Anatomie d'un appareil de confiance

Découvrez ce qui fait des PC professionnels Dell équipés de la plateforme Intel vPro® les PC professionnels les plus sécurisés au monde[1]

MENACES ET DÉFIS

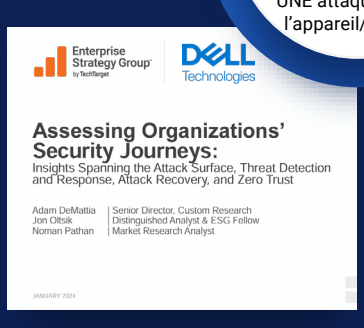
Les vecteurs d'attaque émergents visent désormais sous le système d'exploitation, créant de nouveaux risques

Les points de terminaison sont une porte d'entrée majeure pour les violations. Avec l'expansion de la surface d'attaque liée au travail hybride, les inquiétudes liées à la sécurité des appareils ont augmenté ces dernières années. Les pirates ciblent de plus en plus la chaîne logistique, ainsi que les rootkits et autres failles de sécurité du firmware, qui échappent en grande partie aux logiciels EDR existants.

Les menaces ciblant les appareils ont été multipliées par 1,5 depuis 2020.[2]

69 %

des organisations signalent au moins UNE attaque ciblant l'appareil/le BIOS[2]



Principaux critères d'évaluation lors de l'achat de nouveaux PC :

- Détection automatisée des événements du BIOS[3]
- Gestion des configurations à haut risque[3]

Pour lutter contre les menaces modernes, les appareils doivent être conçus de manière sécurisée et dotés d'une sécurité intégrée pour détecter et contrer les attaques.

LA SOLUTION

Prévenir et détecter les attaques de base, savoir réagir et être en mesure de s'en remettre en s'appuyant sur les PC professionnels les plus sécurisés[1]

La sécurité d'un parc est proportionnelle à celle de ses différents PC. Mais qu'est-ce qui fait qu'un appareil est fiable et sécurisé ? La visibilité et la facilité d'action. L'accès à davantage de données permet une prise de décision éclairée, ce qui contribue à identifier les menaces émergentes, aussi sournoises soient-elles. L'automatisation permet une résolution plus rapide des problèmes potentiels.

Les défenses au niveau du matériel et du firmware des PC professionnels Dell reposant sur la plateforme Intel vPro ont été pensées pour offrir cette visibilité et cette facilité d'action à votre parc.

Anatomie d'un appareil de confiance Dell

Avantages

- Garantissez la sécurité dès le premier démarrage avec des contrôles rigoureux de la chaîne logistique
- Préservez l'intégrité du BIOS avec une visibilité approfondie au niveau du firmware
- Protégez l'identité de l'utilisateur final contre les logiciels malveillants qui cherchent à voler ses identifiants
- Enrichissez les données au niveau du système d'exploitation avec la télémétrie « sous le système d'exploitation » pour accélérer la détection, la réponse et les mesures correctives

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 informatique.[1] En savoir plus →

Maintien de l'intégrité du BIOS

Détectez et neutralisez les menaces avec l'outil Dell de vérification du BIOS. Évaluez un BIOS corrompu, réparez-le et obtenez des informations qui réduiront l'exposition aux menaces futures avec la capture d'images du BIOS. [1] En savoir plus →

Repérez les bombes à retardement

Indicateurs d'attaque, une fonctionnalité d'alerte précoce proposée uniquement par Dell, analyse les menaces basées sur le comportement avant qu'elles ne puissent vous causer du tort.[1] 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. [1]

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.[1] 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[1] En savoir plus →

Garantissez la sécurité tout au long du cycle de vie des PC

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, à la livraison et sur toute sa durée de vie.[1] En savoir plus →

LEADER DU SECTEUR

Aucun fabricant de PC n'offre autant de visibilité sur le BIOS que Dell. [1]

Découvrez comment rassurer les clients face aux menaces modernes.

En savoir plus →


A Principled Technologies report: In-depth research. Real-world value.

A comparison of security features in Dell, HP, and Lenovo PC systems

Approach

Dell™ commissioned Principled Technologies to investigate 10 security features in the PC security and system management space:

- Support for monitoring solutions
- BIOS security and protection features
  - Platform integrity validation
  - Device integrity validation via off-site measurements
  - Component integrity validation for Intel® Management Engine (ME) via off-site measurements
  - BIOS image capture for analysis
  - Built-in hardware cache for monitoring BIOS changes with security information and event management (SIEM) integration
- Microsoft Intune management
  - BIOS setting management integrations for Intune
  - BIOS access management security enhancements for Intune
- Remote management
  - Intel vPro® remote management
  - PC management using cellular data

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original

Explorer les appareils Dell Trusted Device

Latitude →

OptiPlex →

Precision →

Travaillez partout en toute sécurité avec Dell Trusted Workspace

Sécurité matérielle intrinsèque et intégrée

Sécurité logicielle complémentaire

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
delltechnologies @delltech

Sources et mentions légales

[1]D'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.

[2]Source : Futurum Group, Endpoint Security Trends, 2023.

[3]Source : Enterprise Strategy Group, une division de TechTarget, étude personnalisée réalisée à la demande de Dell Technologies, *Assessing Organizations' Security Journeys*, novembre 2023.