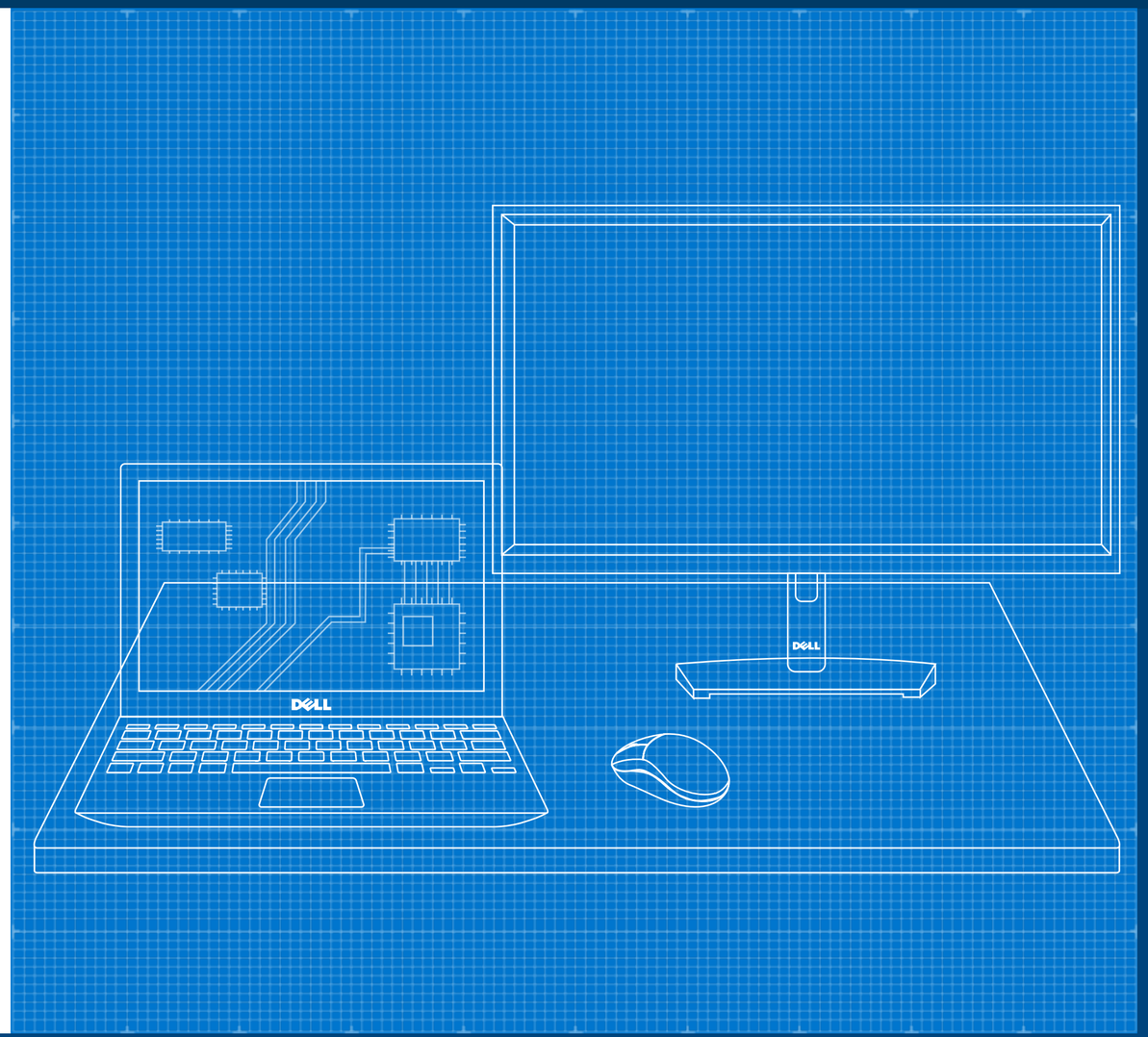
DELL Technologies

Anatomie d’un espace de travail de confiance

Renforcez la sécurité de votre parc en ajoutant plusieurs niveaux de protection



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.

Sommaire

1 Le paysage des menaces

2 Défis

3 Sécurisation des espaces de travail modernes

4 Anatomie d’un espace de travail de confiance

5 L’approche Dell

6 Synthèse

7 Informations à retenir et appel à l’action

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 s'agrandir.**

De plus, les cybercriminels ont désormais recours à des techniques sophistiquées qui ciblent différentes couches de la pile informatique, en se dissimulant dans des processus système valides. Certaines méthodes permettent même aux acteurs malveillants d'obtenir un accès privilégié et de désactiver des protections logicielles *sans être détectés*.

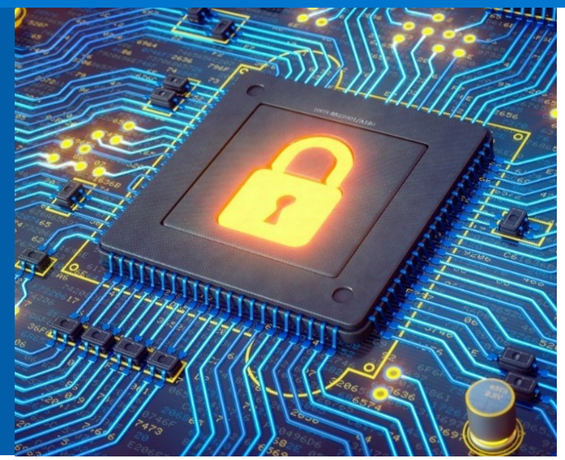
De nombreuses organisations ont emprunté la voie du Zero-Trust pour faire face à ces menaces. Toutefois, mettre en œuvre les principes Zero-Trust nécessite d'avoir confiance en ses appareils.

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 ?

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

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 sans conteste que la sécurité est intégrée dans leurs technologies et 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*.

Défis

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

Compte tenu des gains potentiels d'une violation, **les attaquants tentent souvent de pénétrer à plusieurs reprises dans la même organisation, en utilisant différentes méthodes et divers points d'entrée pour améliorer leurs chances.** Par exemple, tout au long du cycle de vie d'un même appareil, les attaquants 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 à droite

Attaque de la chaîne logistique : cible les fournisseurs pour accéder à leurs systèmes, leurs données et/ou leurs réseaux et, par extension, à leurs clients. **EXEMPLE : une attaque matérielle de la chaîne logistique initiée par une altération des composants :**

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

Le département IT déploie les appareils compromis dans la société.

Les attaquants 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 courriel de phishing et communique ses informations d'identification sur une page web malveillante.

L'attaquant utilise les informations d'identification valides pour accéder à distance au réseau.

L'attaquant exfiltre les données vers un service web, chiffre les données volées et ne les rend qu'en échange d'une rançon.

Sécurisation des espaces de travail modernes

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, et récupération et mesures correctives, et ce, de l'approvisionnement et de la fabrication du PC à son utilisation et sa mise au rebut, en passant par son expédition et son 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 les attaques aussi rapidement et aussi souvent que possible. Cela suppose également de mettre en place des mesures correctives afin de minimiser le risque de récidive.

[3] Dell Innovation Index, 2023.

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 vigilants.

RÉCUPÉRATION ET MESURES CORRECTIVES

Diminuez l'impact d'une attaque et retrouvez une activité normale.

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.

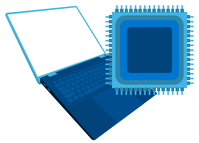
3. **Sécurité de la chaîne logistique :** les appareils doivent être construits de manière sécurisée. Cela implique de travailler avec des fournisseurs qui a) comprennent le paysage des menaces et b) peuvent mettre ces connaissances en application lorsque ce paysage évolue. Concevoir, développer et tester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

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

Notre approche : Dell Trusted Workspace

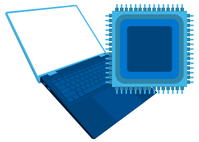
Dell est un partenaire IT et de sécurité pour les organisations du monde entier. À la différence des solutions ad hoc, Dell préfère se concentrer sur des résultats généraux en matière de sécurité en mettant au point une suite de solutions qui interrompent les « kill chains » et augmentent votre résilience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

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

Sécurité logicielle *complémentaire* de la part de l'écosystème de partenaires

- **Dell SafeGuard and Response :** **CrowdStrike**, **VMware Carbon Black** et **Secureworks** fournissent des solutions de détection des menaces, de réponse et de mesures correctives.
- **Dell SafeData :** **Netskope** fournit des solutions en matière de visibilité, de surveillance et de prévention de la perte de données pour les applications basées sur le 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 des firmwares hors hôte** protège l'intégrité des firmwares à privilèges élevés*.
- Avec le **logiciel Dell Trusted Device**, Dell intègre la télémétrie des appareils à des logiciels leaders sur le marché pour améliorer la sécurité du parc informatique*.

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.

** Spécifique à Dell*

Tout regrouper avec Dell

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, si vous travaillez 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**, sont également mise en place.

Dans le cas d'une attaque par ingénierie sociale, même si un attaquant arrive 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 attaquants interceptent une expédition de PC et modifient les disques durs.

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

Le département IT déploie les appareils compromis dans la société.

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

Les attaquants 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 courriel de phishing et communique ses informations d'identification sur une page web malveillante.

- NGAV
- EDR
- XDR

L'attaquant utilise les informations d'identification valides pour accéder à distance au réseau.

- Authentification multifacteur avec SafeID
- Accès réseau Zero-Trust

L'attaquant exfiltre les données vers un service web, chiffre les données volées et ne les rend qu'en échange d'une rançon.

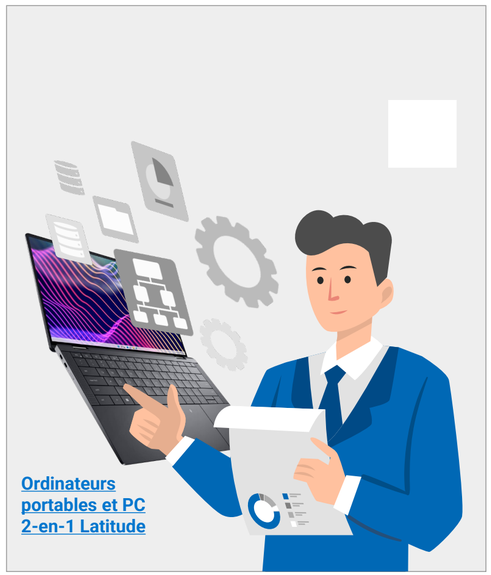
- Passerelle Web sécurisée de nouvelle génération + analytique comportementale de l'entité utilisateur

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.



Ordinateurs portables et PC 2-en-1 Latitude

Pour en savoir plus :

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

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

Suivez-nous sur : LinkedIn @DellTechnologies | X @DellTech

Aller de l'avant

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 contribue à sécuriser les points de terminaison d'un environnement informatique moderne basé sur une stratégie Zero-Trust. Réduisez la surface d'attaque à l'aide d'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.