolidation des fournisseurs

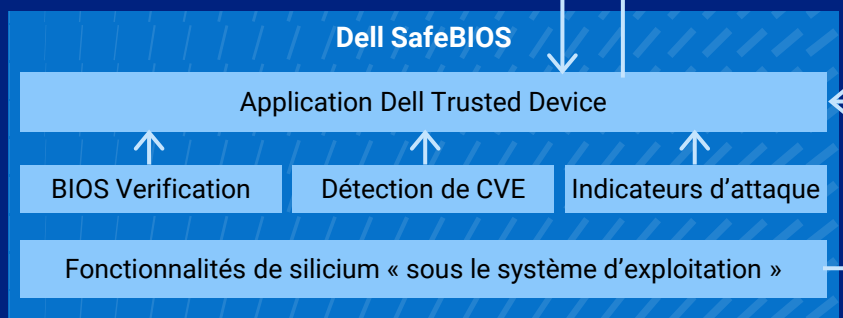
Sécurité logicielle complémentaire

Le système d'exploitation

Dell est la seule entreprise à intégrer la télémétrie des PC à des logiciels leaders sur le marché pour améliorer la sécurité à l'échelle du parc informatique^{1,2}



Sécurité matérielle et des firmwares intégrée



Sécurité intrinsèque de la chaîne logistique



Travaillez partout en toute sécurité avec **Dell Trusted Workspace.**



Sécurité matérielle
intrinsèque et intégrée



Sécurité logicielle
complémentaire

Réduisez la surface
d'attaque et
améliorez la
cyberrésilience sur
le long-terme avec
plusieurs couches
de défense.

Venez-nous voir

dell.com/endpoint-security

Nous contacter

global.security.sales@dell.com

En savoir plus

[Blogs sur la sécurité des points de terminaison →](#)

Prenez part à la conversation

[LinkedIn /delltechnologies](#)

[X @delltech](#)

Sources et mentions légales

¹D'après une analyse interne réalisée par Dell en 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. Validé par Principled Technologies. [Comparaison des fonctions de sécurité](#), avril 2024. ²Intégrations disponibles pour CrowdStrike Falcon Insight XDR.