DELL Technologies

Comment lutter contre les cybermenaces modernes

grâce à une sécurité et une gestion intégrées des points de terminaison

CROWDSTRIKE intel ABSOLUTE®

DELL Technologies

Synthèse

Les nouveaux vecteurs d'attaque génèrent de nouveaux risques. Gardez une longueur d'avance sur les menaces modernes qui pèsent sur les points de terminaison en utilisant plusieurs couches de défense coordonnées. Découvrez comment la télémétrie matérielle peut s'intégrer aux logiciels pour améliorer la sécurité et faciliter la gestion dans l'ensemble du parc. Stoppez plus rapidement les attaques, adoptez les principes Zero-Trust et innovez en toute sécurité grâce à des appareils et des solutions faciles à gérer.

Sommaire

Le paysage des menaces

Étude de cas

En 2023, Eclypsium a découvert une faille dans le firmware de cartes mères vendues par un fabricant taïwanais. Des chercheurs ont constaté que l'implémentation du code destiné à mettre à jour le firmware n'était pas sécurisée et pouvait permettre de pirater le mécanisme pour installer des logiciels malveillants.

Cette découverte était particulièrement alarmante pour plusieurs raisons

- Les clients ont été exposés à des risques en raison d'une vulnérabilité du firmware.
- La vulnérabilité était localisée dans une zone de l'appareil où il est typiquement difficile de détecter les menaces.
- Elle pouvait être utilisée pour lancer une attaque à distance en contournant la vérification des informations d'identification.

Dans l'actualité…

Le paysage des menaces

Implications.

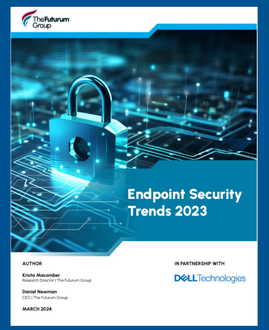
Voici un type d'attaque qui constitue une préoccupation majeure pour les équipes en charge de l'IT et de la sécurité :

les attaques basées sur les appareils.

Ces attaques sophistiquées et malveillantes peuvent permettre aux pirates d'obtenir un accès privilégié. Qui plus est, nombre d'entre elles peuvent désactiver les protections purement logicielles classiques, comme les antivirus, sans être détectées.

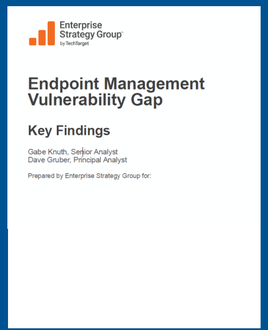
Selon une récente enquête mondiale menée auprès de professionnels de l'IT et de la sécurité[1], lorsque les entreprises recherchent de nouveaux équipements, la qualité constitue l'un de leurs principaux critères d'évaluation :

Automatisation de la détection des événements de firmware du BIOS



69 % des entreprises ont signalé au moins UNE attaque au niveau d'un appareil au cours des douze derniers mois. C'est 1,5 fois plus que dans l'étude de 2020[2] !

Configurations à haut risque



Plus de 75 % des entreprises indiquent avoir subi au moins une cyberattaque causée par un point de terminaison inconnu, non géré ou mal géré[3].

Défis

Qu’est-ce qui fait d’un appareil une cible facile ?

Visibilité

Ces attaques sont difficiles à repérer, car elles sont exécutées sur une partie de l’appareil qui n’est typiquement pas assez visible et observable.

Capacité d’action

Les entreprises disposent souvent de dizaines d’outils qui fonctionnent en silos. Par conséquent, si une attaque est détectée, la mise en œuvre rapide de mesures correctives représente un défi majeur, impliquant un travail manuel considérable.

Solution

Visibilité

Capacité d'action

Dell est l'un des plus grands fournisseurs de technologies au monde, et en tant que tel, l'entreprise se préoccupe beaucoup de la sécurité. C'est pourquoi **nous fabriquons nos PC professionnels en mettant dès le départ l'accent sur la visibilité et la capacité d'action**. Cela donne toute latitude aux équipes chargées des opérations IT et de sécurité.

Nos PC professionnels sont dotés de **fonctions de sécurité intégrées uniques**, telles que la vérification du BIOS[4] et les indicateurs d'attaque[4], qui permettent de détecter les menaces avant qu'elles ne causent des dommages. Ces détections sont rendues visibles grâce à la **télémétrie des appareils proposée uniquement par Dell**[4]. Lorsqu'un PC professionnel Dell équipé d'Intel vPro® détecte une menace potentielle au niveau de l'appareil, il peut l'envoyer au système d'exploitation pour accélérer et optimiser l'investigation et la réponse

Leadership du secteur

Dell propose les ordinateurs professionnels les plus sécurisés au monde[4]

Découvrez comment rassurer les clients face aux menaces modernes.

Lisez l'étude de Principled Technologies sur la sécurité des appareils →


Principled Technologies®

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 equipment manufacturers (OEMs): Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device application.

In this report, we indicate that an OEM supports a given feature if its published materials mention that feature is present. We have done our best to determine which features each OEM supports, using a variety of search terms and brand-specific phrasing to locate features. Some of the features we mark as being absent might be present but not covered in the OEM marketing or documentation. It is also possible that, despite our best efforts, we missed or overlooked some features that the OEM marketing or documentation does address.

We completed no hands-on validation of any of the features we discuss below. Therefore, we cannot verify the functionality, scope, or reliability of these features. We do not cover system requirements or any licensing, services, or additional hardware or software that might be necessary to use the features.

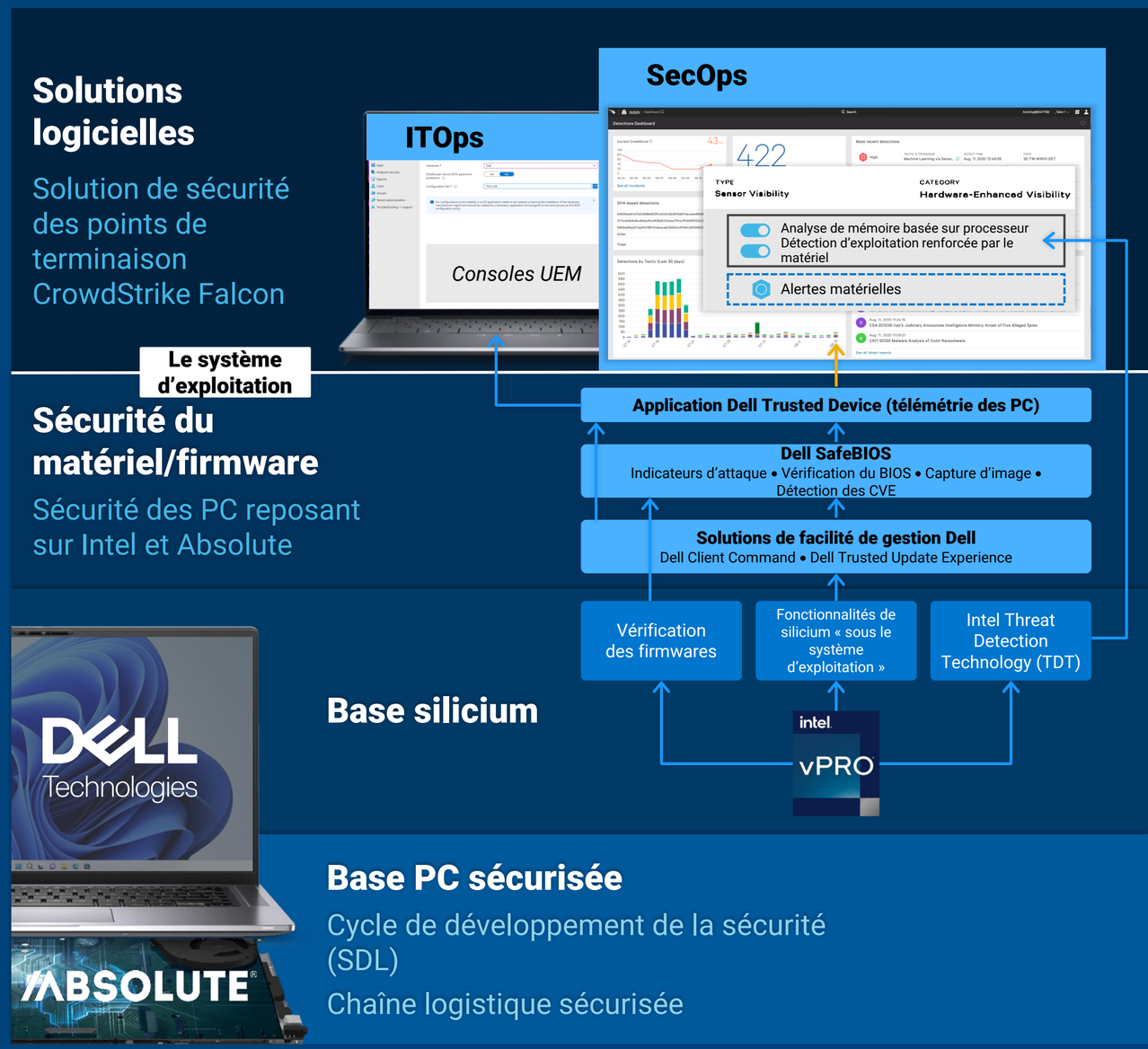
Solution

Luttez contre les menaces en coordonnant la sécurité et la gestion

Dell et notre écosystème de partenaires connectés œuvrent pour améliorer la visibilité et la capacité d'action au niveau de l'espace de travail. Celle-ci inclut :

- Sécurité de la chaîne logistique et mécanismes de défense intégrés au niveau du matériel et du firmware de Dell
- Protections de base « sous le système d'exploitation » intégrées dans le silicium d'Intel
- Facilité de gestion via les consoles de gestion unifiée des points de terminaison et Dell
- Protection contre les menaces avancées au niveau des points de terminaison, des réseaux et du Cloud, assurée par des partenaires tels que CrowdStrike et Absolute

L'écosystème utilise la télémétrie des PC comme connecteur, ce qui permet de combler l'écart entre les solutions IT et de sécurité, où des menaces peuvent s'insinuer. Non seulement cette approche aide à éviter les attaques, mais elle permet également de les détecter, d'y répondre, de les surmonter et d'appliquer les mesures correctives nécessaires.



Cas d’utilisation et contre-mesures

Pour illustrer de quelle manière la sécurité et la gestion intégrée permettent d’améliorer la cyberrésilience, nous allons examiner deux cas d’utilisation, avec les scénarios d’attaque et les contre-mesures.

Premièrement, penchons-nous sur une attaque au niveau du firmware du BIOS. Nous voyons ici comment peut se dérouler la cyberchaîne de frappe[5] d’une attaque par rétrogradation du BIOS.

Attaque par rétrogradation du BIOS

Accès initial : réplication par le biais de supports amovibles et hameçonnage

Étape 1a

Un employé malveillant exploite une vulnérabilité existante du BIOS pour voler à distance des informations d’identification du système d’exploitation. Il pirate l’appareil et rétrograde le BIOS.

Étape 1b

Il lance une attaque d’hameçonnage ciblé, en volant un jeton de session lorsqu’un administrateur s’authentifie par mégarde sur un site malveillant.

Étape 2

Accès aux informations d’identification

Le pirate maintient un accès continu en créant des comptes administrateur supplémentaires et se déplace sur le réseau.

Étape 3

Déplacement latéral

Le pirate mappe le réseau et localise les serveurs de gestion du système.

Étape 4

Exfiltration

Le pirate exfiltre les données par le biais d’un service Web.

Cas d’utilisation et contre-mesures

Contre-mesures des rétrogradations du BIOS

Les pirates s’insinuent dans le réseau plus rapidement que jamais. Selon le Global Threat Report de CrowdStrike, le délai moyen d’intrusion lors d’une cyberattaque (le temps nécessaire pour s’introduire dans un système et se déplacer latéralement) est passé à 62 minutes en 2023, contre 84 minutes en 2022. Le délai d’intrusion le plus rapide a été de seulement 2 minutes et 7 secondes[6] !

Voici comment Dell et ses partenaires Intel® et CrowdStrike vous aident à détecter et à repousser une attaque par rétrogradation du BIOS tout au long de la chaîne de frappe grâce à la sécurité assistée par matériel.

Prévenir | **Détecter et répondre** | **Surmonter et corriger**

Sécuriser la chaîne logistique : des contrôles rigoureux protègent les PC depuis la conception et le développement jusqu’à la livraison, en passant par l’approvisionnement et l’assemblage. Dell et Intel travaillent sans relâche pour s’assurer que leurs produits sont développés de manière à limiter le risque d’exposition aux vulnérabilités et aux tentatives de falsification tout au long du cycle de vie du produit.




Security	Integrity	Quality	Resilience
• Secure development lifecycle • Software partners securely onboarded • Information exchange with partners securely • Quality Process Audit • Separation of Duties • Least Privilege Access	• Supplier accountability • Supplier due diligence • Piece-Part Identification • SAFECode • US Exec Order 14028 SBOM -SPDX	• Counterfeit prevention & detection • Enhanced manufacturing security program • Enterprise code signing • Secured Component Verification • Freight Tracking	• Silicon Root of Trust • Platform Firmware Resiliency Guidelines • BIOS Protection Guidelines • Built-in Supplier Redundancy

Cas d’utilisation et contre-mesures

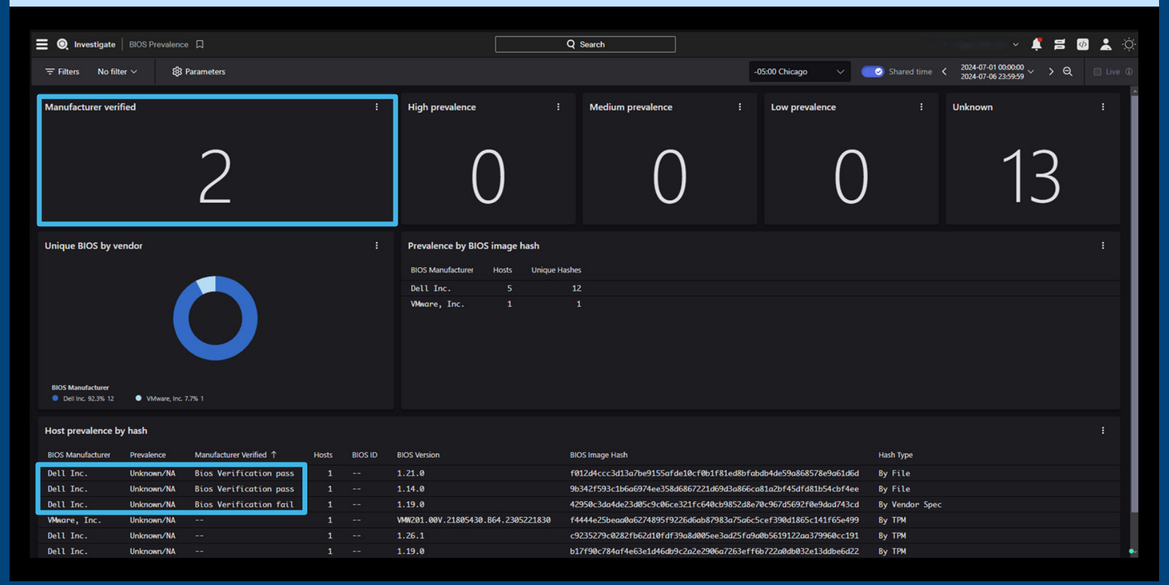
Contre-mesures des rétrogradations du BIOS

Les pirates s’insinuent dans le réseau plus rapidement que jamais. Selon le Global Threat Report de CrowdStrike, le délai moyen d’intrusion lors d’une cyberattaque (le temps nécessaire pour s’introduire dans un système et se déplacer latéralement) est passé à 62 minutes en 2023, contre 84 minutes en 2022. Le délai d’intrusion le plus rapide a été de seulement 2 minutes et 7 secondes[6] !

Voici comment Dell et ses partenaires Intel® et CrowdStrike vous aident à détecter et à repousser une attaque par rétrogradation du BIOS tout au long de la chaîne de frappe grâce à la sécurité assistée par matériel.

Prévenir | **Détecter et répondre** | **Surmonter et corriger**

Détecter l’attestation du BIOS sur la plateforme CrowdStrike Falcon : lorsque la télémétrie des appareils Dell est activée, un administrateur peut consulter les notifications provenant des fonctionnalités de sécurité intégrées telles que la vérification du BIOS à distance dans CrowdStrike Falcon, ce qui permet d’accélérer la détection des activités suspectes avant qu’elles ne causent des dommages irréversibles.



Cas d’utilisation et contre-mesures

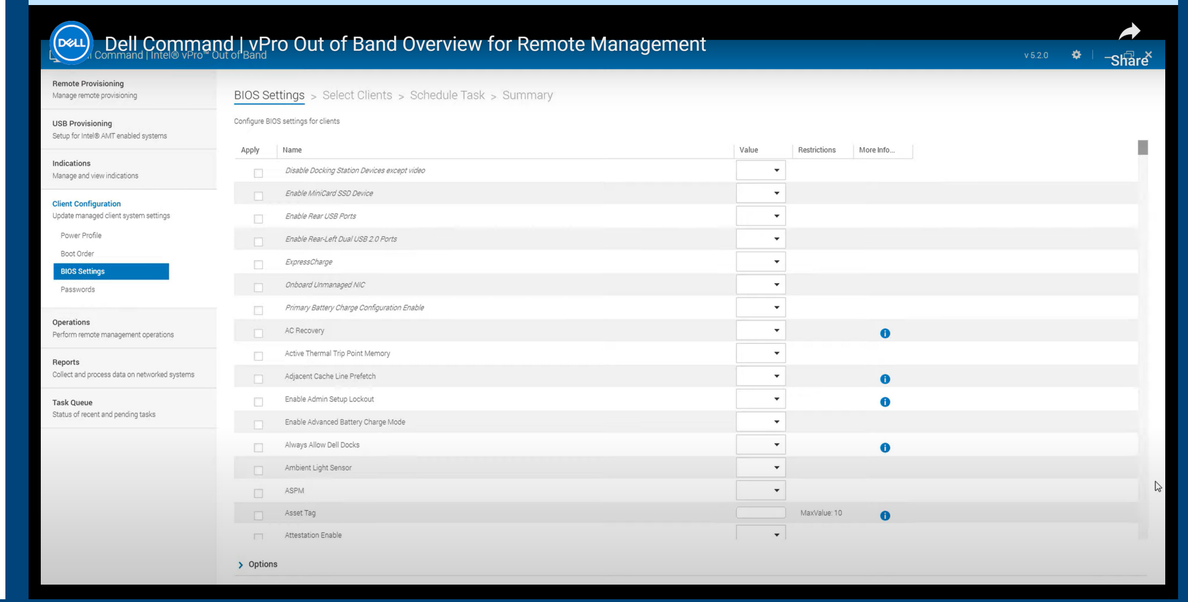
Contre-mesures des rétrogradations du BIOS

Les pirates s’insinuent dans le réseau plus rapidement que jamais. Selon le Global Threat Report de CrowdStrike, le délai moyen d’intrusion lors d’une cyberattaque (le temps nécessaire pour s’introduire dans un système et se déplacer latéralement) est passé à 62 minutes en 2023, contre 84 minutes en 2022. Le délai d’intrusion le plus rapide a été de seulement 2 minutes et 7 secondes[6] !

Voici comment Dell et ses partenaires Intel® et CrowdStrike vous aident à détecter et à repousser une attaque par rétrogradation du BIOS tout au long de la chaîne de frappe grâce à la sécurité assistée par matériel.

Prévenir | **Détecter et répondre** | **Surmonter et corriger**

Appliquer une mesure corrective en cas de rétrogradation du BIOS : cela aide à prévenir les menaces futures pour les systèmes hors bande. Dell Client Command Suite avec Intel vPro permet l’application de mesures correctives à distance.



Cas d’utilisation et contre-mesures

Dans ce deuxième cas d’utilisation, voici comment peut se dérouler le processus dans la chaîne de frappe d’une attaque au niveau de la chaîne logistique logicielle.

Attaques de chaîne logistique logicielle

Étape 1

Accès initial : compromission de la chaîne logistique

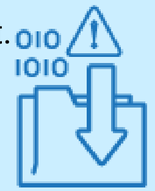
Le pirate injecte du code malveillant dans un utilitaire logiciel (BIOS/firmware).

Étape 2

Persistance

Les clients téléchargent le code malveillant lorsqu’ils mettent à jour leurs appareils.

Le pirate installe le logiciel malveillant.



Étape 3

Déplacement latéral

Le pirate usurpe l’identité d’un utilisateur qu’il vient d’attaquer et envoie un lien malveillant à un autre utilisateur. Ce dernier clique sur le lien et le pirate vole ses informations d’identification.

Étape 4

Exfiltration

Le pirate exfiltre les données.

Cas d’utilisation et contre-mesures

La chaîne logistique est devenue une cible clé pour les pirates. Bien que ces attaques soient moins courantes, les effets en cas de réussite peuvent être dévastateurs, car les entreprises cherchent encore à comprendre comment renforcer leurs défenses pour les contrer.

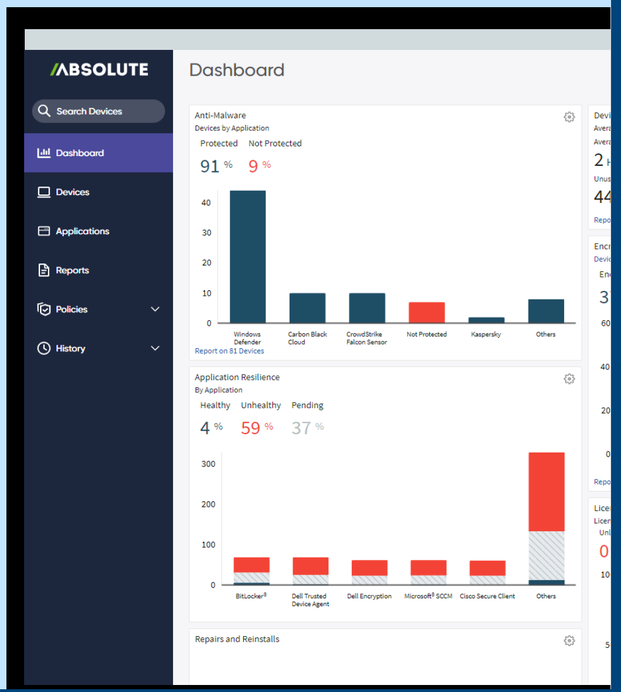
Il incombe à tous les fournisseurs de technologies de s’assurer que les solutions qu’ils vendent n’exposent pas involontairement les utilisateurs à des risques en raison de vulnérabilités.

Pour éviter les attaques et assurer la résilience au niveau de la pile de sécurité, Dell et Intel® respectent le processus et les protocoles stricts de notre cycle de développement sécurisé[7]. Une assurance supplémentaire de la chaîne logistique, par exemple Dell Secured Component Verification[8], ainsi que la sécurité au niveau du firmware d’Absolute (illustration à droite) rassurent les clients tout au long de la durée de vie du PC.

Prévenir | **Détecter et répondre** | **Surmonter et corriger**

Visibilité des points de terminaison depuis l’usine : visualisez tous les appareils situés dans le réseau et hors du réseau grâce à l’intégration d’Absolute dans les usines gérées par Dell. Absolute Custom Factory Install (CFI) supprime une étape dans le déploiement et protège les appareils susceptibles d’être expédiés vers des entrepôts et de multiples sites d’utilisateurs finaux. Limitez les risques grâce à une vue complète du parc à partir d’un tableau de bord basé sur le Cloud.

- Dressez et gérez facilement l’inventaire complet de toutes vos ressources et applications IT
- Repérez et cartographiez l’intégralité de votre parc
- Optimisez l’utilisation des ressources et surveillez votre posture de sécurité
- Bénéficiez de la prise en charge de plusieurs plateformes (Windows, Mac et Chrome)
- Profitez de l’intégration au BIOS de 27 OEM de PC leaders



Cas d’utilisation et contre-mesures

La chaîne logistique est devenue une cible clé pour les pirates. Bien que ces attaques soient moins courantes, les effets en cas de réussite peuvent être dévastateurs, car les entreprises cherchent encore à comprendre comment renforcer leurs défenses pour les contrer.

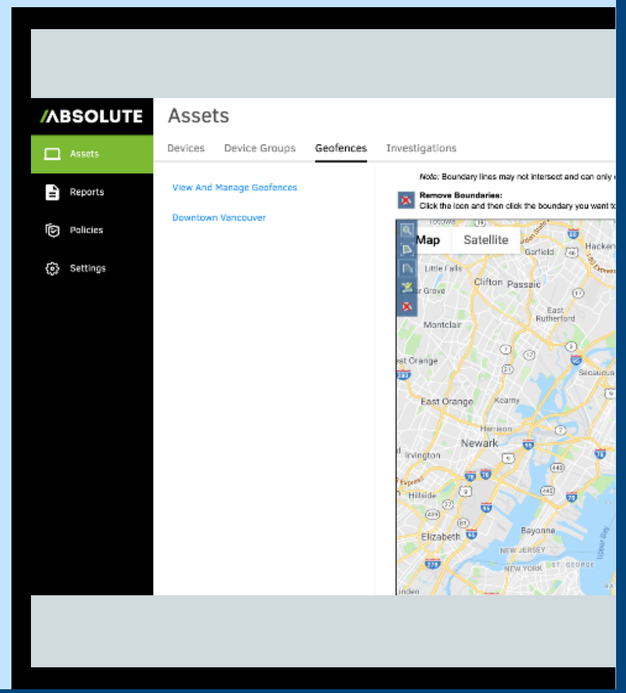
Il incombe à tous les fournisseurs de technologies de s’assurer que les solutions qu’ils vendent n’exposent pas involontairement les utilisateurs à des risques en raison de vulnérabilités.

Pour éviter les attaques et assurer la résilience au niveau de la pile de sécurité, Dell et Intel® respectent le processus et les protocoles stricts de notre cycle de développement sécurisé[7]. Une assurance supplémentaire de la chaîne logistique, par exemple Dell Secured Component Verification[8], ainsi que la sécurité au niveau du firmware d’Absolute (illustration à droite) rassurent les clients tout au long de la durée de vie du PC.

Prévenir | **Détecter et répondre** | **Surmonter et corriger**

Contrôlez les points de terminaison : avec Absolute, détectez les points de terminaison compromis (par exemple, une application critique est corrompue par un logiciel malveillant ou un PC disparaît pendant le transport). Prenez des mesures à distance pour contrer immédiatement les menaces en rendant les appareils inutilisables et/ou en supprimant les données qu’ils contiennent.

- Protégez vos appareils au-delà du périmètre défini
- Protégez et nettoyez à distance les données critiques
- Effectuez un nettoyage des données en fin de vie avec certificats de conformité
- Verrouillez les appareils pour protéger les ressources critiques à la demande
- Déployez une protection à distance des firmwares



Cas d’utilisation et contre-mesures

La chaîne logistique est devenue une cible clé pour les pirates. Bien que ces attaques soient moins courantes, les effets en cas de réussite peuvent être dévastateurs, car les entreprises cherchent encore à comprendre comment renforcer leurs défenses pour les contrer.

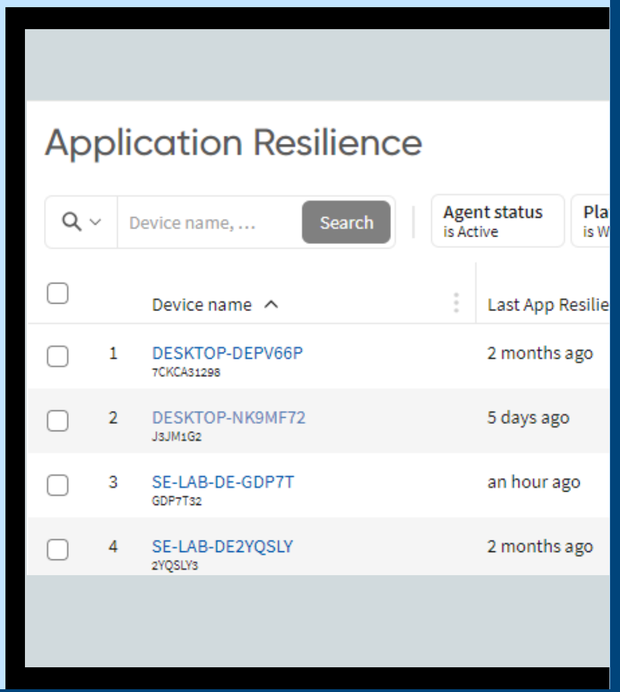
Il incombe à tous les fournisseurs de technologies de s’assurer que les solutions qu’ils vendent n’exposent pas involontairement les utilisateurs à des risques en raison de vulnérabilités.

Pour éviter les attaques et assurer la résilience au niveau de la pile de sécurité, Dell et Intel® respectent le processus et les protocoles stricts de notre cycle de développement sécurisé[7]. Une assurance supplémentaire de la chaîne logistique, par exemple Dell Secured Component Verification[8], ainsi que la sécurité au niveau du firmware d’Absolute (illustration à droite) rassurent les clients tout au long de la durée de vie du PC.

Prévenir | **Détecter et répondre** | **Surmonter et corriger**

Autoréparation : grâce à l’intégration d’Absolute Persistence dans le firmware du BIOS Dell, rétablissez l’état d’origine en cas de détection d’une falsification. Absolute peut autoréparer ou préserver n’importe quel point de terminaison compromis ou application prise en charge figurant dans le catalogue Application Resilience (plus de 80 applications), y compris une bibliothèque de contre-mesures supplémentaires en place, par exemple l’application Dell Trusted Device ou Zscaler.

- Trouvez et supprimez facilement les données sensibles des points de terminaison
- Engagez des mesures correctives sur les appareils grâce à une bibliothèque de scripts personnalisés
- Surveillez et autoréparez vos applications
- Profitez d’un catalogue Application Resilience étendu et évolutif de contrôles de points de terminaison tiers
- Investiguez et repérez les appareils perdus ou volés avec l’aide de l’équipe d’investigation d’Absolute



Principales informations à retenir

La sécurité d'un parc est proportionnelle à celle de ses différents PC.

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

Détectez, repoussez et surmontez les attaques en veillant à ce que la sécurité et la gestion des points de terminaison soient coordonnées.

La sécurité est un travail d'équipe. Appuyez-vous à la fois sur le matériel et sur les logiciels pour vous assurer la meilleure défense possible.

Pour en savoir plus :

Contactez-nous à l'adresse : Global.Security.Sales@Dell.com

Rendez-vous sur : Dell.com/Endpoint-Security

Suivez-nous : LinkedIn @DellTechnologies | X @DellTech

Passez à l'étape suivante

La sécurité est un sujet complexe, quelle que soit la taille des organisations. **Faites appel à un partenaire expérimenté en matière de sécurité et de technologie pour moderniser la sécurité de vos points de terminaison**.

Dell Trusted Workspace permet de mieux sécuriser les points de terminaison pour un environnement IT moderne adapté au Zero-Trust. Réduisez la surface d'attaque grâce à une gamme complète de solutions matérielles et logicielles de sécurité, caractéristiques de l'innovation Dell. Hautement coordonnée, notre approche de la sécurité allie solutions de protection intégrées et surveillance continue pour neutraliser d'éventuelles menaces. Les utilisateurs finaux maintiennent leur niveau de productivité et les équipes IT travaillent en toute sérénité avec des solutions de sécurité pensées pour l'univers Cloud actuel.

1. Source : Enterprise Strategy Group, une division de TechTarget, étude personnalisée réalisée à la demande de Dell Technologies, *Assessing Organizations' Security Journeys*, novembre 2023.
2. Source : Futurum Group, Endpoint Security Trends, 2023.
3. Source: Enterprise Strategy Group, une division de TechTarget, étude *Managing the Endpoint Vulnerability Gap: The Convergence of IT and Security to Reduce Exposure*, mai 2023.
4. 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. A comparison of security features, avril 2024.
5. Source : What is the Cyber Kill Chain? Introduction Guide – CrowdStrike.
6. Source : CrowdStrike 2024 Global Threat Report.
7. Source : Three Considerations for Establishing Device Trust | Dell USA.
8. Source : How to Keep Device Trust Close to the Vest | Dell USA.