Livre blanc d'entreprise

Bien comprendre les tenants et les aboutissants de la protection des données moderne

Les menaces actuelles imposent une protection et une sécurité Edge to Cloud

3 Synthèse

3 Introduction

4 La croissance exponentielle des données accroît les risques

4 Les conséquences des attaques malveillantes sur les données

5 Une stratégie à grande échelle pour les menaces importantes

5 Fonctionnement de la protection des données

5 Vulnérabilité des données : la lutte contre les ransomwares

6 Tendances et défis en matière de cybersécurité

6 Avantages d'une protection des données moderne

7 Les bons services, les bonnes technologies et les bons experts

8 Conclusion

Synthèse

Les données sont le bien le plus précieux d'une entreprise. Pourtant, nombre d'entre elles ne parviennent pas à traiter ce trésor comme il se doit. Alors que les menaces ne cessent de s'aggraver, les efforts de modernisation et de transformation placent les données dans une multitude de silos et de nouveaux environnements d'hébergement, de l'edge au cloud. Cette complexité accentue la vulnérabilité des données face aux attaques sophistiquées des hackers d'aujourd'hui.

Les approches existantes de protection des données sont de plus en plus défaillantes. Traditionnellement, l'approche de base des clients consistait à copier les données modifiées dans chaque environnement de production et à stocker ces copies dans un emplacement secondaire. Cette opération était généralement réalisée une fois par jour pendant les heures creuses, le plus souvent la nuit pour éviter tout impact sur les performances de l'infrastructure. Cette approche périodique laisse pourtant à désirer dans notre environnement changeant soumis à de nombreuses cybermenaces. Les services informatiques qui cherchent à protéger, récupérer et sécuriser des volumes énormes et croissants de données sont ainsi confrontés à plusieurs défis :

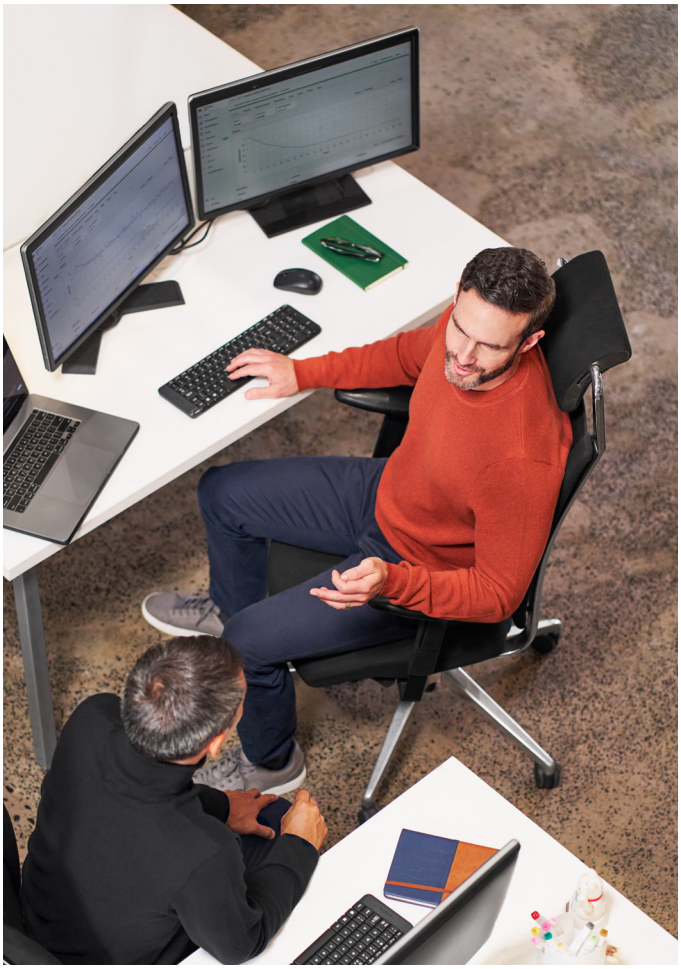
— Incapacité à contrer rapidement les cyberattaques, telles que les ransomwares et les programmes malveillants
— Complexité de gestion et d'utilisation, avec de multiples points de contact d'administration et de maintenance du matériel et des logiciels de protection des données sur site ou dans les environnements de cloud hybride
— Silos de données avec des solutions ponctuelles fragmentées
— Augmentation des coûts, surprovisionnement en capacité et sous-utilisation des ressources en raison d'une planification inefficace de la croissance des données ou, dans le pire des cas, sous-provisionnement qui accroît les risques
— Explosion de la croissance des données, exigences élevées en matière d'accords de niveaux de service (SLA) de reprise et évolution des menaces et de la conformité qui exercent une pression considérable sur les coûts et intensifient les risques
— Pertes de données entre le moment effectif de reprise et la dernière copie intègre des données
— Processus de reprise longs et complexes, qui limitent la capacité à reprendre l'activité

Il faut donc mettre en œuvre des mesures exhaustives et homogènes de protection des données pour en assurer l'intégrité et la disponibilité et garantir leur maintenance en continu, quels que soient leur emplacement et leur plateforme d'hébergement. Une solution solide qui reste en place 24 h/24 et 7 j/7 et garantit que les données sont sauvegardées en intégralité et prêtes pour une restauration immédiate est essentielle pour limiter les dommages potentiels des attaques par ransomware ou d'autres programmes malveillants.

Introduction

La bonne nouvelle, c'est que des technologies de pointe font de la protection des données homogène et efficace une réalité. Les solutions modernes de sauvegarde et de reprise après sinistre peuvent éliminer les silos de données et protéger ces dernières, qu'elles soient au repos ou en transit d'un emplacement à un autre au cours de leur cycle de vie.

Ce livre blanc évoque la nécessité d'adopter une stratégie de protection des données sécurisée avec une approche complète, unifiée et continue pour éviter les pertes ou les piratages de données dus à des intrusions, notamment en cas de ransomware ou de modification de votre code par un programme malveillant. Dans un monde où la cybercriminalité prolifère, avec des attaques dans tous les secteurs d'activité ainsi que sur les fournisseurs d'eau/d'énergie et les organismes publics, les services informatiques ne peuvent relâcher leur vigilance.



Protection des données et sécurité des données

Dans ce livre blanc, une différence est faite entre la protection des données et la sécurité des données :

— **Protection des données :** programme omniprésent et holistique de contrôles, de processus et de contre-mesures qui garantissent la disponibilité et l'intégrité des données, quel que soit leur emplacement.

— **Sécurité des données :** processus et protocoles spécifiques visant à protéger les données des menaces, des agents malveillants ou même des suppressions accidentelles sur l'emplacement de stockage, au moment des transits et lors du traitement des données.

La croissance exponentielle des données accroît les risques

La plupart des services informatiques sont inondés de données, mais ils doivent les protéger à l'aide de technologies obsolètes qui les mènent droit à la catastrophe technologique. Selon une récente étude d'IDC commanditée par Zerto, une société Hewlett Packard Enterprise, 93 % des organisations interrogées ont connu des interruptions liées à des données et 68 % d'entre elles ont enregistré plus de quatre événements entraînant une interruption de l'activité[1].

La prévalence des cyberattaques accroît considérablement les chances d'être victime d'un piratage de données, ce qui représente un risque important pour les opérations de l'entreprise. Cette même étude a révélé que les participants ont enregistré 19,3 cyberattaques (de tous types) et 2,3 attaques par ransomware en moyenne au cours des 12 derniers mois. En outre, 83 % des participants ayant subi une attaque ont signalé une corruption des données associée. Pire encore, 60 % d'entre eux ont également fait les frais d'une perte de données irrécupérables au cours des 12 derniers mois.

Il n'est donc pas étonnant que l'amélioration de la sécurité et de la protection des données fasse aujourd'hui autant figure de priorité pour les services informatiques. Les données en silos, la croissance des données, le développement des menaces dues aux ransomwares et aux autres programmes malveillants et la prolifération des données au cœur, sur le cloud et à l'edge ont aggravé la complexité à un niveau inédit, ainsi que les risques de pertes de données encourus par les entreprises du monde entier.

Les conséquences des attaques malveillantes sur les données

Cet état d'urgence virtuel nécessite une stratégie pour réduire l'exposition aux risques en évitant en premier lieu les piratages de données et les dommages dus aux modifications non autorisées. Les conséquences d'attaques malveillantes sur les données incluent :

— Les dommages liés à la réputation de l'entreprise
— L'impossibilité de fonctionner à court ou à long terme ou même l'arrêt complet
— Les coûts élevés de la remédiation
— Les sanctions sévères liées à la conformité (notamment par rapport aux lois sur la confidentialité)
— Les pertes potentielles d'avantage concurrentiel sur le marché

[1] « State of Ransomware and Disaster Preparedness for 2022 », IDC, mai 2022

Une stratégie à grande échelle pour les menaces importantes

Une autre approche est nécessaire pour que chaque organisation réduise efficacement le risque croissant de perte de données, atténue les menaces en provenance de ransomwares sophistiqués et assure une récupération rapide des données à la suite d'un incident de petite ou grande ampleur. Une stratégie de protection des données générale et sécurisée doit donc être adoptée pour toute l'entreprise, mais également ses avant-postes (filiales), les travailleurs à distance et les entités partenaires qui ont accès aux données pour des projets communs et dans le cadre d'une collaboration.

Une stratégie globale implique également des sauvegardes cloud hybrides protégées et des processus de restauration rapide pour réduire les risques de temps d'arrêt et améliorer la cyber-résilience face aux menaces constantes et changeantes des ransomwares.

Fonctionnement de la protection des données

La protection des données englobe la sécurité des données, mais également leur sauvegarde, leur récupération et leur archivage, ainsi que la reprise après incident et la continuité de l'activité. Une protection des données continue et complète est nécessaire pour réussir : elle doit être simple, robuste et fluide. Les solutions multipoints sont donc tout simplement inadaptées. Dans la mesure où l'emplacement et l'utilisation des données changent constamment, la protection des données doit suivre le rythme pour réduire les risques de perte de données, garantir une récupération rapide des données, évoluer via l'automatisation pour assurer une protection contre les menaces changeantes et couvrir la mobilité des données sur l'ensemble de leur cycle de vie.

Vulnérabilité des données : la lutte contre les ransomwares

Alors que les données d'entreprise résident désormais dans de multiples endroits en dehors du périmètre du pare-feu traditionnel, elles sont exposées à de graves vulnérabilités, créant une faille de sécurité qui ne cesse de progresser. Par exemple :

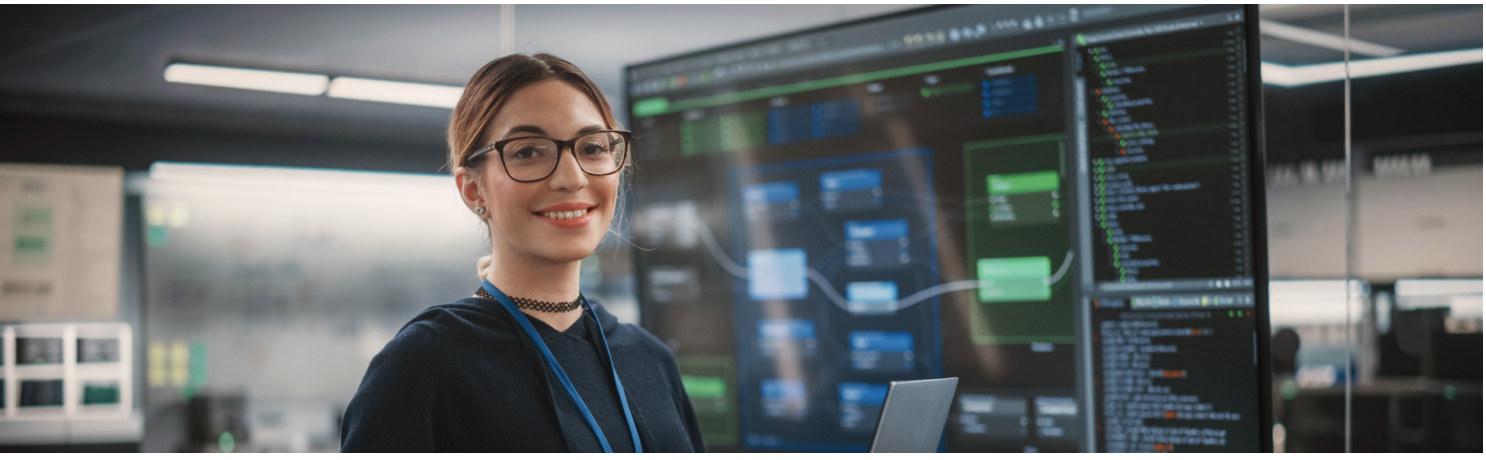
— Une étude réalisée en 2022 a révélé que 94 % des hackers ciblaient les référentiels de sauvegarde, et que 72 % des attaques atteignaient au moins en partie leur objectif[2].

— Dans la même étude, 52 % des personnes interrogées ont signalé un écart entre les stratégies de leur entreprise en matière de cybersécurité et de continuité de l'activité d'une part, et de reprise après sinistre de l'autre, indiquant que des améliorations étaient nécessaires.

— En 2023, des études ont signalé que 43 % des cyberattaques avaient ciblé des petites entreprises, dont 60 % ont dû déposer le bilan dans les six mois suivant l'attaque[3].

Ce niveau d'exposition ouvre la porte à de futures attaques et complique les efforts de récupération de données.

Les programmes malveillants de type zero-day sont de plus en plus répandus et les logiciels antivirus ne sont pas forcément efficaces contre ces menaces changeantes. La sauvegarde de vos données est cruciale, mais il est indispensable de se pencher sur la granularité pour lutter contre les ransomwares. Les méthodes de sauvegarde traditionnelles ne fournissent pas cette granularité, ce qui accroît le risque pour la plupart des organisations ne procédant pas à des sauvegardes régulières en cas d'attaque. Elles peuvent même perdre plusieurs jours de données, ce qui peut être désastreux et coûteux pour l'organisation.



[2] « Paying the ransom is not a good recovery strategy », Help Net Security, mai 2022

[3] « 30 Surprising Small Business Cyber Security Statistics », Fundera, 2023

Une solution idéale pour éviter les pertes dues aux ransomwares consiste à utiliser une protection des données en continu avec des fonctionnalités de réplication toujours en service et une journalisation granulaire pour assurer la reprise la plus rapide et efficace possible. La protection des données en continu permet une reprise rapide après une attaque en évitant des pertes intenables de données. L'alternative qui consiste à payer la rançon et à espérer déchiffrer toutes vos données ne garantit pas une reprise rapide. Un fort pourcentage d'entreprises optent pour le versement de la rançon, avec des résultats contrastés : selon l'étude de 2022, un tiers de celles qui ont payé[4] n'ont pas récupéré l'accès à leurs données.

Aucun secteur n'est épargné par les pirates et les menaces de cybersécurité. Il est donc primordial que toutes les entreprises fassent le point sur les programmes de cybersécurité existants. Une évaluation des risques pour les données permettra d'identifier les lacunes, puis de prendre des mesures pour les résoudre.

Tendances et défis en matière de cybersécurité

Les prévisionnistes estiment que les cybercriminels n'accorderont aucun répit. Au contraire, ils décupleront par la même occasion les défis organisationnels liés à l'informatique. Selon Cybersecurity Ventures[5] :

— Les ransomwares coûteront 265 milliards de dollars par an à l'économie mondiale d'ici 2031.

— La cybercriminalité augmentera de 15 % d'une année sur l'autre au cours des trois prochaines années.

— Elle atteindra un chiffre de 10 500 milliards de dollars d'ici 2025.

— Environ 3,5 millions de postes devraient être vacants dans le domaine de la cybersécurité à la fin 2023.

Autres tendances :

— Seules 55 % des organisations auront mis en œuvre une stratégie de protection des données centrée sur le cloud d'ici 2025[6].

— 51 % luttent pour protéger des surfaces d'attaque complexes et en constante évolution[7].

— 50 % souffrent de la complexité et de l'incapacité à intégrer des solutions de sécurité, ce qui crée des failles dans leurs défenses[8].

Avantages d'une protection des données moderne

La mise en œuvre d'une protection des données moderne offre de nombreux avantages indéniables aux organisations de toutes tailles, en particulier face à la croissance inarrêtable des données et aux silos qui empêchent leur protection dans le cloud, au niveau du cœur, et de plus en plus à l'edge.

La modernisation de la protection des données peut contribuer à éliminer les silos du passé pour endiguer l'aggravation des risques associés à la vulnérabilité des données. Une nouvelle approche intégrée peut protéger les données contre les ransomwares en simplifiant et en automatisant les opérations de sauvegarde, de réplication et de restauration pour garantir une récupération rapide des données. Plus important encore, les copies de données chiffrées mettent vos données protégées hors d'atteinte des cyberattaques, ransomwares compris. Parmi les autres atouts de cette approche, on peut citer la conservation des données à long terme, la mobilité des données, les sauvegardes immuables et les tests réguliers de résilience des données.

Protection des données as-a-service

Dans un secteur dominé par le modèle de l'environnement cloud as-a-service basé sur l'abonnement, la protection des données moderne constitue une offre intéressante pour l'ensemble du cloud hybride.

— **Protection des données as-a-service (DPaaS) :** logiciel as-a-service basé sur le cloud ou fourni sur le Web, qui permet aux organisations de protéger leurs données et applications en sécurisant leur réseau et en proposant des options de restauration.

— **Reprise après sinistre as-a-service (DRaaS) :** déplace la puissance de calcul de l'organisation vers son infrastructure cloud en cas de sinistre.

— **Sauvegarde SaaS :** rationalise les opérations de sauvegarde à l'aide d'une politique de protection globale afin d'homogénéiser les efforts en la matière pour toutes les charges de travail, sur site comme cloud-native, sur l'ensemble du cloud hybride.

À l'aide d'une solution intelligente et économique, confiez aux experts en la matière la protection de vos ressources les plus précieuses : vos données d'entreprise.

[4] « Paying the ransom is not a good recovery strategy », Help Net Security, mai 2022

[5] « 2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics », Cybercrime Magazine, mai 2023

[6] « State of Ransomware and Disaster Preparedness for 2022 », IDC, mai 2022

[7,8] « The 2022 Study on Closing the IT Security Gap », rapport de recherche du Ponemon Institute commandité par HPE, janvier 2022

Les bons services, les bonnes technologies et les bons experts

Hewlett Packard Enterprise et Zerto offrent des solutions de protection des données de l'edge au cloud pour vous aider dans la gestion des risques. Nos experts en sécurité comprennent qu'il ne s'agit pas de savoir si vous subirez une attaque ou un piratage, mais plutôt quand vous la subirez.

HPE et Zerto proposent de nouvelles méthodes pour innover avec davantage d'agilité, maîtriser les coûts, sécuriser leurs données et faire face à des attaques sophistiquées de ransomwares et d'autres programmes malveillants. Les services de données cloud-native flexibles et solutions de protection des données nouvelle génération comportent les éléments suivants :

— Résilience aux attaques par ransomware, reprise après sinistre et services de mobilité multicloud avec Zerto
— Sauvegarde SaaS avec HPE GreenLake for Backup and Recovery

Ensemble, ces services fournissent la flexibilité nécessaire pour moderniser la protection des données. Les innovations vont de la reprise rapide à la protection contre les ransomwares, en passant par la rétention des données à long terme et l'immuabilité des données sur site et dans le cloud public, le tout grâce à des capacités opérationnelles simples. Elles permettent d'accélérer la transformation globale de HPE en société de services cloud, avec pour objectif de vous offrir davantage de choix et de liberté en matière de stratégie commerciale et informatique, grâce à une plateforme ouverte qui fournit une expérience cloud fluide, quel que soit l'endroit.

La possibilité de faire migrer les données et les charges de travail vers et depuis le cloud permet d'assurer la sauvegarde et la récupération de données pour les charges de travail sur site, cloud-native et SaaS. Vous bénéficiez ainsi d'une grande flexibilité pour optimiser vos solutions.

HPE et Zerto peuvent résoudre les problèmes de protection des données dans trois domaines clés :

1. **Protection des données complète et cohérente**

   Une protection des données Edge to Cloud moderne renforce une disponibilité continue grâce à une reprise simple et rapide en cas d'interruption, à des opérations homogènes à l'échelle mondiale et à une mobilité fluide des applications et des données entre plusieurs clouds.

2. **Sauvegarde et restauration efficaces**

   Rationaliser les opérations et limiter les risques à l'aide d'une console de gestion en vue unifiée et d'une politique de protection globale pour des fonctionnalités d'orchestration homogènes sur toutes vos machines virtuelles sur site ou vos charges de travail cloud-native, comme les volumes Amazon EBS, les clusters EKS et les instances EC2 et RDS.

3. **Protection contre les attaques par ransomware**

   HPE et Zerto aident les organisations à protéger leur activité des conséquences des ransomwares avec une solution complète et orchestrée de basculement et de rétablissement qui facilite la récupération des applications et des données infectées ou compromises. Les temps d'arrêt peuvent être limités à quelques minutes, et les pertes de données à quelques secondes seulement.

Faire équipe avec HPE et Zerto pour moderniser la protection des données

Il est temps d'éliminer les silos de données pour enfin sécuriser les données de votre entreprise contre le ransomware. Prenez les mesures pour récupérer vos systèmes après toute interruption et protéger les charges de travail de machines virtuelles sur l'ensemble des environnements sur site, du cloud hybride et multicloud. Nos experts vous aident à redéfinir et à gérer votre processus de sauvegarde et restauration sans effort, avec la simplicité et la flexibilité de l'expérience cloud, afin de garantir une protection des données moderne pour faire front face aux cybermenaces et aux attaques par ransomware. Vous bénéficierez d'une solution équilibrée associant reprise après sinistre, sauvegardes et archives autoconfigurées et autogérées pour protéger les données et applications de votre entreprise.

Toutes les entreprises doivent faire face à des menaces sur les données au quotidien, et les études ont révélé que cette tendance se poursuivra. En matière de protection des données, les entreprises ne peuvent plus se permettre de maintenir le statu quo, car le nombre d'appareils et d'emplacements, y compris dans le cloud, ne cesse de croître (à hauteur des dizaines de milliers).

Dans un environnement d'exploitation extrêmement distribué, l'approche de protection des données doit élargir son champ d'action et examiner l'emplacement de stockage et d'utilisation des données ainsi que leurs administrateurs. Des mesures plus solides et intégrées sont nécessaires pour gagner cette guerre technologique en pleine escalade. Les organisations doivent également disposer de la flexibilité nécessaire pour se moderniser et poursuivre leur parcours de transformation numérique sans être gênées par des obstacles qui les arrêteraient dans leur lancée ou freineraient l'innovation.

Qu'il s'agisse de garde-fous anti-ransomwares, de la récupération rapide de données, en passant par la conservation des données à long terme, la protection des données moderne est cruciale sur site comme dans le cloud public. Elle doit également être simple et efficace du point de vue opérationnel et garantir le respect de tous les accords de niveau de service (SLA) à un coût abordable pour que les entreprises l'adoptent sans hésiter.

Conclusion

Il n'est jamais trop tard pour élaborer une stratégie de protection des données résiliente pour protéger en continu les données de votre entreprise dispersées dans le monde entier et les restaurer rapidement en cas d'incident. La protection des données moderne pourrait être la clé de la survie de l'entreprise au 21e siècle.

Pour en savoir plus

Protégez toutes vos données. En tout temps. Zerto, une société de Hewlett Packard Enterprise

Protégez les données sans effort avec HPE GreenLake for Backup and Recovery

Visit HPE.com

Live Chat Ventes

© Copyright 2025 Hewlett Packard Enterprise Development LP. Les informations figurant dans le présent document sont sujettes à modification sans préavis. Les seules garanties relatives aux produits et services Hewlett Packard Enterprise sont stipulées dans les déclarations de garantie expresses accompagnant ces produits et services. Aucune information du présent document ne saurait être considérée comme constituant une garantie supplémentaire. Hewlett Packard Enterprise décline toute responsabilité quant aux éventuelles erreurs ou omissions techniques ou rédactionnelles qui pourraient être constatées dans le présent document.

a50009795FRE, Rev. 2

HEWLETT PACKARD ENTERPRISE

hpe.com