DELL Technologies

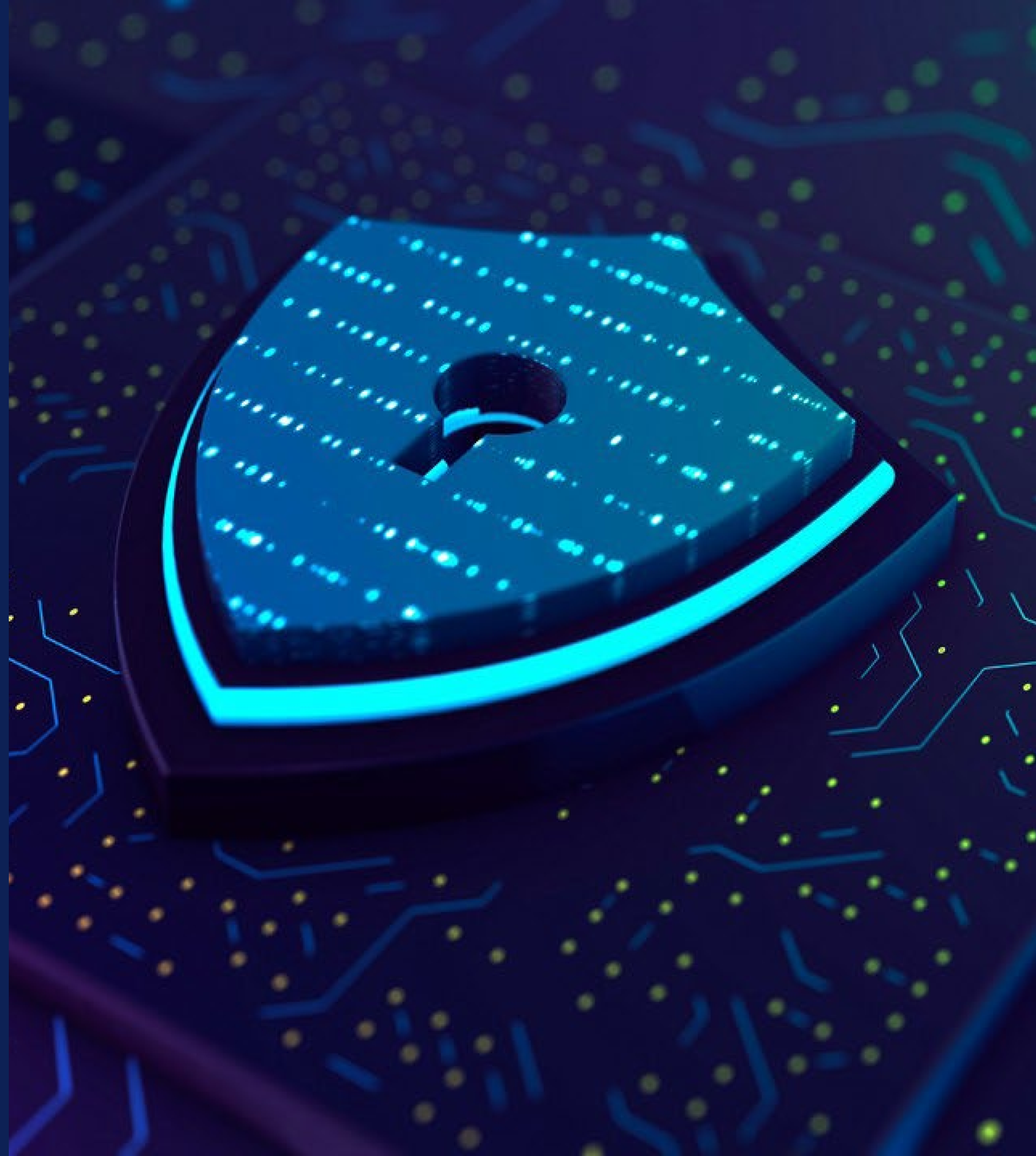
intel. Accelerate AI with Intel®

Windows 11

Anatomie d’un espace de travail de confiance

Renforcez la sécurité de votre parc en ajoutant plusieurs couches de défense

Contenu



Synthèse

De plus en plus nombreuses et sophistiquées, les cyberattaques sont inévitables. Les points de terminaison, les réseaux et les environnements Cloud sont devenus leurs principales cibles.

Cet e-book dispense des conseils aux décideurs des domaines IT et de la sécurité sur les éléments nécessaires pour défendre au mieux les points de terminaison contre les menaces en constante évolution.

Table des matières

Le paysage des menaces

La transition vers le travail hybride a engendré une plus grande complexité et de nouveaux vecteurs d'attaque, et la surface d'attaque des **points de terminaison, des réseaux et des Clouds n'a fait que grandir.**

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*.

De nombreuses organisations ont emprunté la voie du Zero-Trust pour faire face à ces menaces. Toutefois, mettre en œuvre les principes Zero-Trust nécessite d'avoir confiance en ses appareils.

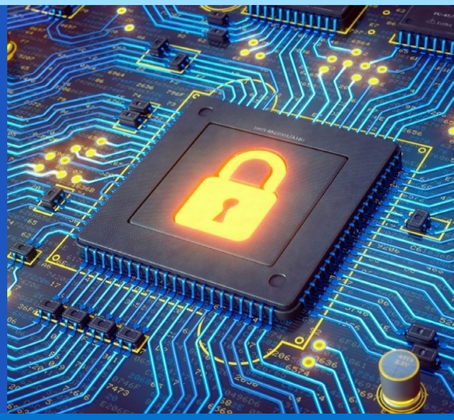
Mais comment maintenir cette confiance face à des attaques de plus en plus fréquentes et à la création de vecteurs d'attaques favorisée par des technologies avancées ?

Dell et Intel appliquent les principes Zero-Trust à leurs PC professionnels pour assurer la sécurité des entreprises et de leurs collaborateurs.

En savoir plus

Le saviez-vous ?

En 2022, 71 % des attaques n'étaient pas dues à des logiciels malveillants, soit une hausse de 9 % par rapport à 2021[1]



Seules 41 % des organisations peuvent affirmer en toute confiance que la sécurité est intégrée dans leurs technologies et leurs applications[2]

Vous envisagez le Zero-Trust pour faire évoluer votre cybersécurité ?

Consultez notre e-book :
Sécurité des points de terminaison : une composante essentielle de votre stratégie Zero-Trust.

1. CrowdStrike Global Threat Report, 2023.
2. Dell Innovation Index, 2023.

Défis

Sécuriser ses points de terminaison avec efficacité nécessite de comprendre votre adversaire et la façon dont il agit.

Compte tenu des gains potentiels, **les cybercriminels tentent souvent de pénétrer à plusieurs reprises dans la même organisation, en utilisant différentes méthodes et divers points d'entrée pour augmenter leurs chances d'y parvenir.** Par exemple, tout au long du cycle de vie d'un même appareil, les cybercriminels peuvent essayer de profiter de failles de sécurité via une douzaine de vecteurs.

Les moyens de défense actuels ne suffisent pas à garder les points de terminaison en sécurité. À mesure que les organisations renforcent leur surface d'attaque, les acteurs malveillants se tournent vers des cibles plus faciles. Avec la transition généralisée vers le travail hybride, les acteurs malveillants ont identifié de nouveaux vecteurs d'attaque des points de terminaison, ce qui a eu des retombées dévastatrices.

Voir les exemples d'attaques sur la droite

Attaque de la chaîne logistique : cible les fournisseurs pour accéder à leurs systèmes, à leurs données et/ou à leurs réseaux et, par extension, à leurs clients.

EXEMPLE : une attaque matérielle de la chaîne logistique initiée par une altération des composants :

Les cybercriminels interceptent une expédition de PC et modifient les disques durs.

Le département IT déploie les appareils compromis dans la société.

Les cybercriminels installent des logiciels malveillants pour extraire les informations d'identification lorsque les utilisateurs se connectent.

Attaque par ingénierie sociale : incite les utilisateurs finaux à fournir des données sensibles pouvant être utilisées pour obtenir un accès à des appareils ou des réseaux.

EXEMPLE : une attaque par usurpation d'identité, initiée par un e-mail de phishing :

L'utilisateur final se laisse piéger par un e-mail de phishing et communique ses informations d'identification sur une page web malveillante.

Le cybercriminel utilise les informations d'identification valides pour accéder à distance au réseau.

Le cybercriminel exfiltre les données vers un service Web, chiffre les données volées et ne les rend qu'en échange d'une rançon.

Contenu

Sécurisation de l’espace de travail moderne

En matière de protection des points de terminaison, vous avez besoin de plusieurs éléments à différents stades du cycle de vie de l’appareil : prévention, détection et réponse, récupération et mesures correctives, et ce, de l’approvisionnement et de la fabrication des PC à leur utilisation et à leur mise au rebut, en passant par leur expédition et leur déploiement. Imaginez l’ampleur d’une telle surface d’attaque combinée !

Les stratégies de cybersécurité les plus efficaces anticipent les pires scénarios. Il faut partir du principe qu’une violation est possible et mettre en place plusieurs couches de protection afin d’interrompre l’attaque aussi rapidement et aussi souvent que possible. Cela suppose également de mettre en place des mesures correctives afin de réduire le risque de récidive.

PRÉVENTION

Devenez plus difficile à atteindre grâce à des défenses conçues pour bloquer les attaques.

DÉTECTION ET RÉPONSE

Préparez-vous toujours à une violation et restez vigilant.

RÉCUPÉRATION ET MESURES CORRECTIVES

Atténuez l’impact d’une attaque et retrouvez une activité normale.

Le saviez-vous ?

Seules 33 %

des organisations utilisent une stratégie de sécurité globale de bout en bout intégrant des protections matérielles et logicielles[3].

3. Dell Innovation Index, 2023.

Une solution complète pour protéger le travail quotidien

Le PC étant devenu le nouveau « bureau », vous avez besoin d'une solution complète alliant productivité, facilité de collaboration, sécurité, fiabilité et confidentialité. Et les collaborateurs hybrides d'aujourd'hui doivent adopter un régime de **cyberhygiène**.

L'authentification multifacteur (MFA), l'application des principes du Zero-Trust, l'utilisation de solutions de détection et de réponse étendues (XDR) et anti logiciels malveillants, les mises à jour de correctifs et la protection de vos données les plus précieuses peuvent protéger les utilisateurs contre 99 % des attaques*.

Bases de la cyberhygiène

* www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

Garder un temps d'avance sur les menaces actuelles

Lors de la conception des systèmes de demain, Dell et Intel atténuent les risques tout au long de nos chaînes logistiques afin de veiller à ce que les appareils soient sécurisé dès le premier démarrage. Depuis des années, Intel permet aux fournisseurs de garantir la transparence et la traçabilité de la chaîne logistique numérique de base.

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.

La combinaison avec la solution Dell Secured Component Verification (SCV) offre une compatibilité et une interopérabilité qui améliorent l'assurance de la sécurité de la chaîne logistique numérique pour les appareils basés sur Intel.

En outre, Dell, Microsoft et Intel ont mis en place des politiques d'approvisionnement en composants, d'assemblage et de livraison afin de réduire la surface d'attaque, de protéger l'intégrité des appareils et de garantir la sécurité des appareils professionnels.

La sécurité matérielle des technologies Dell Trusted Device et Intel® Hardware Shield renforcent les défenses des appareils via un cadre de prévention, de détection et de réponse. En outre, Dell et Intel disposent toutes deux d'équipes de sécurité pour tester les produits et rechercher de nouvelles failles de sécurité avant que des pirates ne les trouvent, et pour créer et déployer rapidement des correctifs afin de vous aider à protéger vos équipes et votre entreprise.

Une solution complète pour protéger le travail quotidien

Sécurité Windows 11 et Microsoft 365 : sécuriser le travail quotidien.

Windows 11, couplé à la sécurité Microsoft 365 offre une solution complète qui assure une sécurité robuste pour le travail quotidien à tous les niveaux de l'organisation. Découvrons pourquoi cette combinaison de solutions de sécurité sort du lot.

Protection de base plus élevée :
Windows 11 met la barre plus haut en matière de sécurité, en intégrant des processeurs modernes avec des fonctionnalités comme la sécurité basée sur la virtualisation (VBS), l'intégrité du code protégée par l'hyperviseur (HVCI) et Secure Boot.

En savoir plus

Authentification sans mot de passe :
Windows 11 propose une authentification sans mot de passe, réduisant le risque de piratage via des attaques ciblant les mots de passe.

En savoir plus

Authentification multifacteur (MFA) :
Windows 11 propose des options d'authentification multifacteur qui vont au-delà des mots de passe.

En savoir plus

Préparation pour le travail hybride :
Les fonctions de sécurité avancées de Windows 11 sont conçues pour les scénarios de travail hybride.

En savoir plus

Antivirus Microsoft Defender :
Intégré dans Windows 11, l'antivirus Microsoft Defender assure une protection continue.

En savoir plus

Fonctions de sécurité rationalisées :
Windows 11 simplifie la sécurité en activant des fonctionnalités par défaut.

En savoir plus

Anatomie d’un espace de travail de confiance

Bénéficier d’une sécurité des points de terminaison moderne nécessite trois choses :

1. **Sécurité logicielle :** il n’y a jamais eu autant d’utilisateurs, d’appareils et de données en dehors des réseaux d’entreprise qu’à l’heure actuelle. La sécurité logicielle ne protège pas seulement les appareils, elle étend cette défense aux réseaux et aux environnements Cloud, là où les activités malveillantes trouvent leur source.

2. **Sécurité matérielle :** les appareils doivent inclure des fonctions de sécurité intégrées. Cela concerne la sécurité matérielle et de firmware qui protège l’appareil utilisé. Protéger votre espace de travail implique des fonctionnalités intégrées qui vous offrent visibilité et contrôle sur l’appareil.

3. **Sécurité de la chaîne logistique :** les appareils doivent être conçus de manière sécurisée. Cela implique de travailler avec des fournisseurs qui a) comprennent le paysage des menaces et b) peuvent mettre ces connaissances en application lorsque ce paysage évolue. Concevoir, développer et tester le PC en toute sécurité limite le risque de failles de sécurité, tandis que les contrôles de la chaîne logistique diminuent le risque d’altération des produits.

A Chief Technology Officer’s Vision Board For 2024 And Beyond - Lisez l’article Forbes

Décomposer les multiples couches de sécurité

(Liste d’exemples représentatifs de mesures de sécurité)

Sécurité logicielle

- Antivirus de nouvelle génération (NGAV)
- Détection et réponse au niveau des points de terminaison (EDR)
- Détection et réponse étendues (XDR)
- Protection des données dans le Cloud
- Protection du réseau
- Autoréparation automatisée

Sécurité du matériel/firmware

- Vérification de l’heure de démarrage
- Vérification du runtime
- Authentification des utilisateurs
- Notifications et alertes de sécurité/télémétrie

Sécurité de la chaîne logistique

- Pratiques de développement sécurisées
- Pratiques de chaîne logistique sécurisées
- Vérification des composants
- Emballage inviolable

Sécurité Windows 11 et Microsoft 365

Windows 11 et la sécurité Microsoft 365 créent un environnement de confiance qui stimule la productivité sans compromettre la sécurité, depuis les tâches de première ligne jusqu'à la prise de décisions stratégiques.

Copilot dans Windows et Copilot pour Microsoft 365 jouent un rôle crucial dans l'amélioration de la productivité et de la sécurité des utilisateurs.

Le rôle de Microsoft 365 et de Windows Copilot dans les PC pour offrir un espace de travail de confiance
Copilot orchestre les tâches, fournit des réponses précises et permet aux utilisateurs de se concentrer sur le travail stratégique.

S'assurer que les appareils répondent à des exigences professionnelles spécifiques
Copilot simplifie la configuration des appareils en ajustant les paramètres et en ins tallant des logiciels essentiels, et aide à répondre à des besoins spécifiques, assurant efficacité et efficience.

Facilité de gestion, de mise à niveau et d'utilisation des systèmes d'exploitation
Copilot assure un support pour la gestion des tâches du système d'exploitation.

Gestion du parc d'appareils

Sécurité des points de terminaison face aux cyberattaques
Copilot contribue à la sécurité globale en adhérant aux politiques de sécurité de Microsoft 365 et de Windows 11.

Applications collaboratives pour les professionnels de l'information et les collaborateurs en première ligne
Windows Copilot et Microsoft 365 Copilot améliorent la collaboration et la productivité des professionnels de l'information et du personnel en première ligne grâce à une assistance intelligente et à une intégration transparente entre les appareils.

En résumé, Microsoft Copilot contribue à créer un espace de travail de confiance, en rationalisant les opérations, en renforçant la sécurité et en favorisant la collaboration entre les différents rôles et appareils.

Lire le blog

Notre approche : Dell Trusted Workspace

Dell est un partenaire IT et de sécurité pour les organisations du monde entier. À la différence des solutions ad hoc, Dell préfère se concentrer sur des résultats généraux en matière de sécurité en mettant au point une suite de solutions qui interrompent les « kill chains » et augmentent votre résilience face aux cyberattaques.

Dell Trusted Workspace comprend :

- Des **protections matérielles et logicielles** uniques qui font des PC professionnels Dell les plus sécurisés du secteur[4] *(sécurité intégrée et sécurité intrinsèque)*
- Un écosystème de partenaires **logiciels leaders sur le marché** fournit une protection contre les menaces avancées pour les appareils, sur le réseau et dans le Cloud. *(sécurité complémentaire)*

Sécurité logicielle *complémentaire* de l'écosystème de partenaires

- **Dell SafeGuard and Response : CrowdStrike, Carbon Black** et **Secureworks** proposent des solutions de détection des menaces, de réponse et de mesures correctives
- **Dell SafeData : Netskope** offre visibilité, surveillance et prévention de la perte de données pour les applications Cloud. **Absolute** permet l'autoréparation des applications et des réseaux.

Sécurité logicielle et de firmware *intégrée* via les PC professionnels les plus sécurisés du secteur[4]

Exemples de fonctionnalités de protection de l'appareil :

- **Dell SafeBIOS** : une vérification* du BIOS hors hôte et des indicateurs d'attaque* aident à détecter les activités malveillantes avant qu'elles ne compromettent l'ordinateur.
- **Dell SafeID** sécurise les informations d'identification de l'utilisateur dans une puce de sécurité dédiée*.
- **La vérification du firmware hors hôte** protège l'intégrité du firmware à privilèges élevés*
- **Avec le logiciel Dell Trusted Device**, Dell intègre la télémétrie des appareils dans des logiciels leaders sur le marché pour améliorer la sécurité du parc informatique*
- **Intel® Hardware Shield** permet de prévenir les attaques contre le firmware et de protéger les applications contre les attaques qui s'exécutent via le BIOS.

La sécurité *intrinsèque* de la chaîne logistique aide à garantir la sécurité des PC dès le premier démarrage

- Des modules complémentaires de **Dell SafeSupply Chain** tels que Dell Secured Component Verification offrent une assurance supplémentaire de l'intégrité des produits.

* Exclusivité Dell

4. D'après une analyse interne réalisée par Dell en septembre 2023. S'applique aux PC équipés de processeurs Intel. Toutes les fonctionnalités ne sont pas disponibles sur tous les PC. Certaines fonctionnalités sont vendues séparément.

Tout regrouper avec Dell, Intel et Microsoft

Une fois les contre-mesures matérielles et logicielles mises en place, réduisez la surface d'attaque à l'aide de solutions de défense contre les attaques courantes.

Des fonctionnalités de détection et de réponse traitent les attaques furtives passées entre les mailles du filet.

Dans le cas d'une attaque de la chaîne logistique comme celle évoquée en page 4, dans le cadre de votre collaboration avec Dell, des mesures préventives telles que des **pratiques de chaîne logistique** sécurisées peuvent interrompre une attaque au tout début de la « kill chain ». Si une attaque passe entre les mailles du filet, des contre-mesures supplémentaires, comme **SCV** (Secured Component Verification), sont également mises en place.

Dans le cas d'une attaque par ingénierie sociale, même si un cybercriminel parvient à mettre la main sur les informations d'identification d'un utilisateur, **une vérification utilisateur basée sur du matériel telle que SafeID** peut l'empêcher d'aller plus loin.

Une solution de sécurité logicielle de type **passerelle Web sécurisée de nouvelle génération** fournit une autre couche de protection par surveillance.

Contrer une attaque matérielle de la chaîne logistique initiée par une altération des composants.

Les cybercriminels interceptent une expédition de PC et modifient les disques durs.

- **Pratiques de chaîne logistique sécurisées**
- Emballage inviolable
- Verrous

Le département IT déploie les appareils compromis dans la société.

- Vérification des composants sécurisés (SCV)
- Vérification du runtime

Les cybercriminels installent des logiciels malveillants pour extraire les informations d'identification lorsque les utilisateurs se connectent.

- Broker de sécurité d'accès au Cloud
- Passerelle Web sécurisée de nouvelle génération

Contrer une attaque par ingénierie sociale initiée par un e-mail de phishing.

L'utilisateur final se laisse piéger par un e-mail de phishing et communique ses informations d'identification sur une page Web malveillante.

- NGAV
- EDR
- XDR

Le cybercriminel utilise les informations d'identification valides pour accéder à distance au réseau.

- **Authentification multifacteur avec SafeID**
- Accès réseau Zero-Trust

Le cybercriminel exfiltre les données vers un service Web, chiffre les données volées et ne les rend qu'en échange d'une rançon.

- Passerelle Web sécurisée de nouvelle génération + analytique comportementale de l'entité utilisateur

Le modèle de sécurité Zero-Trust

Windows 11 adopte un concept connu sous le nom de modèle de sécurité Zero-Trust. Cette approche sur trois piliers :

1 **Pas d'accès sans preuve de sécurité et d'intégrité :**
Windows 11 part du principe qu'aucun utilisateur ou appareil ne doit avoir accès à quoi que ce soit tant que sa sécurité et son intégrité n'ont pas été vérifiées. Pour s'assurer qu'un ordinateur n'a pas été altéré, Windows 11 s'appuie sur une vérification explicite (authentification et autorisation) basée sur tous les points de données disponibles. Il s'agit notamment de l'identité de l'utilisateur, de sa localisation, de l'état de l'appareil, du service ou de la charge applicative, de la classification des données et des anomalies.

2 **Droit d'accès minimal :**
Windows 11 encourage l'utilisation du droit d'accès minimal. En limitant l'accès des utilisateurs grâce à des politiques adaptatives basées sur le risque, les données et la productivité sont sauvegardées.

3 **Supposer qu'il y a eu violation :**
Dans ce scénario, on suppose qu'un pirate informatique se trouve déjà dans le système. L'approche consiste à opérer de manière à réduire le rayon d'action et à segmenter l'accès. Le chiffrement de bout en bout est vérifié et l'analytique est exploitée pour gagner en transparence, faire progresser la détection des menaces et améliorer la défense.

Ce modèle de sécurité garantit une protection solide de A à Z, profitant à tous, des collaborateurs en première ligne aux cadres supérieurs.

Windows 11 Professionnel :
Favoriser des environnements de travail hybride

Windows 11 Professionnel, conçu spécialement pour les environnements de travail hybride, offre des fonctions de sécurité avancées et une protection contre les attaques. Les appareils Dell équipés de processeurs Intel® Core™ Ultra, fonctionnant sous Windows 11, représentent l'option la plus sûre du marché, car ils sont dotés d'une sécurité matérielle intégrée. Bénéficiez d'une productivité et d'une sécurité inégalées avec Windows 11, équipé de composants de sécurité préactivés.

Associés à Microsoft 365, les appareils Dell Trusted Devices offrent une sécurité d'entreprise complète sans nécessiter d'efforts en local. Choisissez Microsoft 365 pour réaliser des économies, bénéficier d'une sécurité robuste, d'une productivité accrue et d'une intégration transparente. Avec Dell Technologies, vous avez accès à une équipe de service dédiée, à un support complet pour la configuration et l'installation, et bénéficiez de services de gestion et d'une assistance à distance 24x7.

En savoir plus sur les fonctions de sécurité de Windows 11

Regarder la vidéo sur les fonctions de sécurité de Windows 11

Éléments clés à retenir

Les violations sont inévitables.
Une stratégie de sécurité efficace en matière de points de terminaison anticipe toujours le pire scénario. Son but est d'interrompre les « kill chains » où qu'elles interviennent, de l'appareil au réseau en passant par le Cloud.

Aucune solution ne peut bloquer 100 % des attaques.
Combinez des contre-mesures matérielles et logicielles pour une défense optimale.

Votre sécurité dépend de celle de vos fournisseurs.
Invitez vos fournisseurs à vous présenter leurs mesures de sécurité.

Pour en savoir plus :

Contactez-nous :
Global.Security.Sales@Dell.com

Consultez la page :
Dell.com/Endpoint-Security

Suivez-nous :
LinkedIn @DellTechnologies
X @DellTech

Aller de l'avant

La sécurité est un sujet complexe, quelle que soit la taille des organisations. **Les protections matérielles et logicielles complètes d'Intel et de Microsoft, réunies par Dell, permettent de créer une solution de sécurité moderne pour les points de terminaison.**

Dell Trusted Workspace contribue à sécuriser les points de terminaison d'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.

DELL Technologies

intel. Accelerate AI with Intel®

Windows 11