DELL Technologies

Présentation de solution

Protégez votre infrastructure contre les rançongiciels et les cybermenaces

La gamme de stockage Dell Technologies propose des solutions sécurisées, robustes et évolutives pour tous vos besoins en matière de charges applicatives stratégiques.

Cette présentation met en évidence les méthodologies, les processus et les outils Dell Technologies qui permettent d'appliquer des pratiques de sécurité de pointe tout en veillant à la conformité et au respect des normes du secteur.

La valeur des données comporte des opportunités et des risques

Les données, cette nouvelle devise de l'économie mondiale, sont devenues la ressource la plus précieuse pour une majorité d'entreprises[1]. La capacité grandissante d'extraire des données pour en tirer des informations exploitables pousse les organisations à en créer et à en recueillir davantage. Ces données sont récoltées puis exploitées dans un plus grand nombre d'emplacements et dans des circonstances plus diverses. Cette situation a conduit à une hausse significative des volumes de données globaux, mais aussi à une explosion de la diversité et de la distribution des données. En quelques années, il est devenu évident que les données sont collectées, stockées et traitées partout, du datacenter au Cloud, en passant par la périphérie. Les opportunités de profiter de ces données et de générer de la valeur commerciale semblent infinies.

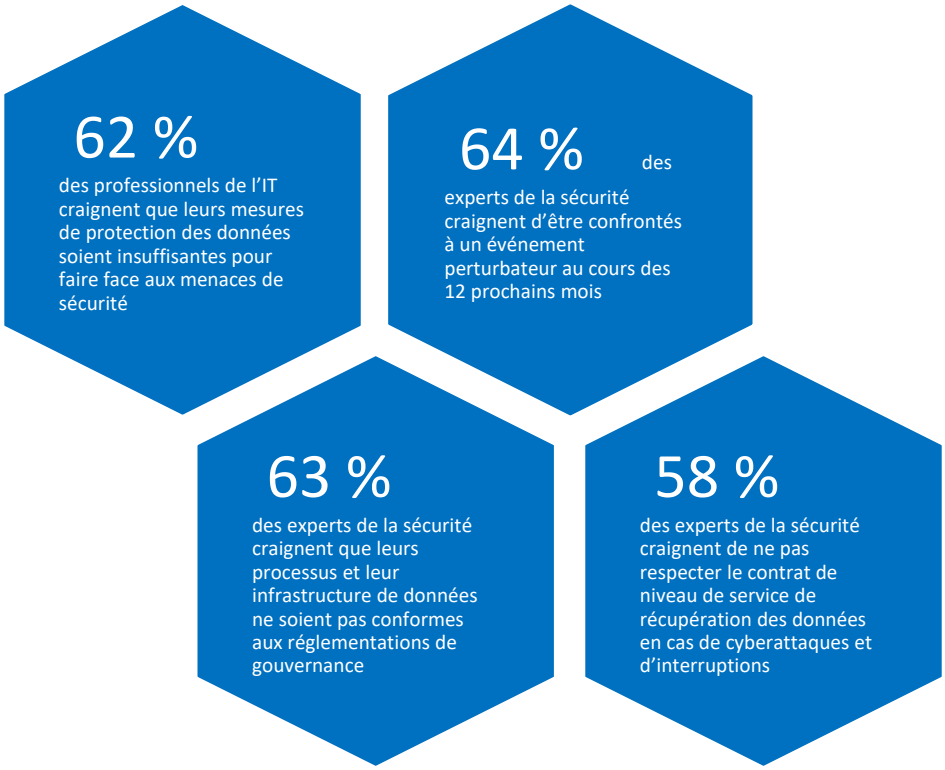
Malheureusement, cette nouvelle valeur représente également une cible de choix. Le commerce en ligne et ses connexions dynamiques reposent sur une combinaison de technologies en constante évolution. La hausse exponentielle du télétravail et « l'hyper-connectivité » générale de nos vies numériques constituent désormais un angle d'attaque informatique sans précédent que les individus malveillants cherchent régulièrement à ébranler à des fins lucratives et préjudiciables.

Que leurs motivations réelles soient idéologiques, politiques ou économiques, les cybercriminels d'aujourd'hui exploitent simultanément les failles de sécurité aux niveaux physique, logique et du composant, en analysant le matériel, les logiciels et les aspects « humains » de n'importe quel système. Les cybercriminels novices ou aguerris disposent d'un marché virtuel d'outils et de techniques allant d'approches rudimentaires à des techniques sophistiquées, comme les courriers électroniques indésirables, les logiciels malveillants, les rançongiciels et les attaques « zero-day ». Pour les individus malveillants, tous types confondus, les occasions de détourner, de prendre en otage ou de détruire vos données stratégiques sont légion. Selon le rapport Cybersecurity Ventures, des cyberattaques ou rançongiciels se produisent **toutes les 11 secondes**, ce qui, en 2021, a représenté un coût mondial colossal de **6 000 milliards de dollars**.

Des entreprises informées, mais pas préparées

La menace est bien connue, tout comme l'importance de préserver la confidentialité, la disponibilité et l'intégrité des données. Les stratégies de cyber-résilience, sous diverses formes, sont devenues obligatoires pour la majorité des organisations et responsables gouvernementaux, et sont même désormais considérées comme un avantage concurrentiel dans un monde axé sur les données.

Pourtant, en dépit de connaissances et de priorités claires, peu d'organisations s'estiment, en réalité, capables de garantir la protection et la reprise de leur activité après une cyberattaque sophistiquée. Le rapport Global Data Protection Index 2021 de Dell révèle que la majorité des professionnels de l'IT sont conscients et préoccupés par l'impact qu'une attaque pourrait avoir sur leur organisation. Parallèlement, 62 %[1] craignent que leurs mesures de protection des données soient insuffisantes pour faire face aux logiciels malveillants, rançongiciels et autres menaces du monde actuel. Ce qui est alarmant concernant l'avenir, c'est que 82 % de ces professionnels s'inquiètent que leurs solutions existantes ne répondent pas aux défis futurs en matière de sécurité.



Quelles en sont les raisons ? Selon nous, ces données illustrent la difficulté du juste équilibre à trouver pour mener à bien la gestion des risques de sécurité et réaliser les objectifs métier, en matière de délai de commercialisation, de flexibilité, de simplicité et de contrôle global des coûts. Dans la plupart des entreprises, les organisations humaines et l'infrastructure technologique vitale se sont développées en faisant l'impasse sur les besoins de sécurité modernes. De nombreuses entreprises estiment que la mise en place d'une sécurité adéquate, qu'elle soit secondaire ou partie intégrante, est onéreuse et source de bouleversements, malgré le coût très réel que représente l'inaction.

Besoin d'une approche globale et orientée métier

Pour assurer leur sécurité, les organisations ne peuvent plus se contenter d'une solution complémentaire ponctuelle. Un plan réussi doit prendre en compte l'ensemble d'un écosystème composé de solutions technologiques de bout en bout et de facteurs environnementaux, mais aussi les directives stratégiques et financières spécifiques qui rendent chaque secteur et société uniques.

En tant que leader mondial du Cloud, de l'IT et de l'infrastructure mobile, Dell est particulièrement bien placé pour accompagner les entreprises. Nos technologies de confiance en matière d'infrastructure, de calcul virtuel, de réseau et de stockage peuvent exécuter la majorité des charges applicatives mondiales dans des milliers de datacenters. Nous avons été maintes fois confrontés à des cyberattaques à tous les niveaux, c'est pourquoi nous comprenons les risques métier et les défis de devoir y répondre.

Méthodologie de sécurité Dell Technologies

L'approche de Dell est globale et orientée métier. Elle comporte des méthodes complètes qui intègrent la sécurité de bout en bout tout au long du cycle de vie des produits et des solutions. Les méthodologies de sécurité Dell s'appliquent à tous les produits de notre gamme, depuis la phase d'identification des besoins, jusqu'aux phases de conception, de lancement et de support après-vente.

La sécurité est présente dans notre ADN

Chez Dell, la sécurité et la résilience relèvent de la responsabilité de tous. Avant même que nos développeurs ne commencent à élaborer les produits, nous leur fournissons une formation rigoureuse sur les pratiques d'excellence et les politiques spécifiques au métier afin de créer une culture axée sur la sécurité dans l'ensemble de notre communauté de développement.

Dell adopte une posture de sécurité intrinsèque intégrée, du code jusqu'au déploiement

L'un des aspects de cette formation est le cycle de vie de développement sécurisé (SDL, Secure Development Lifecycle) de Dell, qui définit les contrôles de sécurité que les équipes de produits adoptent tout en développant de nouvelles fonctionnalités. Les ingénieurs matériels et logiciels Dell doivent appliquer un ensemble de procédures strictes pour éviter l'apparition de faiblesses et de failles de sécurité, issues de notre propre développement ou de composants tiers.

Le programme SDL de Dell inclut des analyses et des contrôles prescriptifs qui s'appliquent aux domaines de risque clés, à savoir la modélisation des menaces, l'analyse de code statique, la gestion des composants et les tests réguliers. Nous utilisons divers outils internes et sectoriels, y compris les listes CVE (Common Vulnerabilities and Exposures) et CWE (Common Weaknesses Enumeration) publiées par MITRE, le rapport OWASP (Open Web Application Security Project Top 10) et les contrôles SANS (Top 25 Most Dangerous Software Errors). Dell collabore également avec de nombreux organismes de normalisation, tels que SAFECode (Software Assurance Forum for Excellence in Code), BSIMM (Building Security In Maturity Model) et IEEE Center for Secure Design afin de s'assurer que les pratiques du secteur sont respectées.

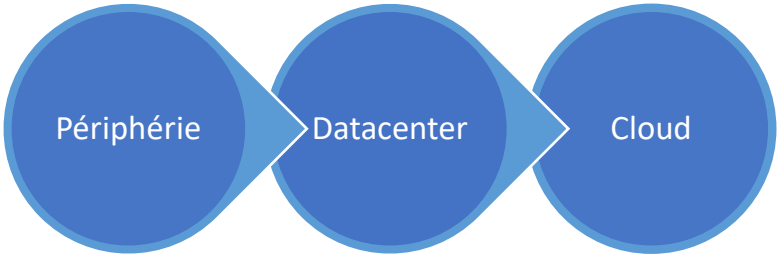
Prise en charge continue de la sécurité

Notre programme de développement de la sécurité ne s'arrête pas à la réception d'un produit Dell. Il intègre les nouvelles failles de sécurité (en particulier liées aux logiciels et firmwares) qui sont régulièrement identifiées dans l'ensemble du secteur. L'équipe PSIRT (Product Security Incident Response Team) de Dell supervise le Programme de réponse aux failles de sécurité (VRP) et est responsable de la coordination de la réponse et de la publication de toutes les failles de sécurité identifiées sur les produits. La politique de réponse aux failles de sécurité de Dell s'aligne sur les pratiques d'excellence du secteur issues du cadre PSIRT Forum for Incident Response and Security Teams (FIRST) et des normes ISO/IEC 29147 et ISO/IEC 30111. Dell fournit, en temps voulu, des informations, des conseils et des solutions à ses clients afin qu'ils limitent les risques associés aux failles de sécurité et les publie sur le portail Conseils et avis de sécurité Dell.

Les programmes SDL et de réponse aux failles de sécurité de Dell font partie intégrante des processus globaux de gouvernance du cycle de vie des produits, qui comprennent une vérification du niveau de préparation de l'entreprise et une évaluation de la sécurité interne de chaque produit.

Résultats du développement

L'attention constante que Dell porte à la cybersécurité pendant la phase de développement, à laquelle s'ajoute sa longue expérience des cas d'utilisation métier, garantit une gamme de systèmes, de solutions et de services sécurisés de classe mondiale. Que ces systèmes s'exécutent en périphérie, dans un datacenter principal, sur un site de colocation ou dans un Cloud, ils constituent la base d'une infrastructure de confiance qui favorisera l'innovation de demain.

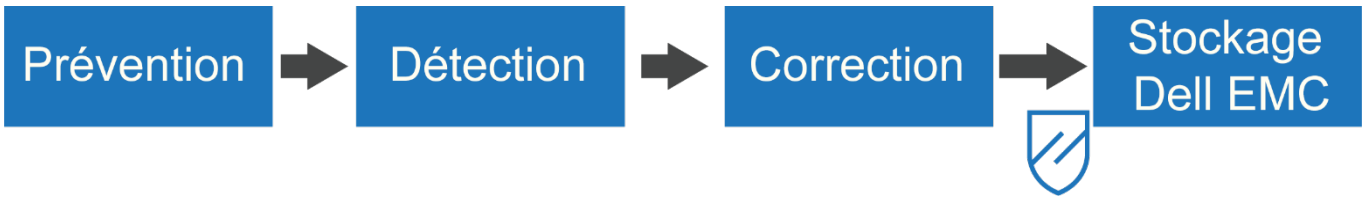


Gamme Power de Dell Technologies

PowerEdge ; PowerMax ; PowerStore ; PowerScale ; PowerFlex ; PowerVault ; PowerProtect

L'ensemble de notre gamme se compose de solutions aux finalités diverses, c'est pourquoi différentes fonctionnalités de sécurité sont déployées en fonction des besoins métier associés à chaque produit. Qu'il s'agisse de fonctionnalités Hardware Root of Trust dans la gamme de serveurs PowerEdge ou de chiffrement de bout en bout dans PowerMax, nous cherchons à répondre aux besoins de sécurité uniques de la manière la plus rentable, automatisée et évolutive possible.

Chaque solution Dell Technologies fournit un éventail de fonctionnalités de sécurité dans les catégories générales suivantes.



Prévention

Le premier élément d'une cybersécurité résiliente est la prévention. La prévention des activités malveillantes et des accès utilisateur non autorisés ainsi que le renforcement de tous les points d'accès au stockage réduisent les risques. Les produits de stockage Dell Technologies offrent un contrôle d'accès robuste basé sur les rôles (RBAC) pour permettre uniquement aux utilisateurs autorisés d'effectuer des opérations désignées, telles que le provisionnement du stockage, l'administration du réseau et la configuration des paramètres VMware. En outre, PowerMax offre une option de snapshot sécurisé pour garantir la sécurité des données en empêchant la suppression de snapshots effectuée par des individus malveillants.

Les solutions de stockage Dell intègrent une authentification multifacteur avancée pour contrôler les opérations de stockage sensibles, ainsi qu'un pare-feu, le verrouillage des ports SAN et un ID d'hôte sécurisé afin de limiter uniquement l'accès aux hôtes autorisés. Les journaux d'audit inviolables garantissent le suivi de l'utilisation et des modifications des systèmes, afin que les administrateurs IT puissent identifier les activités suspectes et réagir.

Dell garantit également la sécurité de vos données au repos. Le chiffrement des données protège le contenu des lecteurs Flash contre tout accès non autorisé, même après avoir été retirés du datacenter. Les exigences strictes de sécurité FIPS 140-2 et la gestion contrôlée des clés sont respectées pour obtenir le plus haut niveau de confiance en matière de sécurité en tant que dépositaire de données, sans compromettre les performances ni l'évolutivité.

Détection

Après avoir pris toutes les mesures de prévention, le stockage Dell surveille en permanence les activités des systèmes pour détecter les événements suspects à l'aide d'outils et de processus compatibles avec l'apprentissage automatique afin de prévenir rapidement tout impact négatif. Les produits de stockage Dell permettent une intégration fluide avec CloudIQ, l'application AIOps de Dell qui surveille et analyse la sécurité, la capacité et les performances de l'infrastructure et fournit des recommandations. La solution de cybersécurité CloudIQ vous avertit des erreurs de configuration de la sécurité de l'infrastructure en comparant les configurations réelles à celles souhaitées (par exemple, d'après les normes NIST 800-53 r5 et NIST 800 -209) et recommande des mesures correctives. Ces informations de veille vous aident à préserver l'état d'intégrité de la sécurité de votre environnement de stockage.

Ransomware Defender pour PowerScale permet aux équipes IT de devancer les cybercriminels en détectant des schémas d'accès aux données inhabituels et des comportements suspects indiquant une attaque par rançongiciel.

Correction

La correction rapide des problèmes et la restauration de l'infrastructure ont un impact très positif sur les résultats opérationnels. Les produits de stockage Dell Technologies offrent une disponibilité et une capacité robustes de restauration des données grâce à des services éprouvés tels que les réplications de données locales et distantes, les fonctionnalités de sauvegarde et de restauration directes des données, et la solution Cyber Recovery avec une protection par air gap pour se prémunir contre les rançongiciels et autres menaces modernes.

Les produits de stockage Dell sont encadrés par une réglementation stricte en matière de conformité et de sécurité, ils répondent aux exigences de la certification FIPS 140-2, des critères communs, du renforcement STIG (Security Technical Implementation Guides) et de la certification de la liste des produits approuvés par le ministère américain de la Défense.

Conclusion

Les cyberattaques continueront d'être une menace pour les entreprises, mais avec Dell Technologies, vous aurez l'esprit tranquille en sachant que vos données et vos ressources IT sont sécurisées, protégées et disponibles. Rien ne nous arrête pour contrer les menaces, grâce à une infrastructure et des appareils intrinsèquement sécurisés, une détection et une réponse complètes, la protection des données et la cyber-récupération.

Plus de 95 % des entreprises du classement Fortune 100 utilisent les produits de stockage fiables de Dell pour exécuter leurs charges applicatives stratégiques. Les principales entreprises du secteur financier, de la santé, du transport, des télécommunications, de la vente au détail, de l'énergie, de l'aérospatiale et de la défense utilisent les solutions de stockage différenciées de Dell pour garder une longueur d'avance dans le cadre de leur transformation de l'IT afin de fournir des services sécurisés et optimisés à leurs utilisateurs.

Étapes suivantes

Êtes-vous prêt à améliorer votre protection des données et la résilience de votre infrastructure IT stratégique ? L'évaluation de la cyber-résilience de Dell est un contrôle d'intégrité de la sécurité gratuit de 5 minutes qui fournit des informations et des recommandations d'experts d'Enterprise Strategy Group (ESG). Ensuite, consultez le Global Data Protection Index 2021 de Dell et la page Web Dell Technologies dédiée à la sécurité pour découvrir en quoi la protection des données joue un rôle clé dans la transformation de votre IT et l'optimisation de la valeur de vos données. Vous pouvez également regarder une courte vidéo sur la cyber-résilience de PowerMax et PowerSore pour obtenir des informations sur la sécurité que ces produits proposent.

[1] D'après l'étude « Global Data Protection Index 2021 Snapshot », réalisée par Vanson Bourne à la demande de Dell Technologies, février à mars 2021. Les résultats sont issus de la consultation d'un total de 1 000 décideurs informatiques dans le monde entier provenant d'organisations privées et publiques de plus de 250 collaborateurs.