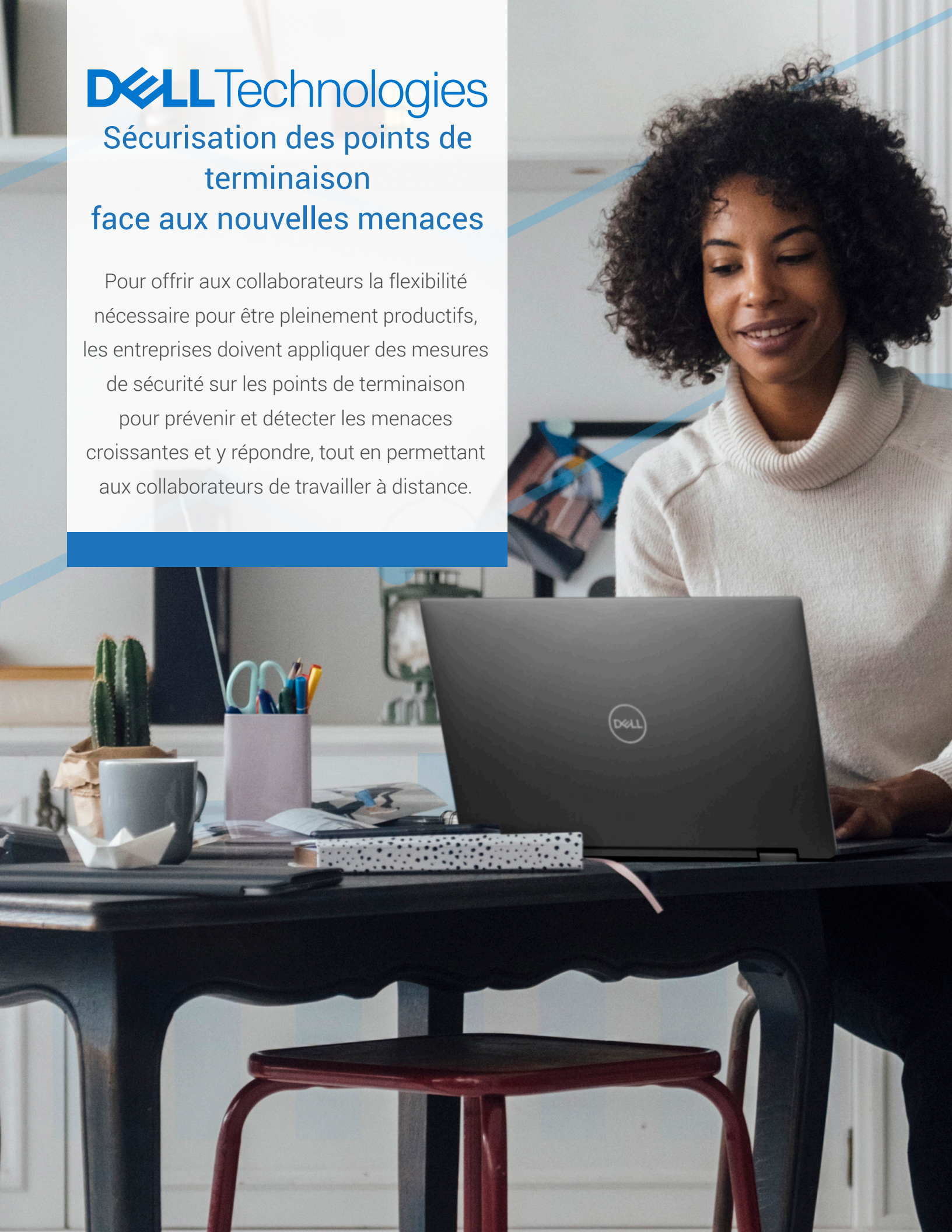
DELL Technologies

Sécurisation des points de terminaison face aux nouvelles menaces

Pour offrir aux collaborateurs la flexibilité nécessaire pour être pleinement productifs, les entreprises doivent appliquer des mesures de sécurité sur les points de terminaison pour prévenir et détecter les menaces croissantes et y répondre, tout en permettant aux collaborateurs de travailler à distance.



Tandis que les responsables IT tentent d'anticiper la fin de la pandémie de COVID-19, bon nombre d'entre eux prévoient que les télétravailleurs seront plus nombreux que jamais et que cette situation deviendra la norme. Si de nombreuses entreprises, ainsi que leurs collaborateurs, bénéficieront d'une productivité accrue et d'un style de travail plus flexible, la protection que cela implique aura un coût. La forte augmentation du télétravail liée à la COVID-19 a rendu la défense des points de terminaison plus difficile : 84 % des responsables IT affirment que la protection des télétravailleurs est plus difficile.[1] Une explication probable est l'augmentation de 148 % des attaques par logiciel de rançon sur les entreprises mondiales au cours de l'épidémie.[2] Cette statistique donne à réfléchir, car les télétravailleurs utilisent la messagerie comme principal moyen de communication professionnelle, ce qui a entraîné une augmentation de 350 % des attaques de phishing.[3]

Tendances actuelles en matière de cybersécurité

La transition soudaine vers le télétravail se déroule dans un contexte d'émergence de nombreuses inquiétudes graves en matière de cybersécurité, qui constituent des défis pour les professionnels de ce secteur. Voici quelques exemples :

1. Attaques au niveau du BIOS : vulnérabilités exploitées dans le matériel ou le silicium. Lorsque le BIOS est compromis, il arrive souvent que le pirate se dissimule pendant que l'appareil dispose d'un accès autorisé au réseau et aux données. 63 % des entreprises ont subi une compromission ou une violation de données liée à de telles attaques.[4]
2. Menaces avancées persistantes (APT) : menaces sophistiquées qui se dissimulent souvent silencieusement, car elles recueillent des informations comportementales avant de procéder au siphonnage de données précieuses. Les victimes peuvent ne pas se rendre compte pendant longtemps (108 jours en moyenne[5]) qu'une attaque silencieuse s'est produite.
3. Logiciels malveillants basés sur des fichiers et sans fichier
   - Logiciels malveillants basés sur des fichiers : il s'agit généralement de types de fichiers dotés d'extensions familières telles que .DOCX et .PDF (le type de fichiers dont les collaborateurs ont besoin pour travailler). Lorsqu'un utilisateur ouvre le fichier, un code malveillant intégré est exécuté.
   - Logiciels malveillants sans fichier : il s'agit généralement d'un programme légitime qui infecte un ordinateur. Lorsque l'utilisateur lance un programme de ce type à partir d'un e-mail, le logiciel malveillant sans fichier infecte l'ordinateur et potentiellement le réseau, échappant ainsi à de nombreuses technologies de sécurité.
4. Attaques provenant d'un État-nation : ces attaques proviennent généralement de Chine, de Corée du Nord, de Russie et d'Iran. Reposant sur l'expertise technologique et le soutien financier de ces États-nations, ces attaques sont souvent sophistiquées et très nuisibles. Cependant, bon nombre de ces attaques exploitent des systèmes qui ne disposent pas des mises à jour et correctifs les plus récents. L'unité CISA du FBI communique régulièrement des conseils.

La transition soudaine vers le télétravail se déroule dans un contexte d'émergence de nombreuses inquiétudes graves en matière de cybersécurité, qui constituent des défis pour les professionnels de ce secteur.

1. « The State of DLP 2020 », Tessian.
2. Blog VMware Carbon Black, Patrick Upatham et Jim Treinen, 15 avril 2020.
3. Rapport Google, cité sur PCMAG.com, 30 mars 2020.
4. « Match Present-Day Security Threats with BIOS-Level Control », un document Forrester Consulting sur le leadership éclairé, commandé par Dell, juin 2019.
5. The 2018 U.S. State of Cybercrime Survey.

5. Les attaques basées sur le Cloud augmentent à mesure que les applications de collaboration et de productivité basées sur le Cloud remplacent les applications de bureau. Avec l'utilisation de plus de 2 400 services Cloud dans l'entreprise moyenne, 93 % des entreprises sont modérément ou extrêmement préoccupées par la sécurité du Cloud.[6] La protection doit inclure la prévention de la perte de données (DLP) et la protection contre les menaces dans le Cloud. En outre, l'authentification de l'utilisateur doit être protégée contre l'usurpation d'identité, et les données doivent être chiffrées vers et depuis le Cloud.
6. Réglementations de conformité : elles visent à protéger les informations d'identification personnelle. Afin d'éviter que les informations d'identification personnelle ne tombent entre de mauvaises mains et ne soient finalement utilisées pour le vol d'identité, certains secteurs ont adopté des réglementations strictes imposant des pénalités sévères. Il s'agit notamment de l'HIPAA dans le secteur de la santé, de la PCI-DSS dans les services financiers et de la vente au détail, et du RGPD pour les entreprises réalisant des transactions avec des citoyens européens.
7. Risque grave : une perte de 6 000 milliards $ due à la cybercriminalité est prévue pour 2021, soit une augmentation par rapport aux 3 000 milliards $ de 2015. Les pertes sont dues à des dommages et à la destruction de données, au vol de fonds, à la perte de productivité, au vol de propriété intellectuelle, au vol de données personnelles et financières, à l'interruption post-attaque, aux dommages à la réputation et plus encore, selon Cybersecurity Ventures.[7]

Repenser la sécurité des points de terminaison

Sécurité des points de terminaison : partie intégrante de la sécurité d'entreprise
Face à un nombre de télétravailleurs plus élevé que jamais, dont beaucoup doivent gérer des données sensibles dans le cadre de leur travail, les responsables IT doivent évaluer l'état actuel de la sécurité des points de terminaison dans leur entreprise. Mais plutôt que d'examiner la sécurité des points de terminaison en elle-même, ils doivent la considérer comme une partie intégrante de la sécurité d'entreprise afin de mettre en œuvre une protection approfondie. Ils doivent donc aller au-delà des points de terminaison pour inclure le stockage, les réseaux et les services basés sur le Cloud. Une approche globale de la création « d'appareils de confiance » au sein de l'entreprise doit prendre en compte les facteurs suivants :

Sécurité intégrée
Plutôt que de s'appuyer uniquement sur des logiciels pour protéger les points de terminaison, une approche globale nécessite l'utilisation d'appareils fiables, c'est-à-dire d'appareils de l'informatique utilisateurs qui implémentent la sécurité au sein des appareils eux-mêmes. Ces appareils protègent les informations d'identification personnelle et jouent un rôle important en matière de conformité aux normes, en cas de perte ou de vol d'un appareil. Les appareils des utilisateurs finaux doivent également inclure la technologie d'écran de confidentialité afin de limiter la capacité des collaborateurs et des visiteurs du bureau à voir des informations confidentielles sur un écran d'ordinateur.

Les responsables IT doivent considérer la sécurité des points de terminaison comme une partie intégrante de la sécurité d'entreprise.

6. Cybersecurity Insiders Cloud Security Reports, 2018, 2019.
7. Cybersecurity Ventures, 2020.

Protection au-dessus et au-dessous du système d'exploitation

Au-dessus du système d'exploitation. L'équipe IT a besoin de visibilité, de surveillance et de sécurité des données ainsi que de prévention des menaces, de détection et de mesures correctives. Le chiffrement sur les appareils est également très important pour répondre aux exigences de conformité, mais il ne doit pas ralentir les performances au risque de diminuer la productivité de l'utilisateur.

Au-dessous du système d'exploitation. L'équipe IT a besoin de protection du BIOS et de l'authentification des puces en raison de la fréquence des attaques sur le firmware et le matériel. Un BIOS corrompu peut permettre aux pirates d'accéder à toutes les données d'un point de terminaison, y compris les informations d'identification, et ainsi de se déplacer au sein du réseau d'une entreprise et d'attaquer l'infrastructure IT dans son ensemble.

IA et MACHINE LEARNING

Au vu des attaques de plus en plus sophistiquées, l'utilisation de l'intelligence artificielle et de l'apprentissage automatique en matière de détection et de mesure corrective est essentielle à la protection des points de terminaison. En observant les schémas comportementaux, les algorithmes d'intelligence artificielle et d'apprentissage automatique peuvent détecter une activité inhabituelle pouvant indiquer et prévenir une violation.

Chaîne logistique sécurisée

Dans le processus de fabrication, des individus malveillants peuvent introduire des composants corrompus pour permettre une attaque par porte dérobée. Une fois qu'ils sont intégrés dans un produit fabriqué, ces composants peuvent permettre une violation qui peut être extrêmement dommageable et difficile à détecter. Il est donc essentiel pour les fournisseurs et les fabricants de mettre en œuvre des mesures de sécurité rigoureuses à des points stratégiques tout au long de la chaîne d'approvisionnement.

Appareils de confiance Dell

Dell renforce la sécurité dans chaque ordinateur à l'aide des technologies suivantes :

SafeBIOS avec BIOS Indicators of Attack (IoA) : fournit une visibilité sur les modifications du BIOS afin d'éviter toute altération. Dell conserve une image protégée hors de l'hôte pour s'assurer de l'intégrité du BIOS. SafeBIOS est désormais intégré à VMware Carbon Black Audit and Remediation, qui améliore la visibilité sur les attaques via la création de rapports automatisés et permet l'accès distant afin de corriger la corruption du BIOS.

SafeID : fournit une authentification basée sur les puces. Les informations d'identification de l'utilisateur final sont vérifiées à l'aide d'une puce de sécurité dédiée, et non à l'aide de logiciels, car cette méthode est moins sécurisée.

SafeScreen : protège les écrans susceptibles d'exposer des données sensibles aux collaborateurs, aux visiteurs, aux employés de maintenance ou à d'autres personnes non autorisées.

SafeGuard and Response. Optimisée par les technologies VMware Carbon Black et SecureWorks, la gamme Dell comprend les éléments suivants :

VMware Carbon Black : une plate-forme Cloud native de protection des points de terminaison qui allie le renforcement intelligent du système et la prévention comportementale nécessaires pour maintenir les menaces émergentes à distance, à l'aide d'un seul agent léger et d'une console facile à utiliser.

Les appareils de confiance protègent les informations d'identification personnelle et jouent un rôle important en matière de conformité aux normes, en cas de perte ou de vol d'un appareil.

Services managés SecureWorks : collectent et mettent en corrélation la télémétrie du Cloud, du réseau et des points de terminaison afin d'identifier les menaces au sein de l'entreprise. Offrant une réponse aux incidents à la pointe du secteur, les services managés SecureWorks sont intégrés à la plate-forme VMware Carbon Black ainsi qu'à de nombreuses autres plates-formes.

SafeData. La collaboration, toujours une marque de fabrique des entreprises prospères, revêt une importance accrue dans un monde où le télétravail s'est généralisé. Indispensable à la collaboration du personnel, la sécurité des données, à la fois sur les appareils et dans le Cloud, ne doit pas ralentir l'utilisateur final. Dell s'associe à Netskope et Absolute pour offrir une sécurité des points de terminaison globale.

Netskope. En adoptant une approche centrée sur les données, la technologie Netskope protège les données créées et exposées dans le Cloud. En fournissant à l'équipe IT la visibilité en temps réel, l'accès au Cloud, la surveillance et la prévention de la perte de données, Netskope redéfinit le Cloud, le réseau et la sécurité des données. Les équipes disposent d'un équilibre parfait entre protection et rapidité, ce qui leur permet de sécuriser le processus de transformation numérique de leur entreprise.

Absolute. Dell intègre la technologie Absolute dans le firmware de chaque appareil, dotant chaque point de terminaison d'un lien d'autoréparation vers le tableau de bord Absolute basé sur le Cloud. Cela permet aux responsables de suivre, de gérer et de sécuriser les points de terminaison et les données qu'ils contiennent, même lorsqu'ils sont hors du réseau. Technologie Absolute :

- Localise et gère les appareils.
- Offre la persistance du VPN et des logiciels de sécurité.
- Met en œuvre une solution isolée pour permettre la récupération après les attaques
- Inclut des solutions de protection des données multi-Cloud qui peuvent être software-defined ou basées sur une appliance.

Conclusion

Le pic de télétravail lié à la pandémie de COVID-19 accroît le danger dans un environnement de cybersécurité dans lequel les menaces sont déjà nombreuses. Une nouvelle approche globale de la protection des points de terminaison est nécessaire. La refonte de la protection des points de terminaison commence par des appareils fiables, protégés à la fois au-dessus et au-dessous du système d'exploitation. Une telle stratégie va également au-delà des points de terminaison eux-mêmes pour adopter une vision d'entreprise de la cybersécurité qui inclut les serveurs, les réseaux, les services basés sur le Cloud et la conformité aux normes. La gamme Appareils de confiance Dell incarne une approche complète. La protection des points de terminaison Dell s'étend à l'échelle de l'entreprise pour inclure des solutions de protection des données multi-Cloud qui peuvent être fournies en tant que solutions software-defined et/ou basées sur des appliances. Les appareils de confiance Dell permettent surtout aux utilisateurs de rester hautement productifs en contrant les attaques de plus en plus sophistiquées à l'ère du télétravail.

Pour plus d'informations, consultez :
https://www.delltechnologies.com/fr-fr/endpoint-security/index.htm

Indispensable à la collaboration du personnel, la sécurité des données, à la fois sur les appareils et dans le Cloud, ne doit pas ralentir l'utilisateur final.