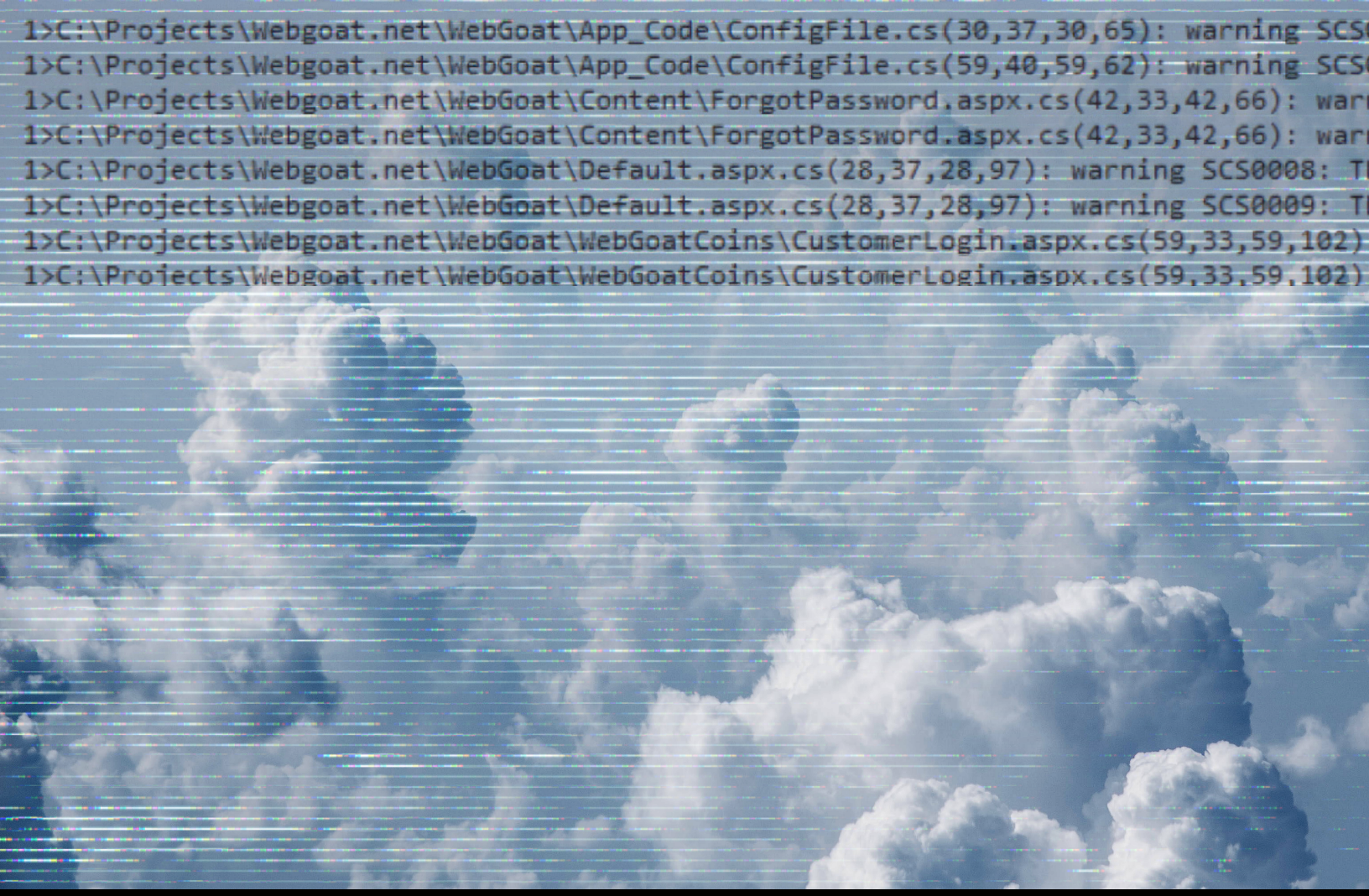


Guide

Commvault®

La solution contre les ransomwares que votre RSSI adorera

LE NOUVEAU PAYSAGE DES MENACES

Dans un contexte actuel marqué par une constante évolution des menaces, les cyberattaques se sont davantage étendues, pour un coût plus élevé que jamais. Pour les responsables de la sécurité et des technologies, l'élaboration d'une stratégie solide de cyber-résilience et de récupération n'est pas seulement essentielle, elle est urgente. Des violations **se produiront**. Disposez-vous des moyens et des ressources nécessaires pour détecter une violation et d'un plan pour y répondre ?

Vous comptez peut-être sur des solutions de sécurité des données traditionnelles qui utilisent un ensemble disparate de solutions de sécurité mal intégrées. Dans ce cas, vos équipes de sécurité seront désavantagées dès le départ lorsqu'elles tenteront d'appréhender toute l'ampleur de l'attaque.

Et tout manque de collaboration entre l'informatique et la sécurité lors d'un incident fera prendre encore plus de retard à votre organisation par rapport à un adversaire qui progresse rapidement.

Le prix d'un plan de réponse mal mis en œuvre se traduit par des temps d'arrêt coûteux, des amendes pour non-conformité, des failles de sécurité et, à terme, une atteinte à la réputation de votre organisation.

365 000 $

est le coût occasionné par heure de temps d'arrêt.[1]

LE CHAOS EXIGE UNE APPROCHE UNIFIÉE

Malheureusement, le chaos et les heures de travail qui font suite à une faille de sécurité peuvent rendre difficile le choix des stratégies et des personnes responsables de leur application. Il n'y a pas de temps à perdre en conflits internes. Les équipes de sécurité et informatique doivent travailler main dans la main, de manière stratégique et tactique. Cette collaboration est essentielle pour garantir une gestion des risques totalement efficace.

Pourtant, seules 30 % des équipes SecOps comprennent pleinement le rôle de l'équipe ITOps.

Et seulement 29 % des équipes ITOps comprennent parfaitement celui de l'équipe SecOps.[2]

La cyber-résilience peut servir de pont entre les services Informatique et Sécurité, améliorant ainsi la posture de sécurité générale de votre organisation. Les responsables de la sécurité et des technologies doivent doter leurs équipes d'outils et de stratégies adaptés pour atténuer les risques et protéger les données et la réputation. Ces outils doivent être intégrés pour offrir un contexte et une compréhension complète des attaques, des incidents ou des atteintes aux données.

Commencez dès aujourd'hui à bâtir une organisation davantage axée sur la cyber-résilience en resserrant les liens entre les équipes ITOps et SecOps. Préparez-vous à faire face à toutes les menaces, y compris les ransomwares, grâce à une solution unifiée qui fournit des alertes précoces, une préparation continue à la récupération et une cyber-récupération qui s'ajuste automatiquement. Choisissez une approche qui protège les données sur l'ensemble de votre infrastructure cloud hybride et facilite la restauration tant sur le cloud que dans les environnements sur site.

61%

des RSSI reconnaissent que leur organisation n'est pas préparée à faire face à une cyberattaque ciblée.[3]

Bien entendu, les ransomwares sont toujours le symptôme d'un problème de violation plus vaste. Il est donc peu pertinent de s'attaquer uniquement au mécanisme de diffusion des ransomwares sans traiter les problèmes sous-jacents liés à la sécurisation contre les violations et à la suppression de toute possibilité d'intrusion par l'attaquant. Le fait est que 80 % des entreprises victimes d'une attaque par ransomware en ont ensuite subi une deuxième ou une troisième. Êtes-vous prêt ?

1 Splunk, « **Digital Resilience Pays Off Report** », février 2023.
2 IDC, « **The Cyber-Resilient Organization : Maximum Preparedness with Bulletproof Recovery** », septembre 2023.
3 Proofpoint, « **2023 Voice of the CISO Report** », mai 2023.

TOUT LE MONDE EST CONCERNÉ

Même si l'objectif de toutes les personnes impliquées dans la cyber-résilience est de protéger l'entreprise contre les atteintes, les équipes informatique et SecOps peuvent s'y prendre de différentes manières, avec à la clé un risque d'exposition à des menaces extérieures. L'essentiel est de trouver un terrain d'entente. Voici quelques exemples :

1. **Objectifs partagés** : l'objectif des équipes informatiques et de sécurité est de protéger les actifs, les systèmes et les données de l'organisation. Elles s'efforcent de maintenir la confidentialité, l'intégrité et la disponibilité des informations.

2. **Collaboration** : les équipes informatiques et de sécurité collaborent souvent étroitement pour mettre en œuvre et maintenir des mesures de sécurité. Elles travaillent ensemble pour identifier les vulnérabilités, mettre en œuvre des contrôles de sécurité et répondre aux incidents.

3. **Gestion des risques** : les deux équipes sont impliquées dans l'évaluation et la gestion des risques. Les équipes informatiques se concentrent sur les risques opérationnels liés à la disponibilité et aux performances du système, tandis que les équipes de sécurité se concentrent sur l'atténuation des risques associés aux accès non autorisés, aux violations de données et à d'autres incidents de sécurité.

4. **Conformité** : les équipes informatiques et de sécurité travaillent ensemble pour garantir le respect des réglementations et normes en vigueur. Elles collaborent pour mettre en œuvre des contrôles et des processus qui répondent aux exigences de la réglementation et du secteur.

5. **Réponse aux incidents** : en cas d'incident de sécurité, les équipes informatiques et de sécurité collaborent pour enquêter sur le problème, le contenir et y remédier. Elles travaillent ensemble pour minimiser l'impact et rétablir le déroulement normal des opérations.

6. **Sensibilisation et formation** : les deux équipes jouent un rôle de sensibilisation à la sécurité et de formation des collaborateurs. Les équipes informatiques sensibilisent les utilisateurs aux pratiques informatiques sûres, tandis que les équipes de sécurité fournissent des conseils sur l'identification et le signalement des menaces de sécurité potentielles.

7. **Tests de résistance** : une équipe qui s'entraîne en groupe noue des liens et progresse davantage. Soumettre vos plans, vos politiques et votre capacité à interagir à des tests permet de mettre en évidence les domaines susceptibles d'être améliorés. Il vaut mieux tout mettre en place dans des conditions idéales, plutôt que sous la pression d'une attaque.

D'une manière générale, une collaboration et une communication efficaces entre les équipes informatique et de sécurité sont essentielles au maintien d'une infrastructure informatique sécurisée et résiliente.

DES ATTAQUES SE PRODUISENT. ASSUREZ-VOUS QUE VOS ÉQUIPES DE SÉCURITÉ ET INFORMATIQUE SONT PRÊTES.

Les cadres supérieurs responsables de la sécurité et de l'informatique ont besoin de capacités avancées de sécurisation des données pour faire face avec efficacité aux cyber-risques, réduire les menaces et améliorer les résultats du processus de récupération.

N'oubliez pas, la question n'est pas de savoir **SI** vous êtes victime d'une violation de données, mais **QUAND** vous la **DÉTECTEREZ**, **CE QUE** vous aurez entrepris pour vous y préparer, et **COMMENT** vous y répondrez.

Démarrer la conversation

Pour favoriser une meilleure collaboration et établir des bases communes, voici quelques questions à considérer :

- Dans quelle mesure votre organisation est-elle bien préparée pour répondre aux cybermenaces et assurer la continuité des activités en cas d'incident ?
- Quels sont les actifs critiques et quelle est la durée d'arrêt prévue pour l'entreprise ?
- Quelles sont les hypothèses retenues en matière de disponibilité : l'exercice a-t-il pris en compte les pannes d'Active Directory (AD), de VMware, de régions cloud ?
- Vos équipes comprennent-elles quels sont leurs rôles et responsabilités lors d'une attaque ?
- Qui dispose d'un droit d'accès et de consultation sur quoi ? Disposez-vous de mécanismes de conversation hors bande ?
- Comment sécuriser et gérer les données lors de l'adoption d'environnements cloud hybrides ?
- Quel serait le coût pour l'entreprise et sa réputation d'une violation de données suivie d'une attaque par ransomware ?

COMMVAULT CLOUD : CYBER-RÉSILIENCE POUR LE MONDE HYBRIDE

Il est également indispensable de disposer de la technologie appropriée pour servir ces objectifs communs. Commvault Cloud®, optimisé par Metallic AI, est la seule plateforme de cyber-résilience, conçue pour répondre aux exigences de l'entreprise hybride et fournir aux équipes SecOps et ITOps les capacités de sécurité et de récupération des données dont elles ont besoin face à l'évolution des menaces basées sur l'IA.

Dans un monde hybride toujours plus vaste et d'une extrême complexité, les procédures de résolution, d'atténuation et d'acceptation présentent des risques. Pouvez-vous rapidement identifier les actifs créés avec peu ou pas d'avertissement ? Savez-vous quels sont les logiciels, le matériel et les services externes susceptibles d'exposer vos données à des cybermenaces ? Tout cela oblige les RSSI à faire des choix difficiles sur la manière de hiérarchiser et d'aligner le plus efficacement possible des ressources limitées, des risques en constante augmentation et les besoins de l'entreprise.

Pour de nombreuses raisons, les organisations recherchent des solutions provenant d'un seul et même fournisseur. Les réglementations, les exigences de conformité et les politiques ont toutes poussé les organisations à vouloir en savoir plus sur la cybersécurité mise en place sur site par un fournisseur de services. Les responsables informatiques et de la sécurité demandent aux fournisseurs de leur transmettre des informations détaillées sur leurs tests d'intrusion, le cycle de vie du développement des logiciels (SDLC), leur nomenclature logicielle (SBOM) et d'autres documents leur garantissant qu'ils ne pâtiront pas d'une cybersécurité de piètre qualité.

Commvault Cloud est spécialement conçu pour protéger, surveiller, signaler, gérer et récupérer les données de n'importe quelle charge de travail à l'aide d'une **solution à guichet unique** et ce depuis n'importe quel endroit. Il élimine les surcoûts dus à l'achat d'outils complémentaires qui finissent par générer des lacunes et des vulnérabilités. Optimisé par un moteur doté d'une IA permanente, Commvault Cloud offre une plate-forme unifiée qui protège toutes vos charges de travail contre les menaces évolutives, tout en garantissant une récupération rapide et surtout propre.

83%

des organisations estiment qu'il serait souhaitable de regrouper leurs systèmes auprès d'un seul fournisseur.[4]

TCO 5 fois inférieur

Commvault offre un TCO 5 fois inférieur à celui des autres outils de protection « cloud native ».[5]

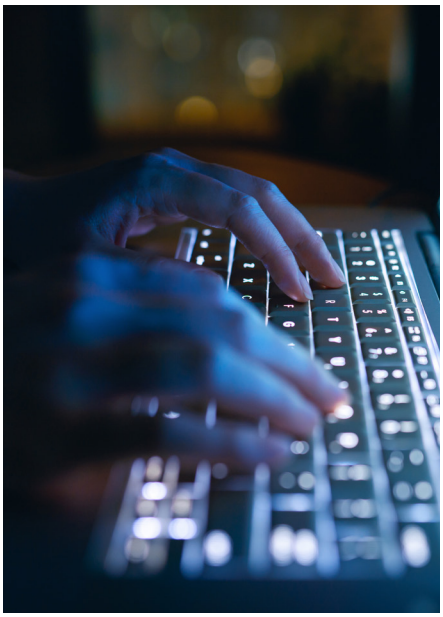
4 Forta, Digital Guardian Data Protection, « **Top Considerations for CISOs When Consolidating Information Security Solutions** », avril 2023.
5 Analyse du TCO des clients de Commvault.

Des capacités de nouvelle génération grâce à une IA avancée

En tant que cadre supérieur responsable de la sécurité des données de votre organisation, vous devez combattre le feu par le feu. Les menaces actuelles basées sur l'IA vous demandent d'être réactif, de prendre des mesures précoces de sécurité des données et de vous tenir prêt à effectuer une restauration à grande échelle.

« La rapidité de détection est clairement essentielle pour atténuer l'impact des intrusions, et la détection, en particulier, nécessite une automatisation pour être efficace. Cependant, la plupart des organisations sont encore sur la voie d'une détection et d'un reporting entièrement automatisés[2]. »
IDC : *The Cyber-resilient Organization : Maximum Preparedness with Bullet-proof Recovery*

Commvault Cloud, optimisé par Metallic AI, utilise l'intelligence artificielle, l'apprentissage automatique (ML) et l'automatisation pour fournir les informations de protection des données les plus avancées du secteur. Il prédit les menaces plus rapidement, garantit des récupérations plus nettes et accélère les temps de réponse.



Plateforme de services innovants

La plateforme Commvault Cloud permet aux équipes SecOps et informatiques de gérer les processus avec plus d'efficacité et de rentabilité.

Nous avons révolutionné la sécurité des données et la cyber-résilience en fournissant une défense à plusieurs niveaux grâce à une expérience simple et unifiée de type SaaS. Nos capacités éprouvées sont fournies par notre plateforme de services, qui vont de l'alerte précoce à la récupération rapide de toutes vos données, quelle que soit la charge de travail et où que vous soyez.

92 %

des organisations prévoient d'utiliser l'IA et l'apprentissage automatique pour renforcer leur cybersécurité.[6]

Alerte précoce	Gouvernance des risques
Détectez plus rapidement les menaces, circonscrivez le secteur touché et réduisez votre exposition aux risques.	Améliorez votre posture en matière de sécurité des données en identifiant et en corrigeant de manière proactive les risques liés aux données de production et de sauvegarde.
Préparation et réponse	**Cyber-récupération**
Assurez la résilience grâce à une préparation de qualité, une validation automatisée et des tests de récupération continus.	Garantissez une récupération rapide, avec la flexibilité nécessaire pour agir d'un point à un autre, et ce à grande échelle.

6 Synchro Works Consulting, « **The Value of Danger of AI in Cybersecurity** », août 2023.

Commvault offre un ensemble approprié de fonctionnalités de détection, de sécurité et de récupération pour réduire les risques, minimiser l'impact des attaques et assurer une continuité d'activité inébranlable face aux menaces. Protégez rapidement et facilement votre environnement de données grâce à ces fonctionnalités :

- **Isolation physique et immuabilité** : protège les données de sauvegarde dans un stockage sécurisé et isolé, doté de contrôles d'accès stricts pour empêcher toute falsification.
- **Validation de points de récupération impeccables** : l'automatisation basée sur l'IA vérifie et garantit la propreté des points de récupération, empêche la réinfection et fournit des jeux de données intacts.
- **Gestion de la posture en matière de sécurité des données** : identifiez, analysez et sécurisez les fichiers sensibles pour réduire les risques d'exfiltration sur tous vos ensembles de données de production et de sauvegarde.
- **Alerte précoce** : détectez les menaces avant le chiffrement, l'exfiltration ou la destruction des données grâce à une technologie brevetée d'alerte précoce qui décèle et détourne les menaces sophistiquées et de type Zero Day avant qu'elles n'atteignent vos données. Elle met ainsi les actifs et les environnements de sauvegarde à l'abri du regard des acteurs malveillants.
- **Résilience et récupération** : éliminez les risques liés aux logiciels malveillants, prévenez la réinfection et organisez des restaurations à grande échelle à l'aide d'une procédure de récupération fiable et rapide.
- **Informations sur la sécurité** : bénéficiez d'un contrôle intégral et gérez efficacement les risques liés aux données. Réagissez plus tôt et limitez votre exposition à l'aide d'une solution à guichet unique.
- **Architecture Zero Trust** : allez plus loin avec l'authentification multifacteur et multipersonne, la gestion des accès privilégiés (PAM) et des outils de gestion des identités et des accès (IAM) comme CyberArk, YubiKey et la biométrie (comme AAL3).

COMMVAULT CLOUD RELIE LES ÉQUIPES INFORMATIQUE ET SECOPS :

En mettant en œuvre Commvault Cloud, votre organisation peut bénéficier d'une véritable sécurité des données et d'une récupération dans le cloud hybride, ce qui vous permet de voir, de gérer et de récupérer les données où qu'elles se trouvent.

Commvault offre à ses clients un avantage en garantissant la résilience face à une cyberattaque. Pour y parvenir, des années d'innovation de pointe et plus de 1 500 brevets ont été nécessaires. L'un des avantages majeurs offerts par Commvault Cloud est une architecture unique conçue pour le monde hybride. Elle permet d'effectuer la récupération de masse la plus prévisible, la plus rapide et la plus rentable du marché.

Libérez le pouvoir d'une cyber-résilience totale

Pour en savoir plus, visitez notre site **www.commvault.fr** ou contactez votre partenaire!