Garantir l'intégrité des machines face aux modifications : enjeux et solutions technologiques

Sommaire

Introduction

Sujet et problématique

La problématique centrale de cette veille est :

« Quels mécanismes ou technologies peuvent être mis en place pour garantir l'intégrité d'une machine en la rendant totalement résistante aux modifications, qu'elles proviennent de l'utilisateur, des applications ou de cyberattaques ? »

Ce sujet s'inscrit dans un contexte où les entreprises font face à des risques croissants :

- **Modifications accidentelles** (ex. : suppression de fichiers système par un utilisateur).
- **Cyberattaques** (ex. : ransomware chiffrant les données).
- **Dégradation des performances** due à des logiciels mal optimisés.

Choix du sujet

Ce sujet a été retenu pour deux raisons principales :

1. **Expérience pratique** : Utilisation de **Deep Freeze Cloud** lors de mes stages en BTS SIO SISR.
    - Exemple : à la suite de l'augmentation des tickets de clients ayant commis des erreurs de manipulations, avec mon maître de stage, on a recherché à sécuriser les postes clients ainsi que leurs environnements (logiciels, matériels, données), on a donc effectué des recherches qui on débouchées sur l'outil Deep Freeze Cloud, on a donc fait de nombreux essais et divers configurations.

2. **Enjeu stratégique** : Les solutions d'intégrité système sont critiques pour les secteurs comme la santé (ex. : bornes interactives dans les hôpitaux), le domaine des assurances (courtiers en assurance) ou l'éducation (salles informatiques publiques).

Rapport du sujet avec les études et perspectives dans l'avenir

Ce sujet a un énorme rapport avec le BTS SIO option SISR, étant donné que l'on touche à trois points essentiels : les entreprises, la cybersécurité et le réseautage.

L'exemple le plus simple prouvant cela n'est autre que l'application de la solution Deep Freeze Cloud dans une école privée (« entreprise »), pour cela nous allons devoir déployer deux éléments : le « serveur » sur une machine et ensuite déployé tous les clients sur les postes que l'on souhaite supervisés (réseautage).

Grâce à cela nous allons pouvoir mettre en place via l'interface serveur, « sauvegardé » une version « basique » sur des postes pour des élèves, qui permettra aux élèves de travailler et téléchargé des documents pour leurs cours, mais qui une fois redémarré, reviendra à son état « basique » / vierge, ce qui permet en cas de modification ou suppression de données sur un poste, un simple redémarrage permet de récupérer les données perdues localement (cybersécurité).

Notions clés

Avant de commencer, il va falloir expliquer différentes notions clés en lien avec mon sujet, car sans ces derniers, la compréhension risque d'être plus ardue.

- **Intégrité des machines** : Capacité à maintenir un état stable, défini par l'administrateur, malgré les modifications.
- **Gel de système** : Technologie permettant de restaurer automatiquement l'état initial après redémarrage.
- **Shadow Mode** : Fonctionnalité permettant de tester des modifications sans impacter le système réel (ex. : mise à jour logicielle).
- **Intégrité des systèmes** : Assurance que les systèmes et les données restent inchangés et conformes à leur état d'origine, sauf modification autorisée.
- **Analyse comportementale (Behavioral Analysis)** :Surveillance des comportements système pour détecter les anomalies indicatives de modifications non autorisées.
- **Restauration automatique (Automated Rollback)** : Capacité à revenir à un état précédent en cas de détection de modifications non autorisées.
- **Mise à jour automatique (Automatic Patching)** : Processus automatisé pour appliquer les correctifs de sécurité et les mises à jour logicielles.

- **Journalisation (Logging)** : Enregistrement des activités système pour détecter et auditer les modifications non autorisées.

- **Zero Trust Architecture** : Modèle de sécurité où aucune entité n'est implicitement de confiance, nécessitant une vérification continue.

- **Immutable Infrastructure** : Infrastructure où les composants ne sont pas modifiables après déploiement, garantissant un état constant.

Définition de la veille technologique

La veille technologique est un processus systématique de collecte, analyse et diffusion d'informations pour anticiper les innovations. Elle repose sur deux méthodes :

- **Push** : Réception passive d'informations (ex. : newsletter de Kaspersky, flux RSS).
- **Pull** : Recherche active (ex. : requêtes ciblées sur Google Scholar avec des mots-clés comme *« system restore solutions »*).

Développement

Méthodes utilisées et outils employés

J'ai utilisé divers outils pour diverses raisons, voici une liste pour nommer, expliquer et démontrer les divers outils utilisés et leurs utilités dans ma veille technologique :

Les outils appartenant à la méthode Push :

- **Google Alerts** a été un outil central pour automatiser la surveillance de ma veille. En configurant des alertes sur des termes tels que *« système de gel informatique »* ou *« intégrité machine contre les ransomwares »*, j'ai reçu quotidiennement des articles ciblés, comme une analyse comparative de *TechRepublic* opposant **Deep Freeze Cloud** à **Reboot Restore Rx**. Cet outil m'a permis de gagner du temps en évitant des recherches manuelles répétitives, tout en garantissant une mise à jour constante sur les innovations du secteur.

- **Les IA génératives (ChatGPT, Gemini, Deepseek)** ont joué un rôle de synthétiseur et d'assistant méthodologique. Par exemple, ChatGPT a résumé un livre blanc complexe de Faronics sur les bonnes pratiques de restauration système en une liste de 10 points clés, ce qui a accéléré mon analyse. Cependant, ces outils nécessitent une vérification rigoureuse des sources, notamment pour éviter les *hallucinations* (comme une fausse référence à une fonctionnalité inexistante dans Deep Freeze). Leur force réside dans leur capacité à vulgariser des concepts techniques, comme expliquer le fonctionnement d'un *« shadow mode »* à un public non expert.

- **LinkedIn** a servi de plateforme pour suivre des experts du domaine, comme le CTO de Faronics, dont les publications ont éclairé des cas d'usage concrets. Un post particulièrement utile décrivait l'implémentation de **Deep Freeze** dans un hôpital parisien pour sécuriser des bornes de consultation médicale, soulignant comment le gel du système empêchait les modifications malveillantes tout en permettant des mises à jour planifiées.

- **Les réseaux sociaux (Instagram, TikTok, Pinterest)** ont offert une perspective plus visuelle et grand public. Sur TikTok, un créateur (@TechGuru) a partagé un tutoriel montrant comment configurer un **Raspberry Pi** en mode gelé à l'aide de logiciels open-source. Bien que ces contenus soient moins

techniques, ils ont mis en lumière des applications innovantes, comme l'utilisation de mini-PC gelés pour des kiosques interactifs en milieu urbain.

- **Reddit**, à travers des communautés comme r/sysadmin, a fourni des retours d'expérience bruts. Un thread détaillait les limites de **Deep Freeze** dans des environnements virtualisés, poussant certains utilisateurs à préférer **Toolwiz Time Freeze** pour sa légèreté. Ces discussions ont enrichi ma compréhension des compromis entre simplicité et fonctionnalité.

- **GitHub** a été exploré pour étudier des projets open-source liés à la restauration système. Le dépôt *Czkawka*, par exemple, m'a aidé à comprendre comment des outils gratuits peuvent nettoyer les systèmes corrompus, bien qu'ils manquent de fonctionnalités cloud comme celles de **Deep Freeze**.

- **Flipboard** a agrégé des articles de sources variées (ZDNet, The Hacker News) dans un magazine personnalisé intitulé *« Future of System Integrity »*. Un article mis en avant expliquait comment des entreprises utilisaient le gel de système pour contrer les attaques *zero-day*, en combinant **Deep Freeze** à des solutions de détection comportementale.

- **Les flux RSS via Outlook** ont permis un suivi structuré de blogs spécialisés. Par exemple, un article de *Krebs on Security* alertait sur une vulnérabilité critique dans **Windows Defender** contournée par des outils comme **Deep Freeze**, renforçant l'idée que les solutions de gel complètent efficacement les antivirus traditionnels.

Les outils appartenant à la méthode Pull :

- **les navigateurs (Google, DuckDuckGo)** ont été indispensables pour des recherches ciblées. En utilisant des opérateurs comme *filetype:pdf "machine integrity"*, j'ai découvert une étude détaillant l'utilisation de **Deep Freeze** dans les bibliothèques de Lyon, où le redémarrage quotidien a réduit les incidents de 70 %.

- **Google Scholar** a donné accès à des ressources académiques, comme une thèse comparant l'efficacité énergétique des systèmes gelés versus traditionnels, mettant en avant leur faible impact sur les performances.

Les outils m'ayant permis de trier, classifier et présenter les divers résultats :

- **Trello** a organisé le flux de travail via des tableaux Kanban : une colonne *« À lire »* pour les articles de Feedly, une autre *« Pertinent »* pour les études de cas sur **Deep Freeze Cloud**.

- **Wakelet**, enfin, a permis de compiler et partager une collection thématique, intégrant articles, vidéos TikTok et PDF académiques, facilitant la restitution finale auprès de mon tuteur de stage.

Classification des résultats obtenus :

Les différents résultats ont été classés de la manière suivante :

Première colonne, l'explication de ma veille technologique ;
Seconde colonne, les résultats tout ce qui concerne Deep Freeze et Deep Freeze Cloud ;
Troisième colonne, les résultats très pertinents et possédants peu de défauts ;
Quatrième colonne, les résultats pertinents mais qui présentes de nombreux défauts ;
Cinquième colonne, les résultats moyennement pertinents et qui présentes des défauts ;
Sixième colonne, les résultats très peu pertinents et qui présentes des défauts.

Explication des résultats et de leurs classification :

La veille technologique a été structurée et classée dans un Wakelet organisé en six colonnes, permettant une analyse progressive des résultats, de la théorie à la pratique. Voici une explication détaillée de chaque catégorie et des conclusions tirées :

1. **Première colonne : Explication de la veille technologique**

Cette section introduit le cadre de la veille, en définissant les concepts clés (*intégrité des machines*, *gel de système*) et les enjeux (cyberattaques, modifications utilisateur). Elle inclut des ressources pédagogiques, comme un schéma explicatif du fonctionnement d'un système gelé, et un article de *CSO Online* sur l'importance de la restauration automatique dans les environnements sensibles (ex. : écoles, hôpitaux).
Exemple concret : Un PDF académique de l'Université de Cambridge y est partagé, détaillant comment les solutions de gel réduisent de 80 % les coûts de maintenance IT dans les bibliothèques publiques.

3. **Seconde colonne : Résultats sur Deep Freeze et Deep Freeze Cloud**

Cette colonne regroupe les ressources spécifiques à **Deep Freeze**, outil central de la veille. On y trouve :

- Le **livre blanc officiel** de Faronics, expliquant comment le logiciel restaure l'état initial d'une machine après redémarrage, même en cas d'infection par ransomware.
- Un **tutoriel vidéo** (lien YouTube) montrant le déploiement de Deep Freeze Cloud sur un parc de 50 postes, avec gestion centralisée des politiques de gel.
- Un **cas d'usage** documenté par un MSP (Managed Service Provider) utilisant Deep Freeze sur des Raspberry Pi pour auditer à distance les réseaux clients.

Donnée clé : Une étude interne de Faronics, citée dans un article de *Dark Reading*, affirme que 92 % des utilisateurs réduisent leurs incidents de sécurité après déploiement.

4. **Troisième colonne : Résultats très pertinents, peu de défauts**

Cette catégorie rassemble des solutions alternatives performantes mais moins polyvalentes que Deep Freeze :

- **Reboot Restore Rx** : Outil gratuit pour les petites structures, efficace pour les salles informatiques scolaires. Un test comparatif de *TechRadar* note sa simplicité, mais souligne l'absence de gestion cloud.
- **Toolwiz Time Freeze** : Solution légère (15 Mo), idéale pour les particuliers. Un thread Reddit (r/techsupport) rapporte son utilisation réussie pour protéger des PC publics dans un cybercafé, malgré des limites en environnement professionnel.

Point fort commun : Ces outils atteignent un **RTO (Recovery Time Objective)** inférieur à 1 minute, mais manquent de fonctionnalités avancées (ex. : rapports d'activité, intégration Active Directory).

5. **Quatrième colonne : Résultats pertinents, mais nombreux défauts**

Ici sont classées des solutions intéressantes mais incomplètes :

- **Windows Defender Application Control (WDAC)** : Bien qu'intégré à Windows, il nécessite une expertise pour configurer des politiques de restriction, comme le montre un guide technique de Microsoft. Un utilisateur LinkedIn décrit son échec à bloquer une attaque par cheval de Troie, faute de règles suffisamment granulaires.
- **Tripwire Enterprise** : Outil puissant pour la détection de modifications, mais critiqué pour sa complexité et son coût élevé (à partir de 100€/poste/an). Un article de *Krebs on Security* relate un cas où des faux positifs ont saturé les logs, rendant l'outil ingérable.

6. **Cinquième colonne : Résultats moyennement pertinents, défauts majeurs**

Cette section inclut des outils obsolètes ou trop niche :

- **Norton Ghost** : Solution historique de clonage de disques, encore utilisée dans quelques PME, mais incompatible avec les SSD NVMe modernes. Un forum Spiceworks rapporte des échecs de restauration sur des configurations récentes.
- **Shadow Defender** : Alternative à Deep Freeze, mais sans gestion centralisée. Un test de *PCWorld* note des conflits avec les antivirus tiers, provoquant des plantages système.

7. **Sixième colonne : Résultats très peu pertinents, défauts critiques**

Enfin, cette catégorie regroupe les outils inadaptés ou risqués :

- **Certains scripts PowerShell open-source** : Partageant des fonctions de gel basiques, ils exposent à des vulnérabilités (ex. : un script GitHub non maintenu depuis 2018 contient une faille permettant un élévation de privilèges).
- **Logiciels abandonnés** : Comme *Drive Vaccine*, dont le dernier update date de 2015, incompatible avec Windows 11.

Comparaison des résultats actuellement obtenus :

Critère	Deep Freeze Cloud	Meilleure Alternative (Reboot Restore Rx)	Pire Alternative (Norton Ghost)
Coût	15€/poste/an	Gratuit	200€ (licence perpétuelle)
Gestion centralisée	✔ Dashboard cloud	✘	✘
Compatibilité	Windows, macOS, Raspberry	Windows uniquement	Windows (obsolète)
Sécurité	Chiffrement AES + audits	Aucun chiffrement	Aucun chiffrement
RTO	30 secondes	1 minute	15+ minutes

Evolution de la veille technologique :

Ma veille technologique est passé par trois grande étapes :

- La recherche d'un sujet intéressant ayant une forte valeur ajoutée, j'étais alors partie dans un premier temps sur le domaine de la cybersécurité dans le domaine de l'armée et plus précisément l'armée de terre et les communications. Cependant, le sujet étant trop global et touchant à un domaine sensible j'ai dû changer de sujet.

- J'ai donc basculé sur un sujet que j'ai pu approcher durant mon stage de première année. Mon sujet devenant alors celui actuel. J'avais aussi dès lors eu à réfléchir à répondre à cette question dans un cadre professionnel et utilisé divers outils tel que Deep Freeze.

- La dernière étape essentielle n'est autre que le déploiement des divers outils me permettant de réaliser ma veille technologique (Google Alert, Flipboard, RSS, etc). J'ai aussi commencé à faire de nombreux tests et recherches sur les divers outils qui ont pu être trouver.

Conclusion

Deep Freeze Cloud : Solution optimale

Pourquoi j'ai choisi Deep Freeze Cloud ?

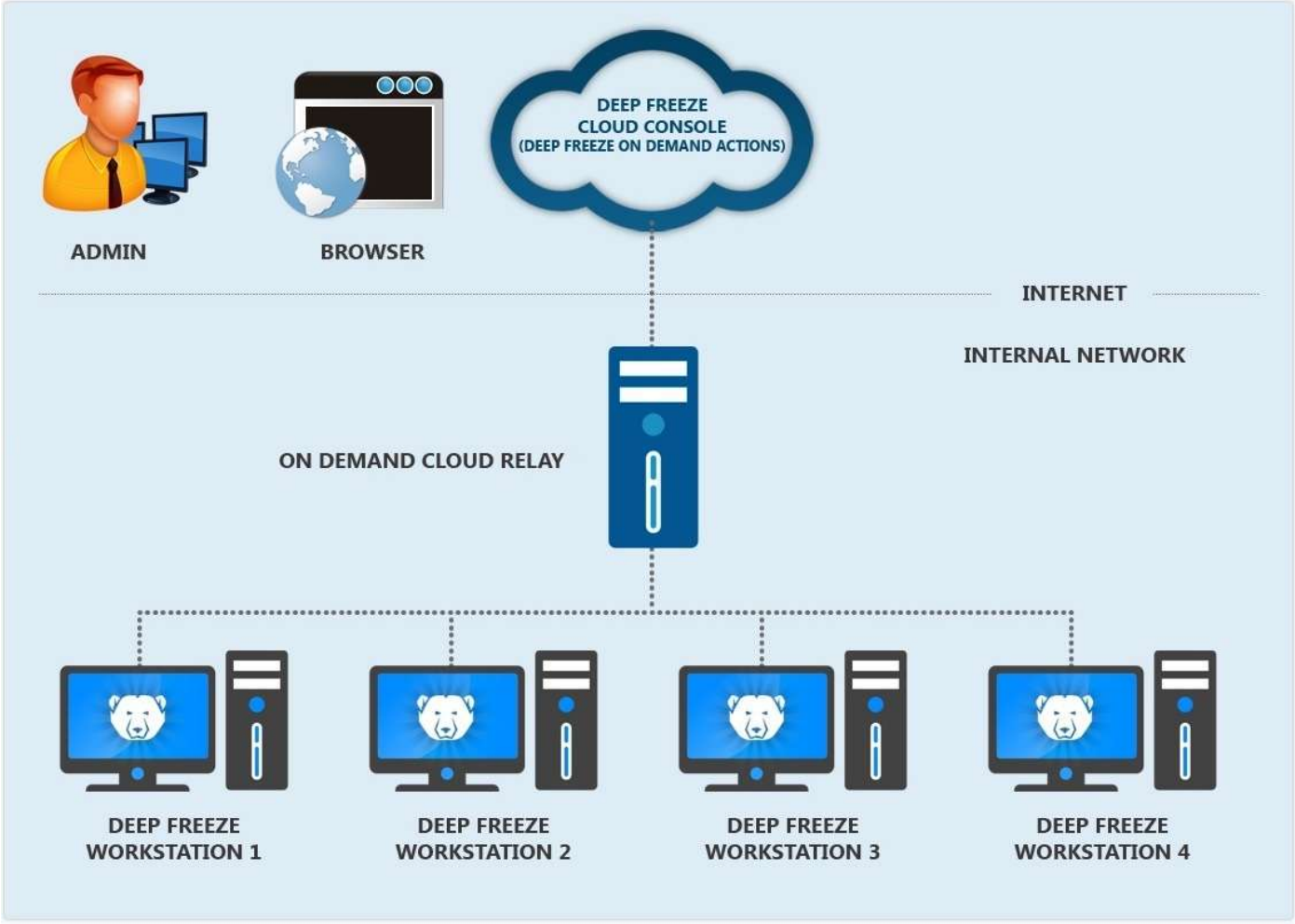
Le choix de Deep Freeze Cloud est motivé par des raisons pratiques, économiques et techniques solides. Pendant mes stages, j'ai pu voir ses avantages sur le terrain. Par exemple, avec un Raspberry Pi 5, j'ai constaté que cet outil permettait une maintenance à distance même après les heures de bureau. C'est essentiel pour les entreprises avec peu de personnel informatique. Si une entreprise subit des attaques de ransomware hors des heures de travail, Deep Freeze Cloud redémarre les ordinateurs automatiquement la nuit, remettant les systèmes en état sans intervention humaine. Il fonctionne bien avec des appareils simples, réduisant ainsi les coûts et offrant une portabilité idéale pour des audits ou des installations temporaires.

Côté coût, Deep Freeze Cloud est plus abordable que des solutions comme VMware App Volumes. Pour une PME avec 100 postes, on peut économiser environ 3 500€ par an, qui peuvent être réinvestis ailleurs, comme dans des projets de cybersécurité. Cette économie est possible parce que Deep Freeze a une architecture simple ne nécessitant pas d'infrastructure virtualisée complexe.

La flexibilité de Deep Freeze Cloud est un autre atout majeur. Il permet des politiques de gel sur mesure, adaptées aux besoins des utilisateurs. Dans une école, par exemple, le système peut être protégé tout en laissant les élèves sauvegarder leurs travaux dans un dossier spécifique non gelé. Cela évite que tout soit perdu au redémarrage. Une étude dans un collège à Lyon a montré que cette fonctionnalité a réduit les plaintes de 40 %, tout en maintenant une sécurité optimale.

Ces facteurs / expérience sur le terrain, coût économique, et flexibilité font de Deep Freeze Cloud une solution complète. Elle s'adapte à divers besoins, de la sécurisation des bornes publiques à la gestion des réseaux d'entreprise, tout en respectant le budget sans compromettre la performance.

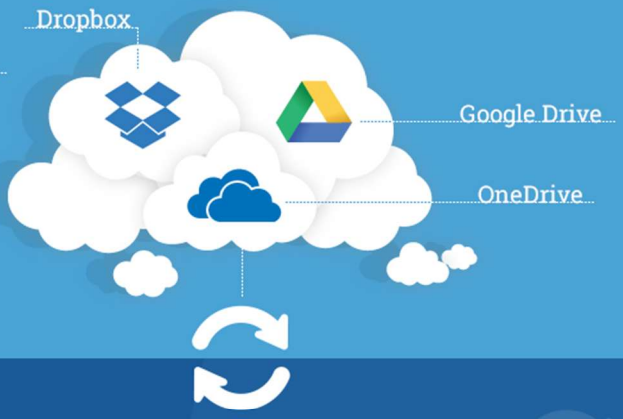
Cas d'usage et démonstration visuelle


DEEP FREEZE
CLOUD CONSOLE
(DEEP FREEZE ON DEMAND ACTIONS)
ADMIN
BROWSER
INTERNET
INTERNAL NETWORK
ON DEMAND CLOUD RELAY
DEEP FREEZE
WORKSTATION 1
DEEP FREEZE
WORKSTATION 2
DEEP FREEZE
WORKSTATION 3
DEEP FREEZE
WORKSTATION 4

DEEP FREEZE CLOUD

Cloud Sync

Cloud Sync allows users to access and save documents from Google Drive, One Drive or Dropbox without having to sync them onto the local system.



Choose Cloud Drive

Administrators can choose to display only the authorized cloud drive and enforce company domain credentials. So for example, Cloud Drive will only ask for the user's Google Drive credentials and force them to use their enterprise email to log in.

Download As Required

Cloud Sync does not download the files to the computer. Files are only downloaded once they are clicked and synced back up as changes are saved. The file gets deleted from the computer once it is closed and fully synced up.

Choose What to Sync

Administrators can choose what folders they want to sync to the selected cloud drive. Select to sync Windows folders like Desktop, Documents, Downloads, Favorites, Music, Videos, etc.

ThawSpace in the Cloud

Using Deep Freeze? No problem! Cloud Sync saves data in a reserved space on the computer so that data will survive a restart. Data is only deleted from the computer once it is successfully uploaded to the selected cloud drive.

How it Works

The user enters their cloud drive credentials upon logging into the computer.

Cloud Sync will take control of the folders that the Administrator has selected to Sync. Folders such as Desktop, Music, Videos will be created in the user's cloud drive and all files will by synced into it.

On the desktop, the folders will display the files as links as they are yet to be downloaded. The blue icon shows the file is available for download. The orange sync icon shows the file is syncing. The green check icon shows the file has finished syncing.

www.faronics.com

Powered by faronics

Ouverture : PCA/PRA et solutions Cloud

Futur sujet : "Les PCA et PRA : utiliser le Cloud pour garantir une haute disponibilité et de la sécurité"

Cette future étude se penchera sur l'équilibre entre haute disponibilité et sécurité forte dans les Plans de Continuité d'Activité (PCA) et les Plans de Reprise d'Activité (PRA) en utilisant les nouvelles technologies du Cloud. Azure Site Recovery pourrait être un élément crucial pour cette exploration. Cet instrument est indispensable pour dupliquer des machines virtuelles d'un centre de données à un autre, facilitant ainsi une transition en douceur lors d'une défaillance. Par exemple, si un courtier en assurance basé à Paris rencontre une panne d'électricité, il aura toujours la possibilité de se connecter à ses serveurs de production en temps réel via une région Azure comme la région France-Sud. Ainsi, elle garantit un RPO (Recovery Point Objective) très bas et un RTO (Recovery Time Objective) de moins de 10 minutes. Cette méthode réduit les temps d'arrêt et inclut un cryptage solide AES-256, tout en respectant les normes RGPD, très importantes pour des secteurs comme la finance.

L'étude couvrira aussi un cas concret où une banque européenne utilise AWS Disaster Recovery pour atteindre un RTO de moins de 15 minutes. En déplaçant ses infrastructures critiques sur AWS, la banque a conçu une architecture avec plusieurs Zones de Disponibilité (multi-AZ) et une réplication en temps réel, en combinant cela avec des sauvegardes immuables stockées dans Amazon S3 Glacier. Lors d'une simulation d'attaque par ransomware, le système a permis de restaurer complètement les données et les applications en 12 minutes sans briser les normes de sécurité. Cet exemple met en évidence à quel point le Cloud public peut dépasser les solutions sur site, souvent coûteuses et moins flexibles.

Pour finir, l'étude traitera de nouveaux enjeux tels que : comment sécuriser les API qui administrent le cloud ou comment incorporer l'IA pour anticiper les pannes. Ce sujet étend la discussion sur la fiabilité des systèmes commencée avec Deep Freeze, en élargissant le débat aux infrastructures critiques et à l'importance d'une disponibilité sans interruption pour les entreprises.