DELL Technologies

La sécurité des points de terminaison est une composante essentielle de votre stratégie Zero-Trust

Trois recommandations pour élaborer une stratégie Zero-Trust performante

DELL Technologies

Synthèse

Le modèle Zero-Trust est un concept stratégique à long terme. Il ne s'agit pas d'un produit ou d'une solution que les organisations décident d'implémenter, mais d'un plan stratégique de gestion de la sécurité qui s'inscrit dans le temps. Riche en conseils pratiques à l'attention des décideurs IT qui s'engagent dans un projet de transition vers le Zero-Trust, cet e-book souligne l'importance de la sécurité des points de terminaison dans la construction d'un environnement moderne ultra-sécurisé pour notre génération de télétravailleurs.

Sommaire

Discours de cyberpolitique générale

Les menaces de sécurité se multiplient alors même que la généralisation des environnements de travail hybrides/distants et Cloud favorise ce phénomène.

Au cours des dernières années, la protection des ressources de données des organisations s'est fortement complexifiée. Le Cloud a révolutionné le mode de productivité des entreprises avec la généralisation des environnements de travail hybride/distant. Et naturellement, cela a un prix. Les organisations sont passées de la gestion d'une simple infrastructure sur site à un univers Cloud, augmentant ainsi la surface d'attaque des pirates informatiques et le préjudice qui en découle. Autrement dit, si l'offensive d'un attaquant aboutit, elle risque non pas d'affecter un client, mais chacun des clients du service Cloud concerné tout au long de la chaîne logistique. Une aubaine qui peut s'avérer très lucrative pour les auteurs de ces menaces (qu'il s'agisse d'États-nations ou de criminels ordinaires), et qui les incite à poursuivre leur quête de nouvelles failles de sécurité à exploiter.

Le montant du préjudice total lié au cybercrime devrait s'élever à **10,5 billions de dollars d'ici 2025**[i]

D'après une étude publiée par Verizon en 2022, **5 200** violations de données confirmées ont été signalées, soit **1,3 fois plus que l'année précédente**[ii]

Les enjeux à l'ère du télétravail

Les organisations doivent trouver le moyen de prendre une longueur d'avance face à l'évolution des menaces.

Alors, quels sont les enjeux d'un monde où le télétravail ne cesse de gagner du terrain ? Deux points sont à retenir :

Toutes les organisations présentent des vulnérabilités…

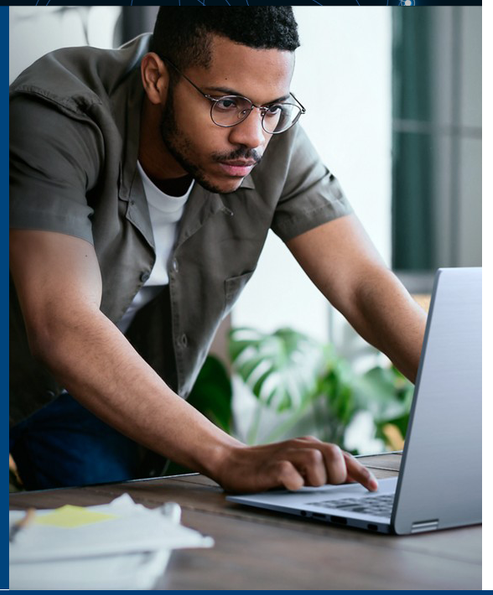
> « [S]i une entité est déterminée à s'introduire dans votre système, elle a de grandes chances d'y parvenir. »
>
> — *Amiral Michael Rogers, ancien directeur de la National Security Agency (NSA) et ancien commandant de l'U.S. Cyber Command*[iii]

…et la moindre erreur peut leur coûter terriblement cher.

> « C'est un nouveau record : le coût moyen d'une violation de données a atteint 4,88 millions de dollars en 2024[iv]. »

Les vecteurs d'attaque se multiplient, les surfaces d'attaque s'étendent et aucune société ne bénéficiera jamais d'une politique de sécurité parfaite. Les organisations doivent envisager un scénario catastrophe et renforcer leur ligne de défense pour se préparer à l'attaque inévitable.

69 % des organisations ont déjà été victimes d'une forme de cyberattaque en raison d'une mauvaise gestion de ressources accessibles par Internet[v].



Stratégies de sécurité : place au changement

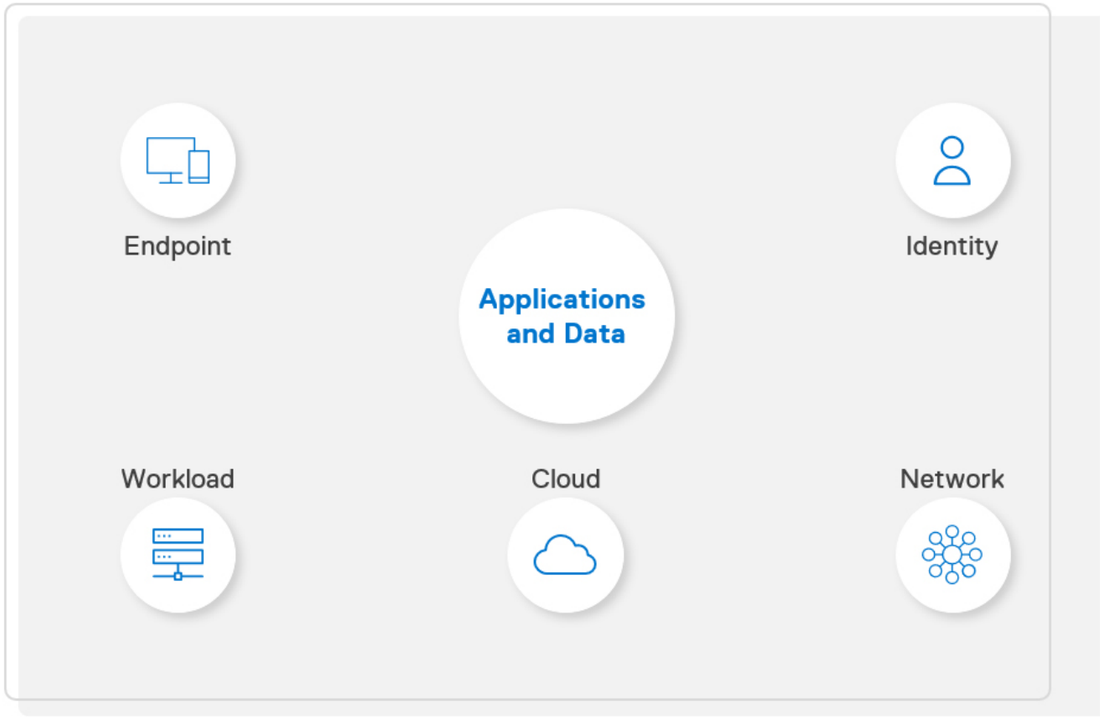
À l'heure actuelle, il est impossible d'échapper au Cloud. C'est là que le Zero-Trust entre en jeu.

Les modèles de sécurité traditionnels sont dépassés. Et voici pourquoi.

Pour maintenir une posture de sécurité efficace, l'organisation doit mettre en place 5 points de contrôle : point de terminaison, charge applicative, identité, réseau et Cloud. L'objectif est d'assurer la protection des applications et des données.

Les approches traditionnelles sont souvent cloisonnées. Les organisations qui adoptent ce type d'approche sont donc d'autant plus vulnérables aux attaques.

Et puis...

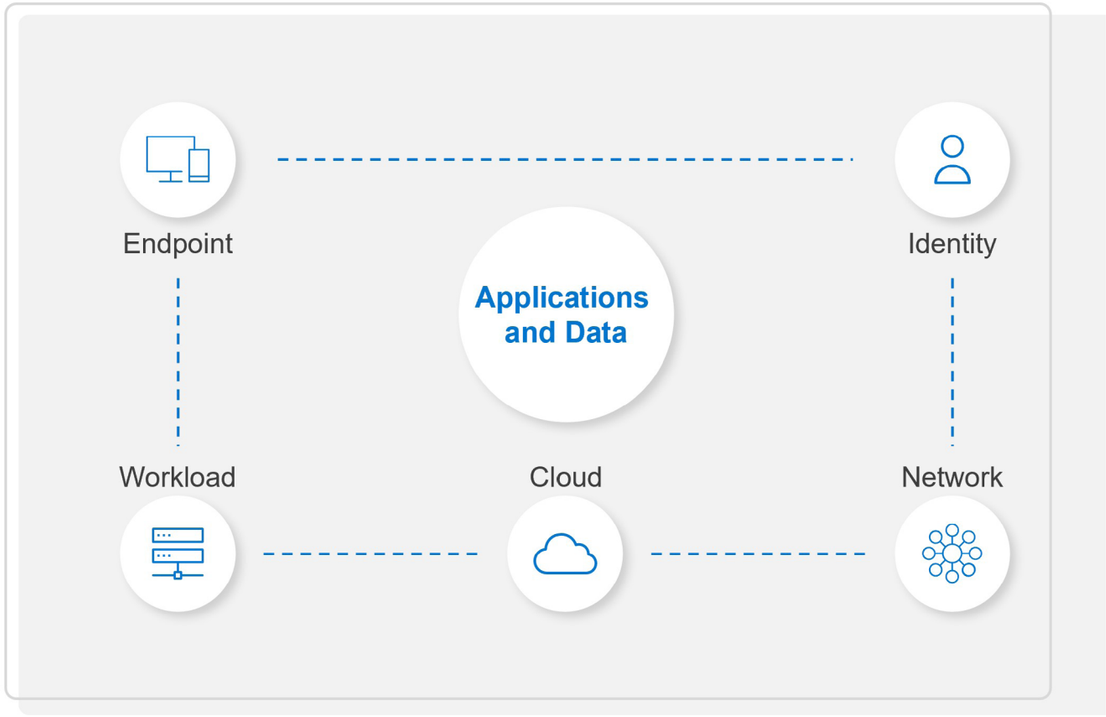


Stratégies de sécurité : place au changement

À l'heure actuelle, il est impossible d'échapper au Cloud. C'est là que le Zero-Trust entre en jeu.

Les approches modernes tendent vers une intensification des contrôles et une meilleure communication entre les points de contrôle. Toutefois, la généralisation des environnements de travail hybrides/distants nous oblige à en renforcer le périmètre.

Et puis...

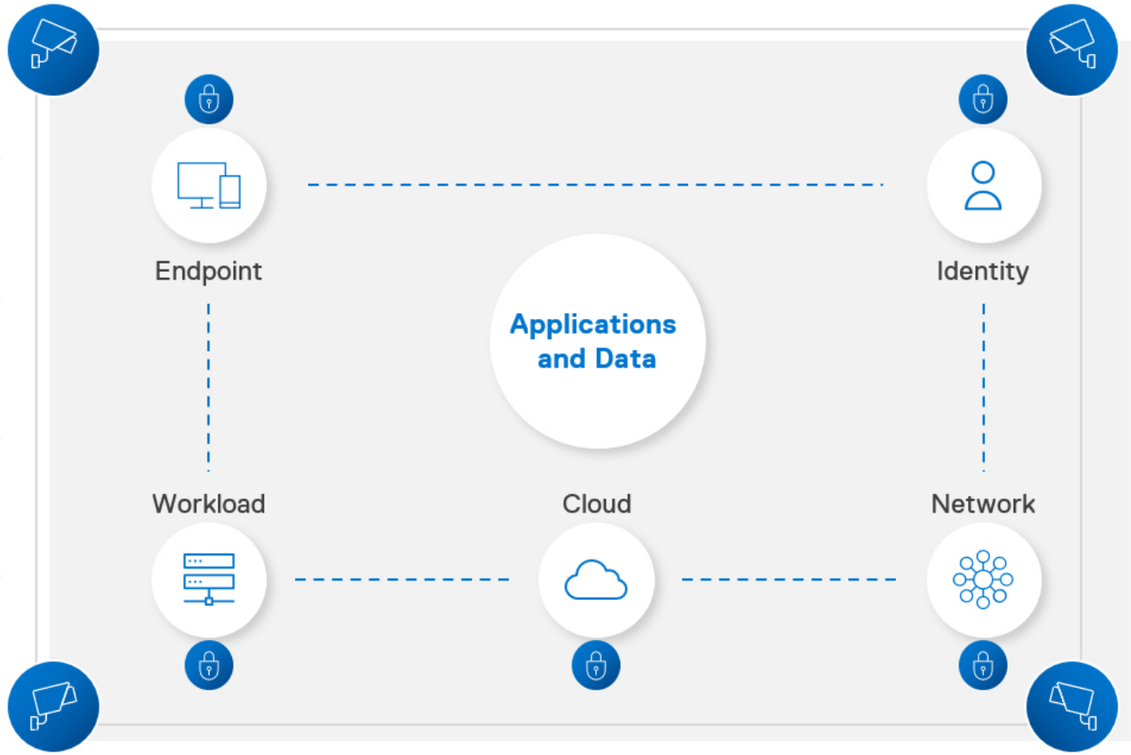


Stratégies de sécurité : place au changement

À l'heure actuelle, il est impossible d'échapper au Cloud. C'est là que le Zero-Trust entre en jeu.

Aujourd'hui, les collaborateurs travaillent où bon leur semble (chez eux, dans un café, à l'hôtel, ou ailleurs). Ils ont donc souvent recours à des réseaux Wi-Fi non sécurisés dont la connectivité vers des bureaux et des datacenters protégés par un pare-feu est limitée, voire inexistante. Ils peuvent, par défaut, connecter leurs appareils directement à Internet pour accéder à des serveurs de fichiers dans le Cloud et à des applications logicielles as-a-service (SaaS), et consulter les données de leur entreprise.

Face à des attaques toujours plus sophistiquées et des vecteurs d'attaque qui ne cessent de se multiplier, les stratégies de sécurité traditionnelles fondées sur une forme de confiance implicite sont désormais dépassées. C'est là que le Zero-Trust entre en jeu.



Comprendre les fondamentaux du modèle Zero-Trust

Le concept Zero-Trust est une nouvelle façon de penser la sécurité. Il remplace la confiance *implicite*, qui permet aux utilisateurs authentifiés de circuler librement sur le réseau. Le modèle Zero-Trust inverse ce modèle pour donner aux organisations un contrôle explicite sur leur environnement IT.

Pour illustrer le modèle Zero-Trust, partons d'un concept éprouvé : le développement des protocoles de sécurité.

Vous travaillez au siège d'une entreprise. Lors de votre première journée, vous avez reçu un badge et été informé des protocoles de sécurité. Chaque jour, votre entrée dans le bâtiment est filmée par différentes caméras et vous devez utiliser votre badge pour accéder à différents endroits. Une fois installé à votre bureau, vous déverrouillez votre ordinateur à l'aide d'un mot de passe.

An employee arrives at their office building and gets their badge out to gain entry.

Et puis...

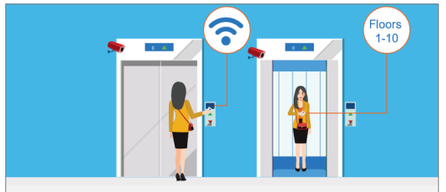
Comprendre les fondamentaux du modèle Zero-Trust

Le concept Zero-Trust est une nouvelle façon de penser la sécurité. Il remplace la confiance *implicite*, qui permet aux utilisateurs authentifiés de circuler librement sur le réseau. Le modèle Zero-Trust inverse ce modèle pour donner aux organisations un contrôle explicite sur leur environnement IT.

Pour illustrer le modèle Zero-Trust, partons d'un concept éprouvé : le développement des protocoles de sécurité.

Vous travaillez au siège d'une entreprise. Lors de votre première journée, vous avez reçu un badge et été informé des protocoles de sécurité. Chaque jour, votre entrée dans le bâtiment est filmée par différentes caméras et vous devez utiliser votre badge pour accéder à différents endroits. Une fois installé à votre bureau, vous déverrouillez votre ordinateur à l'aide d'un mot de passe.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

Et puis...

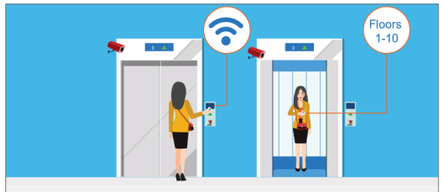
Comprendre les fondamentaux du modèle Zero-Trust

Le concept Zero-Trust est une nouvelle façon de penser la sécurité. Il remplace la confiance *implicite*, qui permet aux utilisateurs authentifiés de circuler librement sur le réseau. Le modèle Zero-Trust inverse ce modèle pour donner aux organisations un contrôle explicite sur leur environnement IT.

Pour illustrer le modèle Zero-Trust, partons d'un concept éprouvé : le développement des protocoles de sécurité.

Vous travaillez au siège d'une entreprise. Lors de votre première journée, vous avez reçu un badge et été informé des protocoles de sécurité. Chaque jour, votre entrée dans le bâtiment est filmée par différentes caméras et vous devez utiliser votre badge pour accéder à différents endroits. Une fois installé à votre bureau, vous déverrouillez votre ordinateur à l'aide d'un mot de passe.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.

Et puis...

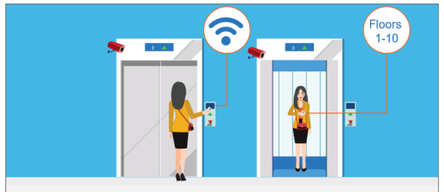
Comprendre les fondamentaux du modèle Zero-Trust

Le concept Zero-Trust est une nouvelle façon de penser la sécurité. Il remplace la confiance *implicite*, qui permet aux utilisateurs authentifiés de circuler librement sur le réseau. Le modèle Zero-Trust inverse ce modèle pour donner aux organisations un contrôle explicite sur leur environnement IT.

Pour illustrer le modèle Zero-Trust, partons d'un concept éprouvé : le développement des protocoles de sécurité.

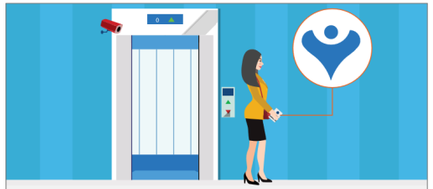
Vous travaillez au siège d'une entreprise. Lors de votre première journée, vous avez reçu un badge et été informé des protocoles de sécurité. Chaque jour, votre entrée dans le bâtiment est filmée par différentes caméras et vous devez utiliser votre badge pour accéder à différents endroits. Une fois installé à votre bureau, vous déverrouillez votre ordinateur à l'aide d'un mot de passe.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

Et puis...

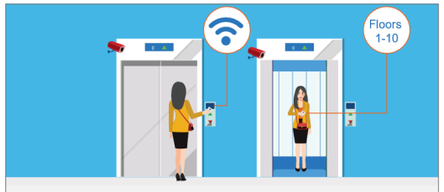
Comprendre les fondamentaux du modèle Zero-Trust

Le concept Zero-Trust est une nouvelle façon de penser la sécurité. Il remplace la confiance *implicite*, qui permet aux utilisateurs authentifiés de circuler librement sur le réseau. Le modèle Zero-Trust inverse ce modèle pour donner aux organisations un contrôle explicite sur leur environnement IT.

Pour illustrer le modèle Zero-Trust, partons d'un concept éprouvé : le développement des protocoles de sécurité.

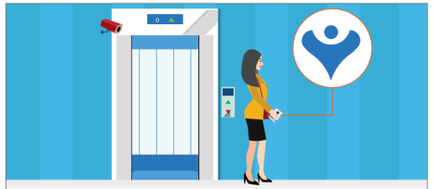
Vous travaillez au siège d'une entreprise. Lors de votre première journée, vous avez reçu un badge et été informé des protocoles de sécurité. Chaque jour, votre entrée dans le bâtiment est filmée par différentes caméras et vous devez utiliser votre badge pour accéder à différents endroits. Une fois installé à votre bureau, vous déverrouillez votre ordinateur à l'aide d'un mot de passe.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

They swipe their ID card to gain entry to their suite.

Et puis...

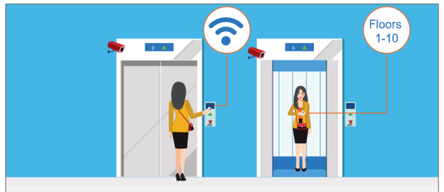
Comprendre les fondamentaux du modèle Zero-Trust

Le concept Zero-Trust est une nouvelle façon de penser la sécurité. Il remplace la confiance *implicite*, qui permet aux utilisateurs authentifiés de circuler librement sur le réseau. Le modèle Zero-Trust inverse ce modèle pour donner aux organisations un contrôle explicite sur leur environnement IT.

Pour illustrer le modèle Zero-Trust, partons d'un concept éprouvé : le développement des protocoles de sécurité.

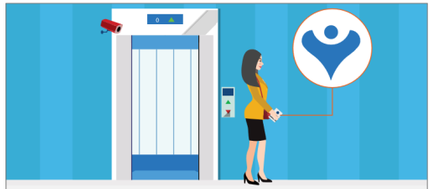
Vous travaillez au siège d'une entreprise. Lors de votre première journée, vous avez reçu un badge et été informé des protocoles de sécurité. Chaque jour, votre entrée dans le bâtiment est filmée par différentes caméras et vous devez utiliser votre badge pour accéder à différents endroits. Une fois installé à votre bureau, vous déverrouillez votre ordinateur à l'aide d'un mot de passe.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

They swipe their ID card to gain entry to their suite.

The employee arrives at their desk and unlocks their computer using a password.

Et puis...

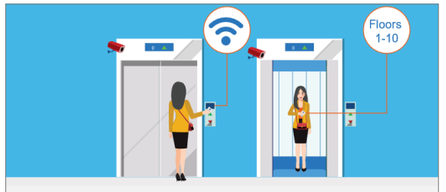
Comprendre les fondamentaux du modèle Zero-Trust

C’est ainsi que fonctionne le Zero-Trust.

Votre employeur vous a identifié·dès votre premier jour dans l’entreprise. Depuis lors, chacun de vos accès est vérifié de manière à protéger les ressources de l’organisation (utilisateurs, données, etc.). Pour renforcer le niveau de sécurité, les agents de sécurité surveillent sur des écrans les déplacements au sein du bâtiment. Tout comportement étrange (tel qu’une tentative d’accès à un espace non autorisé) fait l’objet d’investigations.

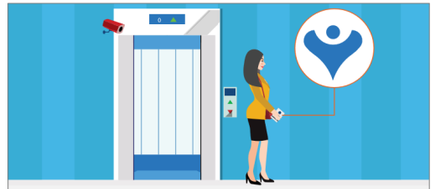
Aujourd’hui, les utilisateurs, les appareils, les applications et les données évoluent plus que jamais en dehors des réseaux de l’entreprise. De fait, l’identité des utilisateurs donne lieu à une zone d’ombre, et l’usurpation des identités devient le principal moteur de la plupart des cas de violation. Une stratégie Zero-Trust remédie à ce risque.

An employee arrives at their office building and gets their badge out to gain entry.



They use their badge to gain access to the elevator assigned to their floor.

The employee uses their badge again to activate their floor selection in the elevator.



Once they arrive on their floor, the employee walks to their office suite.

They swipe their ID card to gain entry to their suite.

The employee arrives at their desk and unlocks their computer using a password.

Instaurer les principes du modèle Zero-Trust

La sécurité des points de terminaison est une pièce maîtresse de la transition vers le Zero-Trust.

Pour élaborer une stratégie Zero-Trust performante, il est capital de sécuriser les points de terminaison.

D'après le framework MITRE ATT&CK®, les pirates informatiques emploient aujourd'hui neuf « techniques d'accès initial » pour accéder aux réseaux qu'ils ciblent *(cf. illustration)*[vi]. Selon différentes études, les systèmes de défense traditionnels basés sur le Cloud ne permettent pas de sécuriser les points de terminaison correctement. Un seul point d'entrée permet au cybercriminel d'atteindre sa cible. Avec les points de terminaison, les auteurs de menaces parviennent à exploiter des dizaines de failles de sécurité tout au long du cycle de vie d'un appareil.

Face à l'augmentation du nombre d'appareils sur les réseaux, les points de terminaison sont désormais un vecteur d'attaque de plus en plus puissant.

Les règles de sécurité du modèle Zero-Trust définissent, en termes explicites, le trafic connu et autorisé et bloquent les autres demandes. Pour identifier le moindre écart, le processus de gestion des menaces mis en place permet de signaler tout comportement inhabituel et de déclencher les mesures correctives nécessaires pour remédier à la menace potentielle.

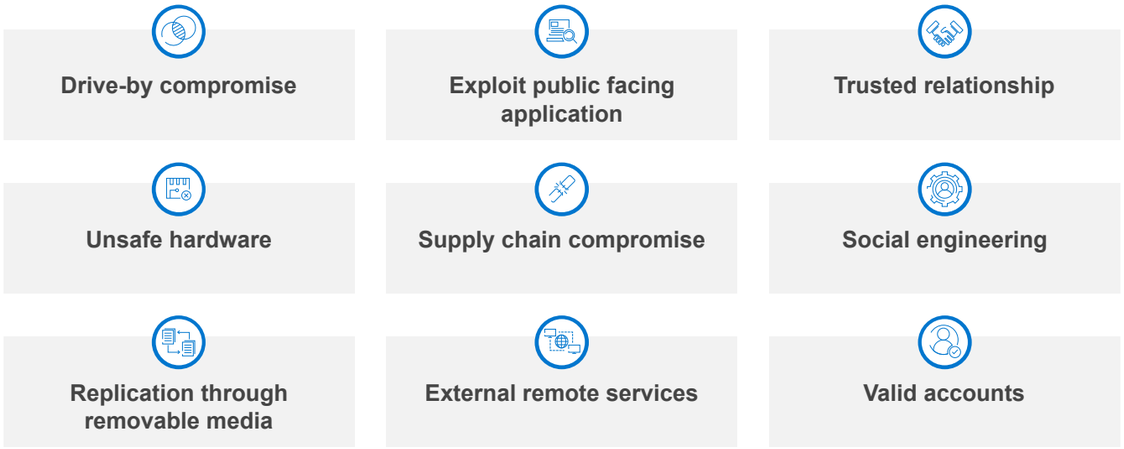


Illustration 1/3

Instaurer les principes du modèle Zero-Trust

La sécurité des points de terminaison est une pièce maîtresse de la transition vers le Zero-Trust.

Pour élaborer une stratégie Zero-Trust performante, il est capital de sécuriser les points de terminaison.

D'après le framework MITRE ATT&CK®, les pirates informatiques emploient aujourd'hui neuf « techniques d'accès initial » pour accéder aux réseaux qu'ils ciblent *(cf. illustration)*[vi]. Selon différentes études, les systèmes de défense traditionnels basés sur le Cloud ne permettent pas de sécuriser les points de terminaison correctement. Un seul point d'entrée permet au cybercriminel d'atteindre sa cible. Avec les points de terminaison, les auteurs de menaces parviennent à exploiter des dizaines de failles de sécurité tout au long du cycle de vie d'un appareil.

Face à l'augmentation du nombre d'appareils sur les réseaux, les points de terminaison sont désormais un vecteur d'attaque de plus en plus puissant.

Les règles de sécurité du modèle Zero-Trust définissent, en termes explicites, le trafic connu et autorisé et bloquent les autres demandes. Pour identifier le moindre écart, le processus de gestion des menaces mis en place permet de signaler tout comportement inhabituel et de déclencher les mesures correctives nécessaires pour remédier à la menace potentielle.

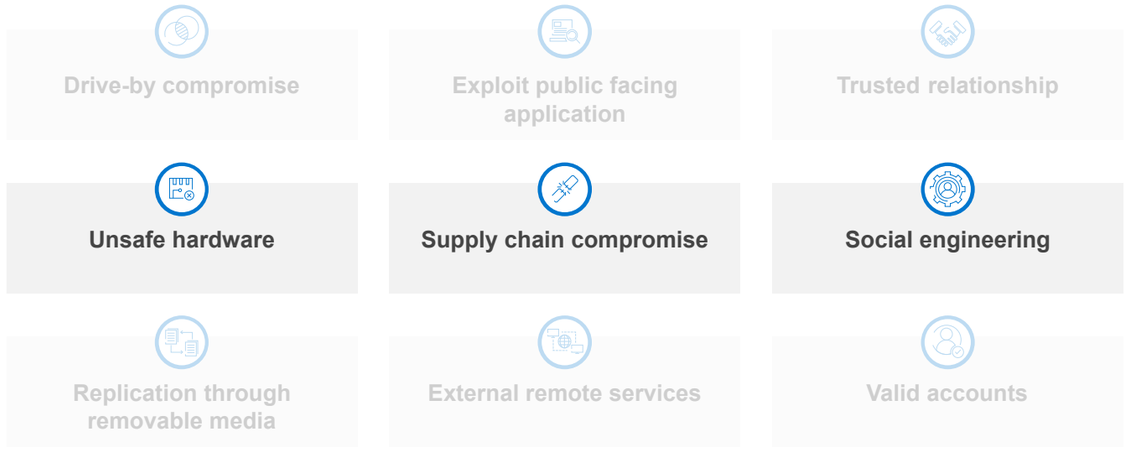


Illustration 2/3

Instaurer les principes du modèle Zero-Trust

La sécurité des points de terminaison est une pièce maîtresse de la transition vers le Zero-Trust.

Pour élaborer une stratégie Zero-Trust performante, il est capital de sécuriser les points de terminaison.

D'après le framework MITRE ATT&CK®, les pirates informatiques emploient aujourd'hui neuf « techniques d'accès initial » pour accéder aux réseaux qu'ils ciblent *(cf. illustration)*[vi]. Selon différentes études, les systèmes de défense traditionnels basés sur le Cloud ne permettent pas de sécuriser les points de terminaison correctement. Un seul point d'entrée permet au cybercriminel d'atteindre sa cible. Avec les points de terminaison, les auteurs de menaces parviennent à exploiter des dizaines de failles de sécurité tout au long du cycle de vie d'un appareil.

Face à l'augmentation du nombre d'appareils sur les réseaux, les points de terminaison sont désormais un vecteur d'attaque de plus en plus puissant.

Les règles de sécurité du modèle Zero-Trust définissent, en termes explicites, le trafic connu et autorisé et bloquent les autres demandes. Pour identifier le moindre écart, le processus de gestion des menaces mis en place permet de signaler tout comportement inhabituel et de déclencher les mesures correctives nécessaires pour remédier à la menace potentielle.

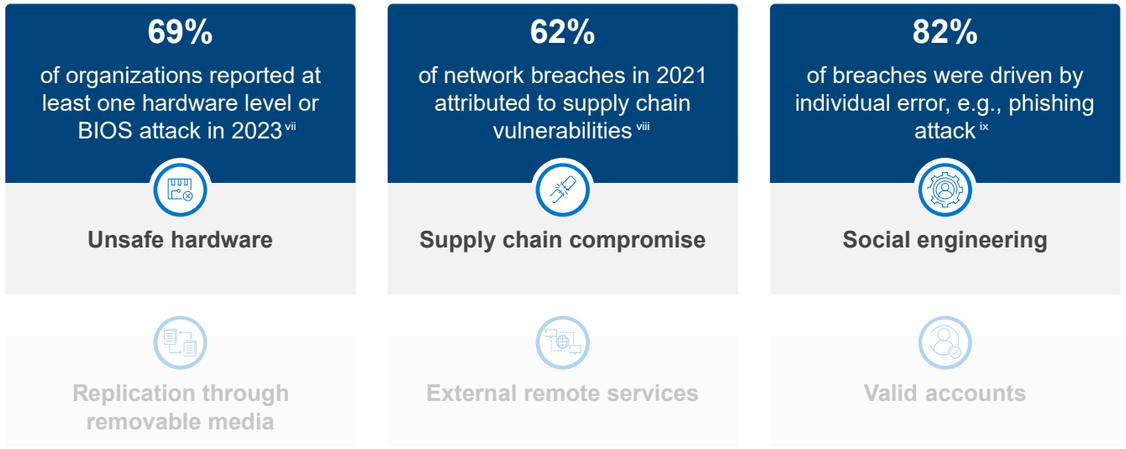


Illustration 3/3

Trois recommandations pour élaborer une stratégie Zero-Trust performante

Réunissez les conditions pour mener à bien un projet de transformation Zero-Trust dans votre organisation.

1

Établissez des règles et des contrôles adaptés aux priorités de votre entreprise.

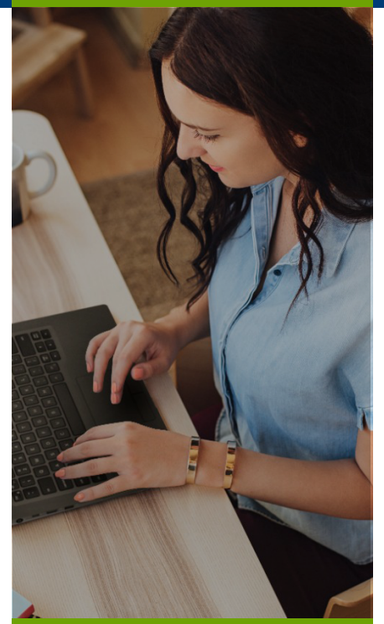
Les moteurs de règles et la gestion de ces règles sont des composantes essentielles à la mise en œuvre d'une stratégie Zero-Trust performante. Mais quelle organisation a les moyens d'allouer un budget illimité à la sécurité ? Mieux vaut donc commencer par déterminer les priorités de votre entreprise. Quels sont les actifs de propriété intellectuelle et les ressources les plus stratégiques que vous souhaitez protéger ? Évaluez la surface d'attaque face au niveau de risque tolérable pour votre organisation.

Ensuite, examinez les règles et les contrôles en place. Dans le contexte actuel, les risques émanent de l'univers du Cloud dans lequel nous évoluons. Votre moteur de règle en tient-il compte ?

La mise en place de règles pour régir l'accès à vos actifs les plus précieux vous permet donc d'élargir votre champ d'action.

EN SAVOIR PLUS

Pour de plus amples informations, *regardez cette vidéo* et écoutez des experts Dell en cybersécurité évoquer les principales menaces de sécurité auxquelles les organisations doivent aujourd'hui faire face.



Parce que les utilisateurs, les appareils, les applications et les données évoluent plus que jamais en dehors des réseaux des entreprises, **82 %** des décideurs en matière de sécurité informatique indiquent avoir repensé leurs règles de sécurité[x].

Trois recommandations pour élaborer une stratégie Zero-Trust performante

Réunissez les conditions pour mener à bien un projet de transformation Zero-Trust dans votre organisation.

2 Optez pour des appareils sécurisés.

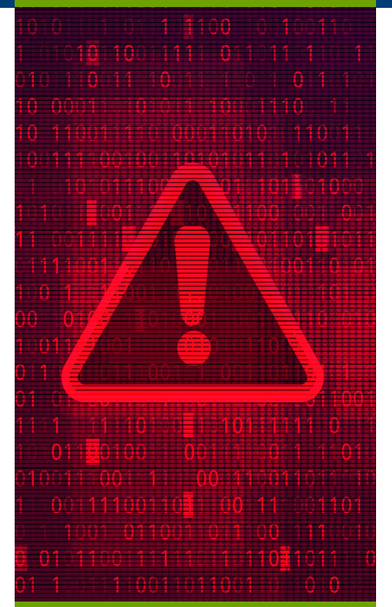
Établissez votre stratégie Zero-Trust sur des bases solides. Renforcez votre ligne de défense avec des appareils pensés et développés pour la sécurité, notamment :

A. **Protection des ressources matérielles et du firmware** pour sécuriser la pile de points de terminaison et gagner en visibilité (par ex., détecter si la sécurité du BIOS a été compromise et alerter l'équipe IT). Équipez votre organisation de technologies permettant de vérifier l'identité à chaque tentative d'accès tout en limitant au maximum leur incidence sur la productivité des collaborateurs.

B. **Contrôles d'intégrité et systèmes de protection de la chaîne logistique** pour sécuriser chaque étape du cycle de vie des PC. Ces dernières années, les chaînes logistiques ont été victimes d'attaques, parfois dévastatrices. Pour bâtir une véritable architecture Zero-Trust, les processus d'authentification, de vérification et de surveillance doivent débuter au niveau de la chaîne logistique. Travaillez avec des prestataires qui 1) adoptent des pratiques sécurisées et 2) vous permettent de valider l'intégrité de vos appareils au moment de l'achat, de la fabrication et de la livraison.

EN SAVOIR PLUS

Pour de plus amples informations sur les pratiques d'excellence en matière de sécurité des appareils, consultez le livre blanc publié par Dell et Intel, « Achieving Pervasive Security Above and Below the OS ».



En **2021**, une société de gestion informatique a été victime d'une attaque par rançongiciel qui a infecté au moins **1 500** de ses clients[xi].

Trois recommandations pour élaborer une stratégie Zero-Trust performante

Réunissez les conditions pour mener à bien un projet de transformation Zero-Trust dans votre organisation.

3

Aspirez à une intégration fluide et à plus d'interopérabilité à tous les niveaux de votre écosystème.

Pour adopter une posture de sécurité efficace de haut niveau, trois points sont essentiels :

A. l'intégration de toutes les solutions de sécurité de l'écosystème IT ;

B. la visibilité en temps réel ; et

C. la capacité à agir lorsque la situation l'impose.

À l'ère du Cloud, la moindre faille de sécurité négligée peut se transformer en un véritable cauchemar. Il est donc essentiel que tous les systèmes parviennent à identifier les menaces potentielles *et* soient paramétrés pour prendre les mesures qui s'imposent.

Vos systèmes sont-ils intégrés ou fonctionnent-ils en silos ? Votre moteur de règle peut-il déclencher un workflow spécifique dès qu'un administrateur IT est informé d'un BIOS corrompu sur le réseau ? Dans un environnement intégré, les systèmes d'automatisation doivent immédiatement mettre en quarantaine le BIOS en question, bloquer tout nouvel accès et lancer l'exécution d'un correctif.

Avez-vous une visibilité sur tous vos points de terminaison ? L'idéal est de bénéficier d'une expérience de télémétrie riche par couche, de la chaîne logistique (par ex., le quai de chargement) au firmware (par ex., les alertes de sabotage au niveau du BIOS).

Cependant, la télémétrie n'a de sens que si elle est associée à des intégrations efficaces. Pouvez-vous agir sur vos données ? Il est capital de pouvoir compter sur les bonnes ressources (par exemple, des professionnels qualifiés en cybersécurité) pour donner du sens aux workflows des données et des programmes permettant de résoudre les problèmes.

41 % des organisations se lancent dans le déploiement d'une stratégie Zero-Trust[xii]

DELL Technologies

Éléments clés à retenir

L'avenir de la sécurité rime avec Zero-Trust.

- Les vecteurs d'attaque ne cessent de se multiplier à l'approche du monde du travail de demain.
- Les failles de sécurité sont inévitables. Limitez la surface d'attaque avec des solutions de sécurité adaptées au scénario le plus catastrophique.
- Le modèle Zero-Trust est une nouvelle façon de penser la sécurité qui confère aux organisations un contrôle explicite sur leur environnement IT.
- La protection des points de terminaison qui s'articule sur les principes du modèle Zero-Trust est essentielle au maintien d'un environnement moderne sécurisé.
- Identifiez vos actifs les plus stratégiques pour hiérarchiser la construction de votre architecture Zero-Trust.
- Procurez-vous des appareils auprès de fournisseurs qui proposent des solutions de sécurité intégrées et investissent massivement dans le contrôle de la chaîne logistique.
- Évaluez la sécurité et l'interopérabilité informatique. Continuez à miser sur l'intégration des workflows pour consolider votre posture de sécurité.

Aller de l'avant

La sécurité est un sujet complexe, quelle que soit la taille des organisations. Choisissez un partenaire technologique avec une solide expérience dans le domaine de la sécurité pour vous accompagner et rationaliser votre projet de transformation Zero-Trust.

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 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.

Contactez-nous : global.security.sales@dell.com

Consultez la page : Dell.com/Endpoint-Security

Suivez-nous : LinkedIn @DellTechnologies | Twitter @DellTech

DELL Technologies

[i] Cybersecurity Almanac 2nd Edition. Cybersecurity Ventures, 2022 https://cybersecurityventures.com/cybersecurity-almanac-2022/

[ii] Ponemon Institute et IBM, Cost of a Data Breach Report, 2024 https://www.ibm.com/security/data-breach

[iii] American College of Cardiology, You Will Be Hacked. Plan Now: Cybersecurity in Health Care, 2021 https://www.acc.org/Latest-in-Cardiology/Articles/2021/11/01/01/42/Feature-You-Will-Be-Hacked-Plan-Now-Cybersecurity-in-Health-Care

[iv] Ponemon Institute et IBM, Cost of a Data Breach Report, 2024 https://www.ibm.com/security/data-breach

[v] ESG Complete Survey Results, Security Hygiene and Posture Management, 2022 https://www.esg-global.com/research/esg-complete-survey-results-security-hygiene-and-posture-management

[vi] MITRE ATT&CK https://attack.mitre.org/tactics/TA0001/

[vii] Futurum Group, Endpoint Security Trends, 2023 https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/industry-market/futurum-group-endpoint-security-trends-research-report.pdf

[viii] Verizon Data Breach Investigations Report, 2022 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[ix] Verizon Data Breach Investigations Report, 2022 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[x] Absolute Endpoint Risk Report, 2021 https://www.absolute.com/go/reports/endpoint-risk-report/

[xi] TechTarget, 2021 https://www.techtarget.com/searchsecurity/news/252503605/Kaseya-1500-organizations-affected-by-REvil-attacks

[xii] Ponemon Institute et IBM, Rapport sur le coût d'une violation de données, 2022 https://www.ibm.com/security/data-breach