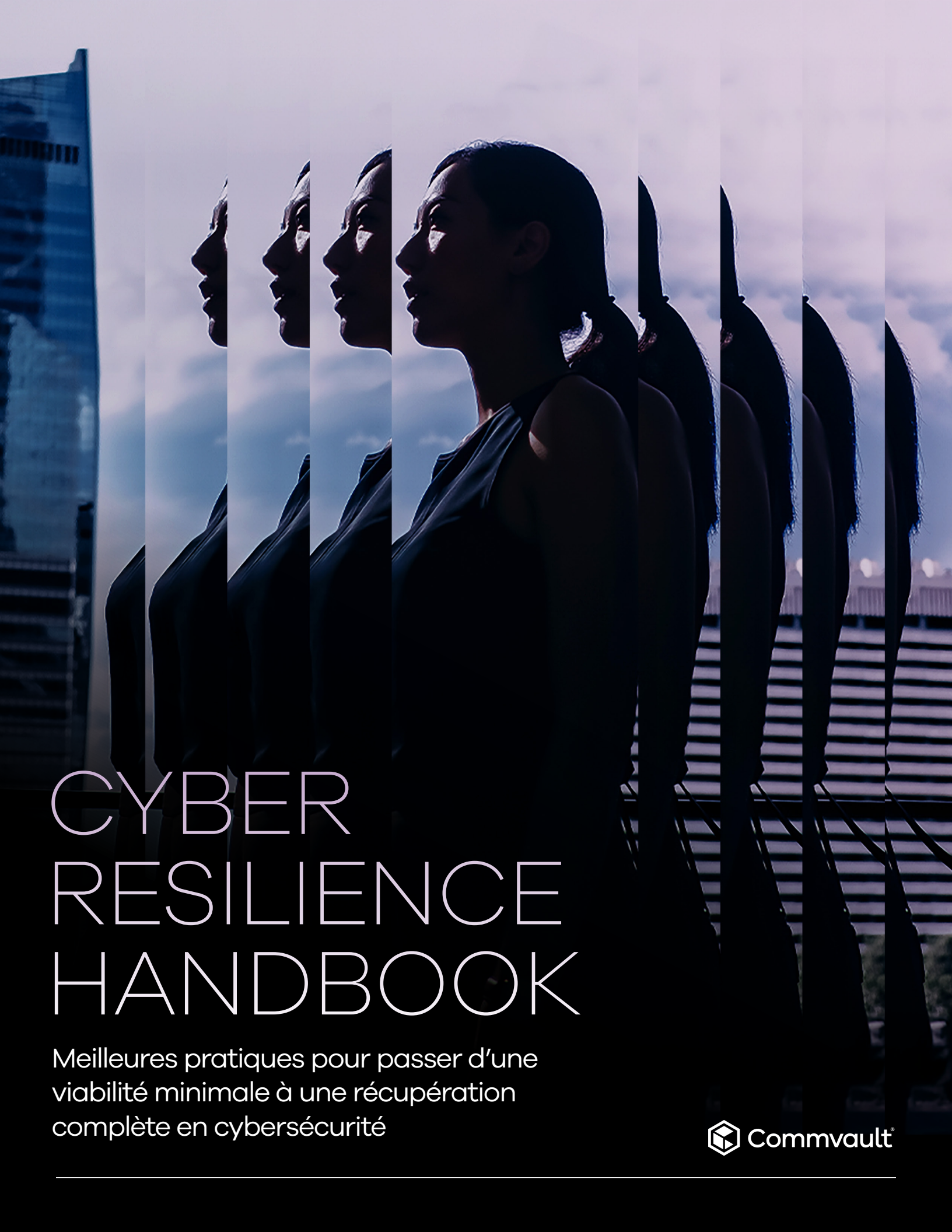

CYBER RESILIENCE HANDBOOK

Meilleures pratiques pour passer d'une viabilité minimale à une récupération complète en cybersécurité

Commvault®

INTRODUCTION

Être prêt à la récupération en cybersécurité est crucial à l'ère numérique actuelle, où les menaces cyber sont de plus en plus sophistiquées et omniprésentes.

Des stratégies de récupération en cybersécurité efficaces sont essentielles pour lutter contre ces menaces et permettre à votre entreprise de restaurer rapidement les systèmes et les données critiques après un incident cyber – minimisant les temps d'arrêt et atténuant l'impact sur les opérations commerciales. En étant prêt en matière de cybersécurité, les entreprises démontrent aux clients, aux parties prenantes et aux organismes de réglementation qu'elles prennent au sérieux la protection des données sensibles et des systèmes qui permettent de tenir leurs engagements envers les clients.

La première étape pour élaborer un plan de préparation à la cybersécurité consiste à identifier les personnes, processus, systèmes et données critiques nécessaires à l'opération – c'est votre viabilité minimale. Pour la plupart des entreprises, cela inclut la direction exécutive et opérationnelle, une compréhension des rôles et responsabilités lors d'une récupération, ainsi que la capacité technique de restaurer les systèmes critiques, tels que l'identité d'entreprise (par exemple, Active Directory), les canaux de communication, et de préparer et valider que les données, applications et infrastructures sont propres et prêtes à être récupérées et restaurées à partir de sauvegardes.

Au-delà des obligations de conformité (comme le RGPD, HIPAA, DORA ou SOCI) qui exigent des plans détaillés de cybersécurité, de résilience, de récupération en cas de catastrophe et de continuité des activités, un plan de récupération en cybersécurité bien structuré réduit le risque de perte de données, garantissant que les informations critiques telles que les détails des clients, les données propriétaires et la propriété intellectuelle restent protégées. En cas de compromission des données, disposer d'un mécanisme de récupération rapide aide à restaurer rapidement les opérations minimales viables et à remettre les systèmes en ligne rapidement.

LE RAPPORT COMMVAULT + GIGAOM SOULIGNE L'IMPORTANCE CRITIQUE DES STRATÉGIES DE CYBERRÉCUPÉRATION COMPLÈTES.

Découvrez les composants essentiels nécessaires pour être prêt à faire face à une cyberattaque—et voyez comment Commvault® Cloud fournit les outils pour vous aider à réussir.

ÉTAPE #01

IDENTIFIER

Un principe clé de toute stratégie est une visibilité approfondie sur l'environnement et une compréhension des applications, systèmes et données nécessaires pour assurer une viabilité minimale en cas de pannes et de cyberattaques.

Avec Commvault Cloud, cela inclut la capacité de découvrir, classifier et surveiller les données sensibles à travers tous vos dépôts de données. La classification des données peut ensuite déclencher des politiques de protection et aider les organisations à identifier ce qui est le plus critique et ce qui nécessite un niveau de protection différent.

Une fois que vous connaissez les éléments qui doivent être protégés, vous pouvez instrumenter l'environnement avec des mécanismes de détection des menaces, de détection des anomalies et d'alerte précoce pour alerter les équipes de sécurité des menaces dans vos réseaux avant qu'elles ne causent des dommages.

Vous avez également besoin d'une approche en couches pour trouver et arrêter les logiciels malveillants, les ransomwares et autres vecteurs de corruption des données. Les données doivent être inspectées à tous les points de leur cycle de vie pour trouver les données corrompues afin de les restaurer à un point dans le temps propre.

PRODUITS COMMVAULT CLOUD POUR AIDER À IDENTIFIER LES MENACES :

- Analyse des risques pour la découverte et le contrôle des données sensibles
- Threatwise™ pour la détection des menaces et des anomalies et les alertes précoces
- Threat Scan pour identifier les données malveillantes ou corrompues

CAPACITÉS DE LA PLATEFORME COMMVAULT CLOUD :

- Cleanpoint Validation

ÉTAPE #02

PROTÉGER

Pour être prêt à faire face à une attaque inévitable, vous devez protéger vos données contre les actions des attaquants, des initiés malveillants, et même des mauvaises configurations ou des pannes.

Cette protection est multiforme et doit prendre en compte les données elles-mêmes, l'identité et les configurations. En commençant par les données, les meilleures pratiques recommandent que les organisations suivent la règle 3-2-1 : trois copies des données, sur deux types de supports (ou sur deux plateformes différentes), et une copie qui est impossible à modifier. Dupliquer les données pour les deux premières étapes est simple, mais la troisième est un peu plus complexe. Vous avez besoin d'un mécanisme pour rendre les données immuables et indélébiles afin de les protéger contre les modifications ou suppressions unilatérales. Cela est particulièrement important pour deux raisons : la majorité des ransomwares ont des mécanismes pour altérer les sauvegardes, et les menaces internes sont réelles.

Vous devez valider que votre infrastructure (cloud et sauvegarde) est configurée selon les principes de la confiance zéro. Il doit y avoir des mécanismes en place qui vérifient les configurations et signalent et alertent sur les changements ou les "dérives".

L'authentification doit également suivre les principes de la confiance zéro et inclure l'authentification multi-facteurs et multi-personnes, en fonction des niveaux d'accès et des actions effectuées. En plus de cela, tout mécanisme que vous avez en place pour valider l'identité, comme Active Directory ou Entra ID, doit également être configuré, sauvegardé et surveillé pour les changements tels que les ajouts, suppressions ou élévations de privilèges.

Toute donnée, configuration ou plan de contrôle doit être sauvegardée pour permettre la restauration en cas d'incident de sécurité, et les sauvegardes doivent être isolées et airgapped pour réduire la probabilité que les attaquants trouvent les sauvegardes lors de la reconnaissance ou qu'elles soient supprimées ou chiffrées par des logiciels malveillants ou des ransomwares.

PRODUITS COMMVAULT CLOUD QUI VOUS AIDENT À PROTÉGER VOS DONNÉES :

- Sauvegarde et restauration des charges de travail cloud, on-prem et SaaS
- Sauvegarde et restauration Active Directory pour protéger Active Directory et Entra ID
- Air Gap Protect pour un stockage immuable, indélébile et déconnecté
- Analyse des menaces pour identifier et mettre en quarantaine les données malveillantes ou corrompues

CAPACITÉS DE LA PLATEFORME CLOUD COMMVAULT :

- Security IQ pour la gestion de la posture de sécurité de votre environnement de sauvegarde
- Contrôle d'accès basé sur les rôles (RBAC) et autorisation multipersonnes

ÉTAPE #03

RÉPONDRE

Aucune technologie ne vous servira bien en silo. C'est pourquoi Commvault Cloud s'intègre avec les logiciels de gestion des informations et des événements de sécurité (SIEM) et les plateformes d'orchestration, d'automatisation et de remédiation de la sécurité (SOAR).

Cela permet le partage de contexte entre Commvault Cloud et d'autres outils de sécurité pour mieux détecter les événements de sécurité, les problèmes d'intégrité des données et les activités anormales.

Que vous utilisiez la plateforme Palo Alto Networks XSOAR, Splunk SIEM, Microsoft Sentinel ou un autre outil, la détection des menaces et des anomalies de Commvault Cloud est un multiplicateur de force pour renforcer la résilience cybernétique et améliorer la réponse aux incidents.

Lorsque Commvault Cloud trouve des fichiers suspects ou reçoit une alerte d'anomalie d'une intégration, ce fichier peut être automatiquement mis en quarantaine de vos données de production et une copie envoyée à un Sandbox pour détonation et analyse afin de déterminer s'il est malveillant.

FONCTIONNALITÉS DE LA PLATEFORME COMMVAULT CLOUD QUI VOUS AIDENT À RÉPONDRE PLUS RAPIDEMENT AUX MENACES :

- Intégrations avec l'écosystème de sécurité y compris les technologies SIEM et SOAR
- Intégrations de renseignements sur les menaces pour une couverture plus large des menaces
- Intégrations avec des bacs à sable pour permettre l'inspection et la détonation des fichiers suspects

ÉTAPE #04

RÉCUPÉRER

Lorsqu'il s'agit de récupérer des données, que ce soit après une catastrophe ou une cyberattaque, vous avez besoin d'un plan qui a été pratiqué et documenté ; des données propres et complètes ; une flexibilité des cibles de restauration ; la capacité de restaurer tout, des données à l'application qui les utilise ; et de la rapidité.

Le pire moment pour réaliser que votre plan de récupération ne fonctionnera pas est lorsque vous êtes confronté à une attaque. Effectuer des tests réguliers des plans de viabilité minimale et de récupération complète est crucial pour savoir que vous pouvez récupérer lorsque c'est nécessaire, et aide les équipes chargées de la récupération à connaître ce qui leur est demandé. Ces tests ou pratiques du processus de récupération doivent vérifier l'intégrité des données et être capables de restaurer les données et de reconstruire les applications dans un nouvel environnement.

La portabilité est importante pour les tests et la récupération, car une attaque ou une panne peut nécessiter le déplacement de charges de travail entières vers un nouvel environnement différent. Cela pourrait signifier simplement changer de compte ou être aussi drastique que passer d'un environnement sur site au cloud, ou à un cloud entièrement différent—votre récupération doit donc être hybride et flexible.

Nous avons déjà discuté de la nécessité de scanner et de surveiller les données pour détecter des anomalies, des logiciels malveillants et autres défauts. Lorsqu'il s'agit de restaurer, il est important de faire une dernière vérification des données pour s'assurer qu'elles sont propres, prêtes à être restaurées et qu'elles ne vont pas simplement réinfecter votre environnement.

Enfin, après une récupération, vous devrez conserver une copie des données et des systèmes affectés par l'attaque pour la fournir à des équipes d'enquête et de réponse aux incidents tierces, aux forces de l'ordre, aux assureurs cybernétiques ou à d'autres parties intéressées. Cette copie forensique doit être conservée séparément de votre environnement de production et préservée telle quelle pour vos enquêtes. Cela peut aider à rétroingénierer les logiciels malveillants, identifier l'attaquant et identifier les techniques et procédures à préparer pour l'avenir.

PRODUITS CLOUD COMMVAULT QUI VOUS AIDENT À RÉCUPÉRER :

- Cleanroom Recovery pour les tests de récupération, la validation et la forensique
- Threat Scan pour valider que les fichiers récupérés sont propres et exempts de logiciels malveillants, de ransomwares et de corruption
- Cloud Rewind pour reconstruire des applications à travers différents clouds, du code aux données
- Récupération Active Directory pour la continuité des identités, même en cas de cyberattaque

CAPACITÉS DE LA PLATEFORME CLOUD COMMVAULT :

- Récupération Cloudburst pour une restauration rapide et à l'échelle du cloud, disponible quand vous en avez besoin
- Validation de Point Propre pour fournir un point connu dans le temps pour la restauration

ÉTAPE #05

SURVEILLER

Toute votre planification et préparation ne fonctionnent que si vous avez instrumenté votre environnement pour alerter les équipes de sécurité et informatiques des anomalies ou des événements sur votre infrastructure.

La surveillance des menaces qui ont infiltré votre organisation et tentent d'échapper à la détection est cruciale pour minimiser les dommages qu'elles peuvent causer. Plus tôt vous en êtes conscient, plus vite vous pouvez les expulser et restaurer les données affectées.

Le défi de la surveillance est que de nombreux outils de cybersécurité déclenchent des centaines ou des milliers d'alertes, créant beaucoup de bruit à cause des faux positifs. Cela conduit les équipes de sécurité à enquêter sur des pistes sans issue, provoquant l'épuisement et la fatigue des alertes, et détournant du temps des enquêtes sur les véritables menaces. Régler les systèmes pour qu'ils n'alertent que sur les véritables attaques est crucial pour aider les équipes à se concentrer et à trouver les véritables menaces.

Les données de production et de sauvegarde doivent être surveillées en continu pour détecter les changements, les anomalies et les logiciels malveillants afin de trouver les menaces plus rapidement, de minimiser le risque d'infection supplémentaire et de restaurer les données connues comme propres. Cela inclut la capacité d'examiner les comportements des fichiers, et pas seulement leur contenu, afin de détecter des attaques jamais vues auparavant.

Vous pouvez également bénéficier de la consolidation de toute la surveillance sur une seule plateforme – dans la plupart des cas, un outil SIEM ou SOAR qui est surveillé en continu par le personnel des opérations de sécurité et utilisé pour coordonner les enquêtes et les réponses.

PRODUITS CLOUD COMMVAULT QUI PERMETTENT UNE SURVEILLANCE CONTINUE :

- Threatwise™ pour la détection des attaquants effectuant des reconnaissances et des pièges qui fournissent des alertes de haute fidélité en cas de violation
- Threat Scan pour l'analyse continue des données de sauvegarde et des fichiers à la recherche de logiciels malveillants
- Threat Scan Predict pour découvrir les attaques de type zero-day ou polymorphes pilotées par l'IA

CAPACITÉS DE LA PLATEFORME CLOUD COMMVAULT :

- Intégrations de l'écosystème de sécurité pour ajouter des niveaux encore plus élevés de renseignement sur les menaces provenant de fournisseurs tiers

RÉSUMÉ

En résumé, vous devez être conscient des risques que vos données présentent pour votre organisation.

01

Identifiez ce dont vous avez besoin pour une viabilité minimale – les systèmes, applications et données critiques pour le fonctionnement de votre entreprise.

02

Investissez dans des outils avancés de protection, de détection et de surveillance pour améliorer la capacité de votre organisation à détecter et à répondre rapidement aux cybermenaces.

03

Développez et maintenez un plan de réponse aux incidents à jour, en définissant clairement les rôles, les responsabilités et les procédures à suivre en cas de violation.

04

Effectuez des tests complets pour valider que vous avez couvert plusieurs scénarios et que vous pouvez vous rétablir complètement.

05

Surveillez vos systèmes et vos sauvegardes pour être sûr qu'ils sont propres et prêts à être utilisés en cas de besoin.

Pour voir comment Commvault Cloud peut vous aider avec la partie technologique du puzzle de la préparation aux cybermenaces, **demandez une démonstration** et une consultation avec nos experts en préparation et en récupération.