PRÉSENTATION ESG

La cyber-résilience est essentielle pour le stockage stratégique

Date : Octobre 2022 **Auteurs :** Scott Sinclair, directeur de cabinet et Monya Keane, analyste de recherche senior

RÉSUMÉ : L'environnement IT a changé. Étant donné que les données sont devenues des ressources à forte valeur ajoutée, les cybermenaces sont également monnaie courante. Ainsi, la cyber-résilience doit être un principe fondamental lors du choix d'un stockage stratégique. Avec PowerMax, Dell Technologies renforce un peu plus sa position de leader du stockage stratégique en créant et en intégrant des fonctionnalités de cyber-résilience essentielles directement dans ces systèmes.

Présentation

Les données sont une ressource vitale et extrêmement précieuse pour l'entreprise. L'étude d'ESG montre que 59 % des organisations interrogées identifient les données comme étant essentielles à leur activité, et ce pourcentage devrait atteindre 81 % d'ici deux ans.[1] Le rôle d'une infrastructure de stockage stratégique est de préserver, protéger et fournir les données qui sous-tendent les charges applicatives et les applications qui ne doivent jamais tomber en panne.

Pendant des décennies, déployer un « stockage stratégique » signifiait fournir les performances et l'échelle requises, tout en garantissant une disponibilité permanente pour se protéger contre les échecs de composants, les pannes du site, les erreurs utilisateur et les catastrophes naturelles. Aujourd'hui, les attaques malveillantes sont de plus en plus répandues. Les principes fondamentaux du stockage stratégique doivent donc évoluer au-delà de ces fonctionnalités traditionnelles pour inclure l'amélioration de la posture de cyber-résilience d'une organisation.

Dell Technologies, un leader du stockage d'entreprise, continue de faire évoluer sa plateforme de stockage phare, PowerMax, pour répondre aux besoins stratégiques des environnements IT les plus exigeants. Les efforts d'innovation récents de Dell ont porté sur l'enrichissement de la gamme PowerMax avec une série de fonctionnalités robustes permettant d'améliorer la posture de cyber-résilience de toute organisation qui cherche à mieux protéger ses données et ses applications vitales, à préserver sa réputation de marque et à atteindre le succès à long terme.

Les cybermenaces qui pèsent sur les données sont omniprésentes

Parallèlement à l'augmentation des cybermenaces, la complexité informatique s'est également amplifiée. Près de la moitié (46 %) des personnes interrogées par ESG affirment que l'IT est aujourd'hui plus complexe qu'il y a deux ans. L'évolution rapide du paysage de la cybersécurité (citée par 37 %) et les efforts visant à respecter les nouvelles réglementations en matière de sécurité et de confidentialité des données (citées par 32 %) sont deux des facteurs de cette complexité IT les plus fréquemment identifiés.[2]

Malheureusement, les organisations peinent actuellement à recruter suffisamment de talents qualifiés dans le domaine de la cybersécurité pour surmonter cette complexité. 48 % des organisations interrogées rapportent qu'elles ne disposent pas de suffisamment d'experts en cybersécurité au sein de leur personnel. Il s'agit du type de pénurie de compétences le plus souvent cité dans l'IT d'entreprise actuellement.[3]

[1] Source : rapport d'étude ESG, *Data Infrastructure Trends*, novembre 2021.
[2] Source : Résultats complets de l'enquête ESG, *2022 Technology Spending Intentions Survey*, novembre 2021.
[3] Ibid.

Les rançongiciels et les logiciels malveillants sont monnaie courante

Parmi les multiples menaces auxquelles les entreprises sont confrontées, les attaques de rançongiciels externes et de logiciels malveillants sont devenues pratiquement inéluctables. Dans une récente enquête d'ESG menée auprès de professionnels de l'IT et de la cybersécurité qui supervisent les technologies et les processus associés à la protection de leur société contre les rançongiciels, 79 % ont signalé avoir été confrontés à une tentative d'attaque par rançongiciel au cours des 12 derniers mois. 30 % ont déclaré que ce type d'attaques se produisait chaque semaine, voire plus fréquemment.[4]

Parmi les organisations ayant été confrontées à une tentative d'attaque, 73 % ont été touchés par au moins une attaque réussie. Or, dans ces circonstances, payer la rançon n'est pas une stratégie optimale et peut même s'avérer peu judicieux. 56 % des organisations victimes d'une attaque réussie ont payé. Toutefois, parmi celles qui ont payé la rançon demandée :

- **87 %** d'entre elles ont ensuite subi d'autres tentatives d'extorsion pour obtenir plus d'argent. En fait, 61 % des organisations qui ont payé tout de suite ont fini par devoir payer encore plus d'argent ultérieurement.[5]
- **Seules 14 %** ont récupéré 100 % de leurs données, même après le paiement de la rançon.
- Et **61 %** n'ont récupéré que 75 % ou moins de leurs données après avoir payé.

De toute évidence, une protection complète contre les rançongiciels nécessite une stratégie avec plus de facettes, qui intègre plusieurs technologies et outils axés sur la détection, la prévention et la récupération.

De nombreuses organisations calquent désormais leurs stratégies de cyber-résilience sur les recommandations fournies par le cadre de cybersécurité NIST, qui recommande aux organisations d'identifier et de protéger les ressources critiques, de détecter les défaillances et les violations, et de planifier la réponse et la récupération à partir des cyberincidents. Un autre composant du cadre NIST largement adopté par les organisations est l'architecture Zero-Trust, qui rejette le concept de périphérie de réseau de protection en faveur de la philosophie suivante : « Ne jamais faire confiance, toujours vérifier ». Dans ce modèle, la configuration de la sécurité des utilisateurs (même des personnes travaillant au sein de l'organisation) doit être validée de manière répétée et routinière pour que ces utilisateurs puissent accéder aux applications/données.

Les systèmes de stockage doivent absolument faire partie de cette approche de cybersécurité. Après tout, le composant d'infrastructure le plus fréquemment ciblé par les attaques par rançongiciels est le matériel de stockage, selon l'étude d'ESG. Cette réponse a été la plus citée (40 % des personnes interrogées).

Comment le stockage stratégique améliore la résilience contre les rançoncigiels

Les attaques par rançongiciels consistent à accéder à des données métiers importantes, puis à les chiffrer. De nombreuses stratégies de cyber-résilience reposent sur des outils et des technologies qui se concentrent sur la **prévention** des menaces en les empêchant d'accéder aux données et la **détection** précoce des attaques qui y parviennent. Mais avec les rançongiciels, il est également important de se focaliser sur la **récupération accélérée**.

Les systèmes de stockage stratégiques se trouvent à un endroit du chemin d'accès des données qui est idéal pour faciliter la récupération rapide des données après une attaque. Par exemple, face à l'augmentation du nombre d'attaques réussies par rançongiciels, certains systèmes de stockage ont été en mesure de tirer parti de leurs fonctionnalités intégrées afin de faciliter une récupération rapide en conservant et en fournissant des copies sécurisées et immuables des volumes de données.

[4] Source : rapport de recherche d'ESG, *The Long Road Ahead to Ransomware Preparedness*, juin 2022. Sauf indication contraire, toutes les références de la recherche d'ESG figurant dans cette présentation sont issues de ce rapport de recherche.
[5] Source : résultats de l'enquête complète d'ESG, *The Long Road Ahead to Ransomware Preparedness*, juin 2022.

Ce type de support est incroyablement profitable pour accélérer la récupération. Les snapshots peuvent rapidement être identifiés comme des volumes « vérifiés » et être récupérés rapidement par le département IT pour restaurer les jeux de données tels qu'ils étaient auparavant. Toutefois, pour les environnements applicatifs stratégiques, *la technologie de stockage doit faire encore plus*.

Dell PowerMax peut améliorer la posture de cyber-résilience d'une organisation

Les noms de produits ont changé et le nombre de fonctionnalités a augmenté au fil des décennies, mais les systèmes de stockage d'infrastructure stratégique de Dell Technologies mènent la danse depuis que le stockage d'entreprise a été établi comme une catégorie distincte de l'IT par EMC à la fin des années 1980. Aujourd'hui, Dell PowerMax offre plusieurs fonctionnalités conçues pour répondre aux exigences élevées des charges applicatives stratégiques, notamment :

- L'architecture scale-out à plusieurs contrôleurs All-NVMe pour des performances optimales et prévisibles à grande échelle.
- La consolidation massive des charges applicatives, avec prise en charge de divers environnements applicatifs en modes bloc et fichier couvrant les charges applicatives mainframe, les systèmes sur matériel vierge, les machines virtuelles, les conteneurs, etc.
- Les plus hauts niveaux de sécurité, de disponibilité et de résilience. PowerMax fournit une disponibilité de 99,9999 % avec le chiffrement des données de bout en bout des hôtes vers PowerMax, le chiffrement des données au repos et les snapshots sécurisés. Plus précisément, la plateforme prend en charge jusqu'à *64 millions de snapshots par baie*, selon Dell. En outre, le logiciel de reprise après sinistre Symmetrix Remote Data Facility (SRDF) de Dell utilise des topologies et des fonctionnalités d'automatisation avancées pour fournir une base solide pour la résilience. Avec SRDF, les organisations peuvent même créer un coffre protégé par « air gap ». Les données y sont isolées et la connexion au coffre est intermittente et hautement restreinte.

Dell a conçu PowerMax pour la résilience

Récemment, Dell a consacré ses efforts à la création et à l'intégration de fonctions de sécurité encore plus complètes dans PowerMax. Par exemple, PowerMax est désormais adapté aux environnements de sécurité Zero-Trust et s'appuie sur les sept piliers de la sécurité Zero-Trust de Dell, y compris la protection/sécurité intrinsèque du système lui-même contre les attaques, avec les fonctionnalités suivantes :

- Racine de confiance matérielle immuable : ces fonctionnalités authentifient les modifications matérielles et logicielles entre les nœuds, les boîtiers de supports et la station pilote. Les clés de chiffrement intégrées et immuables au niveau des composants sont physiquement fusionnées dans la mémoire par le site de fabrication Dell.
- Chaîne de confiance Secure Boot ces fonctionnalités établissent et étendent une « chaîne de confiance » du firmware contre les rootkits malveillants du démarrage, du noyau et du pilote. La chaîne de confiance sécurisée utilise l'authentification cryptographique pour les chargements de firmware suivants/chargeurs de démarrage en fonction des signatures Dell.
- Mises à jour de firmware signées numériquement : PowerMax utilise également l'authentification des signatures numériques Dell pour se protéger contre les mises à jour non autorisées de firmwares. La plateforme effectue des analyses des composants de type nœud, support et station pilote à l'aide de clés d'authentification cryptographique.

En plus de cette conception fiable, PowerMax offre des fonctionnalités supplémentaires pour améliorer la prévention, la détection et la récupération en cas d'attaques par rançongiciels et autres menaces de cybersécurité.

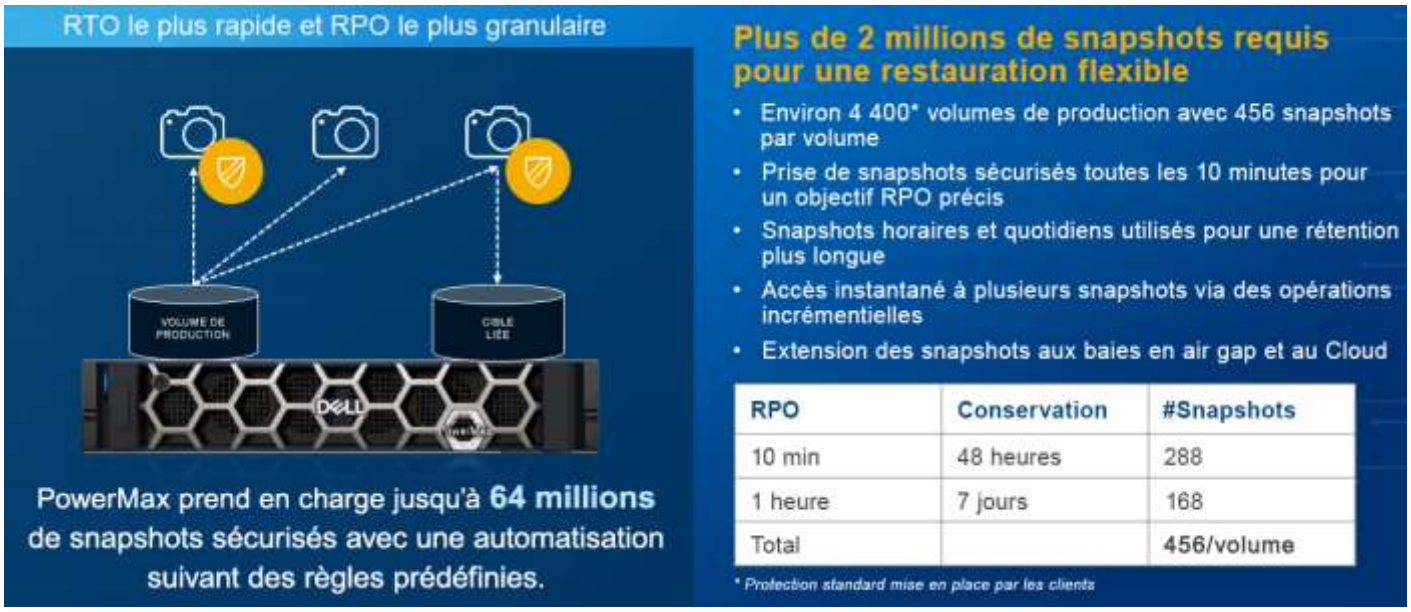
Pour la **prévention**, en plus de posséder une sécurité matérielle intégrée, PowerMax aide à prévenir les attaques grâce à sa sécurité avancée qui empêche l'accès par des utilisateurs non autorisés, bénéficiant des certifications de sécurité Critères communs, Renforcement STIG/APL et FIPS 140, et prenant en charge les mécanismes de contrôle d'accès administrateur de confiance, tels que :

- L'authentification multifacteur SecurID pour vérifier l'identité d'un administrateur.
- La prise en charge des cartes à puce CAC/PIV contenant un certificat/clé privée pour accéder aux ressources en ligne au sein du gouvernement fédéral des États-Unis.
- Les contrôles d'accès basés sur les rôles (RBAC), la prise en charge LDAP et zDP 2 Actor (nécessitant que deux personnes exécutent certaines commandes zDP), pour que seuls les utilisateurs autorisés puissent effectuer certaines opérations telles que le provisionnement du stockage.

Pour la **détection**, le matériel PowerMax et le logiciel d'IA Dell CloudIQ offrent une détection des anomalies liées aux logiciels malveillants. Il s'agit d'alertes de conformité basées sur les protocoles d'alerte de cybersécurité, ainsi que sur les alertes et exportations de journal syslog sécurisées. Plus précisément, CloudIQ détecte rapidement les cyberattaques en surveillant l'utilisation inhabituelle du stockage PowerMax et les indicateurs d'activité suspects. Le logiciel alerte ensuite les administrateurs en cas de modifications radicales dues à un éventuel chiffrement. Il peut également surveiller en permanence l'infrastructure de stockage pour identifier automatiquement les risques de cybersécurité liés à des paramètres système mal configurés, puis fournir des recommandations détaillées pour corriger ces problèmes.

Enfin, pour la **récupération**, la technologie de snapshots sécurisés PowerMax a fait passer la sécurité et la protection des données au niveau supérieur. Selon les objectifs de niveau de service de l'entreprise, le département IT peut configurer jusqu'à 64 millions de copies de snapshots sur chaque baie PowerMax (voir Figure 1).

Figure 1. Comment PowerMax favorise la cyber-récupération rapide



Source : Dell Technologies

Cette fonctionnalité permet à PowerMax de prendre en charge les pertes de données maximales admissibles (RPO) datant seulement de quelques minutes avant la réussite d'une attaque. Avec autant de snapshots, le département IT disposera de suffisamment de copies pour protéger les environnements de stockage stratégiques, même volumineux et consolidés, pratiquement à la minute près, ce qui permettra une restauration quasi instantanée des applications stratégiques. Ce niveau de flexibilité de protection change la donne pour les environnements de production à grande échelle. Selon Dell, PowerMax offre la cyber-récupération la plus granulaire à l'échelle pour optimiser le RPO.

Dell peut également ajouter l'option PowerMax Cyber Recovery Vault pour les organisations qui ont besoin d'une option de restauration par air gap de coffre à distance (SRDF), avec isolement physique/restauration orchestrée pour les systèmes ouverts et le stockage mainframe. L'offre PowerMax Cyber Recovery Vault sera proposée en disponibilité générale plus tard ce mois-ci. Elle utilise la réplication à distance SRDF pour créer un air gap. Cette solution est conçue pour les clients qui ont besoin d'avoir une copie des données en dehors de leur réseau de production avec restauration rapide (RTO). Alors que les clients PowerMax déploient cette configuration manuellement depuis un certain temps, l'annonce de ce mois-ci inclut l'automatisation de l'orchestration du déploiement et les services Dell Professional Services pour rationaliser l'installation.

Ce qu'il faut retenir

Dell n'est généralement pas le premier nom qui vient à l'esprit quand on pense aux fournisseurs de sécurité. Il faut que cela change. Les cybercriminels sont de plus en plus organisés et leurs menaces de plus en plus sophistiquées. Dell a réalisé et continue de réaliser des investissements importants dans la lutte contre ces menaces, la protection des données et la simplification de l'intégralité de la gestion de la sécurité et de la résilience.

Les données constituent les ressources les plus stratégiques d'une entreprise. Elles doivent être protégées et disponibles en permanence. Les dernières menaces pesant sur cette disponibilité sont les rançongiciels, les logiciels malveillants et autres cyberattaques. Oui, PowerMax possède une solide réputation en matière de prise en charge des charges applicatives stratégiques haut de gamme. Dell le fait depuis des années, mais les nouvelles fonctionnalités de PowerMax sont adaptées à presque tous les acheteurs de stockage d'aujourd'hui. Chacun craint les rançongiciels, les logiciels malveillants et le fait de faire la une des journaux.

Et il ne s'agit pas de combattre les voleurs qui tentent de s'enrichir. Il se peut que ces pirates travaillent au service d'un gouvernement étranger et volent des propriétés intellectuelles dans le but de renforcer leur propre sécurité nationale ou leur force militaire. S'ils arrivent à chiffrer vos données, au-delà du fait qu'ils vous empêchent d'y accéder, on ne sait pas ce qu'ils peuvent en faire d'autre.

Si vous disposez d'informations professionnelles qui ne doivent absolument pas être mises entre les mains de personnes mal intentionnées, contactez Dell pour discuter de la manière de protéger une infrastructure de stockage.

Enterprise Strategy Group est une entreprise intégrée d'analyse, de recherche et de stratégie technologiques qui fournit des données relatives aux marchés, des renseignements exploitables et des services de commercialisation à la communauté IT internationale.

www.esg-global.com contact@esg-global.com +1 508.482.0188