koesio
Corporate IT

RENFORCEZ VOS SAUVEGARDES ET SANCTUARISEZ VOS DONNÉES AVEC HPE ET KOESIO

DÉCOUVREZ LES CLÉS POUR FORTIFIER VOTRE CYBERSÉCURITÉ FACE AUX MENACES

EN PARTENARIAT AVEC Hewlett Packard Enterprise

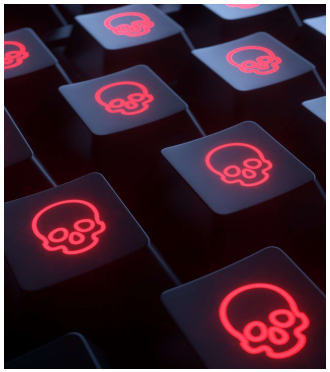
VOS INTERLOCUTEURS

Olivier Tant – HPE
Solution Business Manager, HPE Storage

Patrick De Oliveira – Koesio Corporate IT
Architecte IT Cloud hybride et Cyber-résilience

Top Challenges Pour les DSI

Sécurité et **Conformité à la Réglementation** dans cette période chaotique…

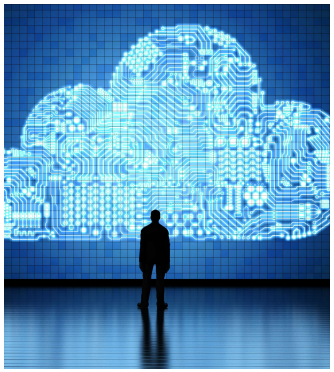


Menaces Cyber

- Attaques parrainées par des Etats
- Cybercriminalité organisée
- Ransomware and Ransomware as a Service (RaaS)

Perturbations non planifiées

- Catastrophes naturelles
- Défaillances matérielles
- Coupure de courant
- Erreurs d’utilisateurs



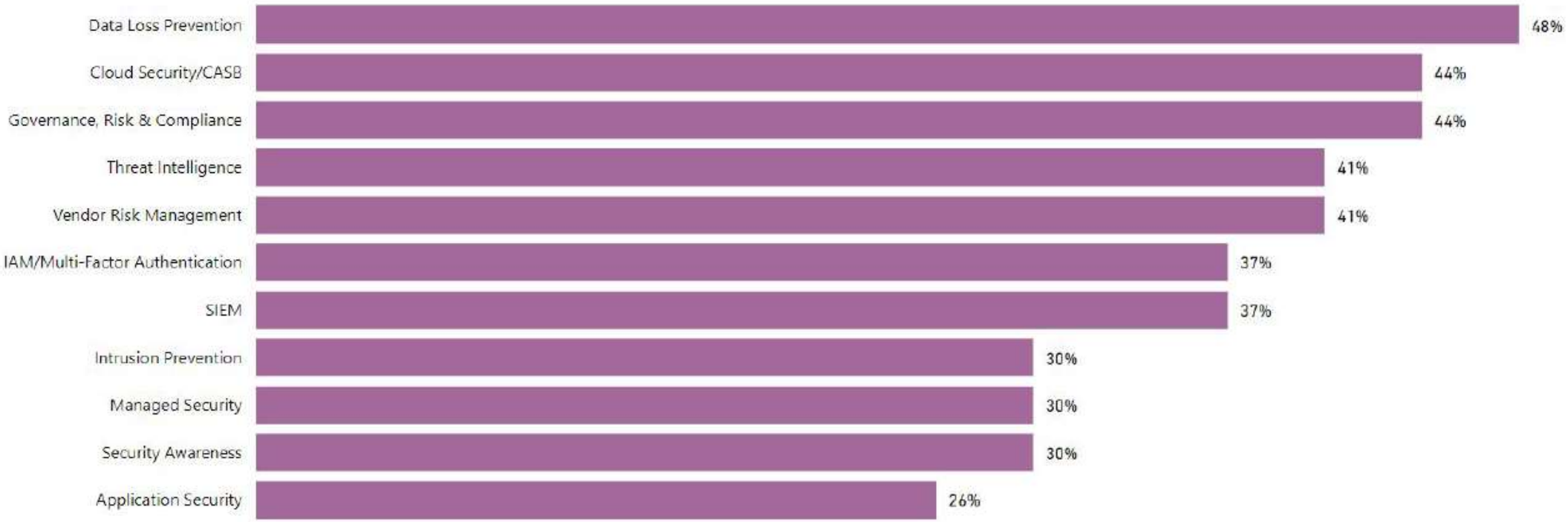
Complexité du Cloud

- Gouvernance et Souveraineté des Données
- Manque de compétences
- Vendor/platform lock-in

koesio Corporate IT

Top PRIORITES POUR LES CISO (Chief Information Security Officer)

Perte de données, conformité , réglementation
sécurité (zero trust, cloud, authentification…), fournisseurs…



koesio
Corporate IT

Top Challenges Pour les DSI

Sécurité et **Conformité à la Réglementation** dans cette période chaotique…

Augmentation des cyberattaques, menaces pendant les Jeux olympiques... Le "8h30 franceinfo" de Vincent Strubel

Mardi 27 février 2024

Cyberattaques : "On n'a plus besoin aujourd'hui d'être une cible pour être une victime", alerte l'Anssi

Vincent Strubel, directeur général de l'Agence nationale de sécurité des système d'information (Anssi), sur franceinfo le 27 février 2024. - FRANCEINFO / RADIO FRANCE

koesio Corporate IT

PROTECTION DES DONNÉES : UN RENFORCEMENT VITAL !

Vital, car la perte de disponibilité, de données peut vous mener à la perte

*50 % des PME ayant eu tout leur système d'information bloqué plusieurs semaines à la suite d'une attaque informatique (généralement un rançongiciel), auraient fait faillite dans les 6 mois ayant suivi - **Etude Hiscox assurance, 2020***

Thales visé par une nouvelle attaque du groupe russophone de ransomware LockBit 3.0

Le groupe d'électronique français Thales confirme l'ouverture d'une enquête interne sur une allégation de vol de données par LockBit 3.0. Le groupe de pirates informatiques russophones a revendiqué une cyberattaque contre Thales dans une communication sur le darknet.

LA TRIBUNE

01 Nov 2022

LeMagIT Akka Technologies aux prises avec un ransomware

Mai 2022

Le groupe français d'ingénierie et conseil Akka Technologies (environ 21.000 salariés) a été frappé par une cyberattaque par rançongiciel qui touche une bonne partie de l'entreprise

L'Institut national polytechnique de Toulouse est en proie à un ransomware

L'USINEDIGITALE

15 Septembre 2022

Des hackers s'en sont pris à l'Institut national polytechnique de Toulouse, qui regroupe six écoles et 6500 étudiants ingénieurs. Les activités seraient fortement perturbées. En

Caen : quatre mois après la cyberattaque, de nombreux sites et services en ligne redémarrent

actu.fr

La cyberattaque ciblant la ville de Caen et la communauté urbaine Caen la Mer a empêché l'usage de services en ligne durant plusieurs mois. Certains viennent de rouvrir.

Économie

Clestra dépose le bilan après une cyberattaque

Publié le 01/08/2022 à 15:38, mis à jour le 02/08/2022 à 12:29

Spécialisée dans la fabrication de cloisons de bureaux, de salles blanches et d'espaces d'isolement, Clestra réalise 145 millions de chiffre d'affaires et emploie 700 salariés.

L'hôpital André-Mignot du centre hospitalier de Versailles victime d'une cyberattaque

L'accueil des patients est limité et une cellule de crise a été ouverte. Par mesure de sécurité, le système informatique est coupé.

franceinfo:

Publié le 04/12/2022 10:22

Après la cyberattaque, une facture de 7 millions d'euros pour l'hôpital de Corbeil-Essonnes

Sécurité : *Outre deux millions d'euros déjà engagés dans la crise, le centre hospitalier de Corbeil-Essonnes va devoir dépenser cinq millions d'euros supplémentaires en 2023 pour rebâtir une infrastructure informatique solide.*

ZDNET

Publié le mercredi 28 sept. 2022

koesio Corporate IT

En France, l'ANSSI définira la réglementation locale pour NIS2

NIS 2 = NETWORK & INFORMATION SECURITY version 2

LES OBLIGATIONS POUR LES ENTITÉS RÉGULÉES

MESURES DE SÉCURITÉ PRÉVUES PAR NIS 2

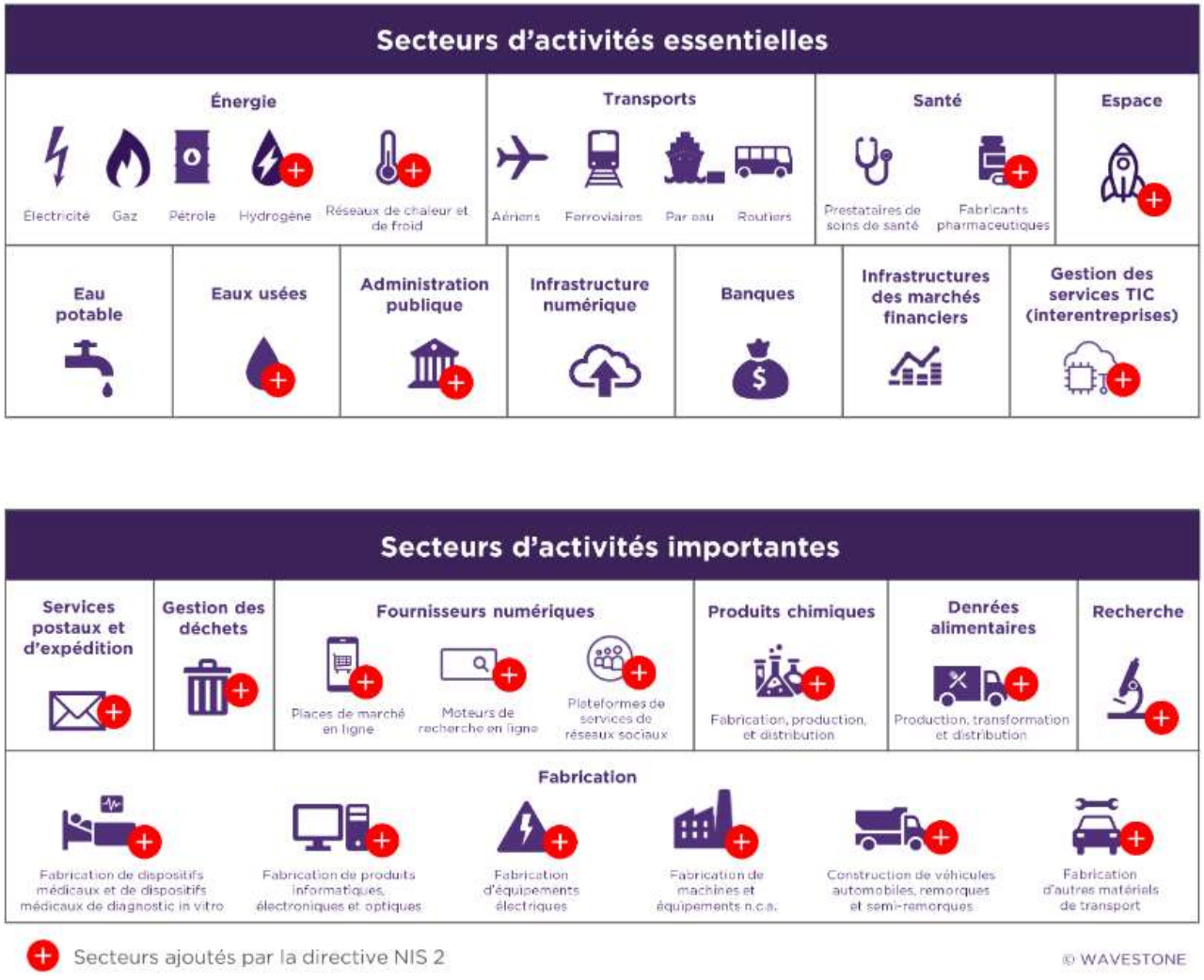
1. les politiques relatives à l'analyse des risques et à la sécurité des SI ;
2. la gestion des incidents ;
3. la continuité des activités (sauvegardes, PRA gestion des crises) ;
4. la sécurité de la chaîne d'approvisionnement (fournisseurs/prestataires) ;
5. la sécurité de l'acquisition, du développement et de la maintenance des SI ;
6. des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité ;
7. les pratiques de base (cyberhygiène et formation à la cybersécurité) ;
8. des politiques et des procédures relatives à l'utilisation de la cryptographie ;
9. la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs ;
10. l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins.

Les personnes physiques en charge de faire appliquer la directive dans l'entités seront tenus comme responsables en cas de non-respect des obligations de la directive

-> La direction des entreprises (DG/DSI/RSSI) doit s'impliquer

koesio Corporate IT

Les entreprises concernées par NIS 2



Pris en compte versus le CA >10m€
et/ou
nb employés (>50)

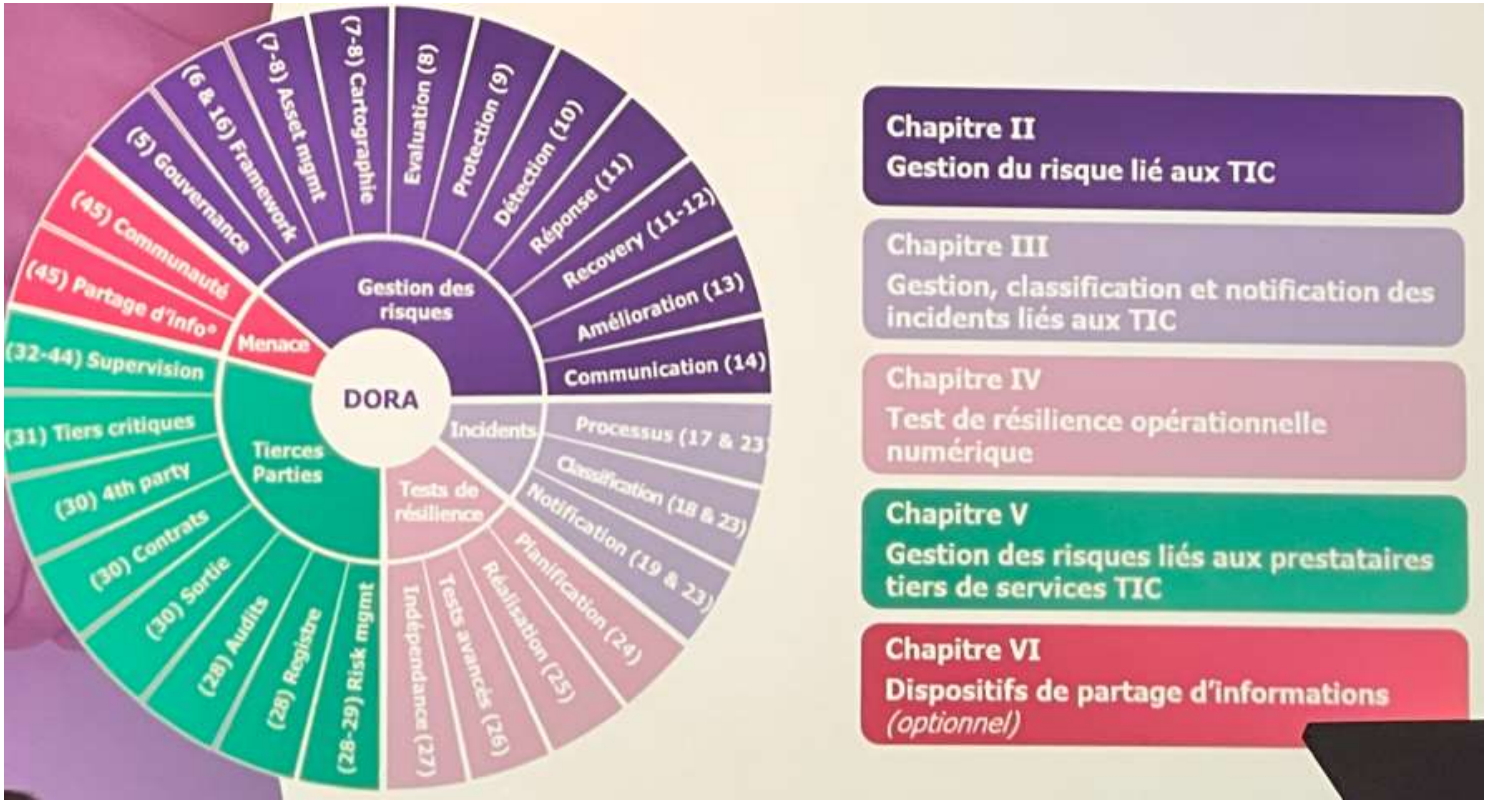
koesio Corporate IT

DORA: les 4+1 chapitres qui s'imposeront dès janvier 2025

DORA = Digital Operational Resilience Act

Réglementation sur la résilience Numérique pour les entités financières.

La non-conformité peut fortement pénaliser ces entreprises (amendes, suspension d'activités…)



Source: Cabinet Wavestone

TEST de la BCE en 2024 sur la capacité de gestion de crise et de restauration

koesio Corporate IT

Les entreprises concernées par DORA

(a)les établissements de crédit,
(b)les établissements de paiement,
(c)les établissements de monnaie électronique,
(d)les entreprises d'investissement,
(e)les prestataires de services sur crypto-actifs, les émetteurs de crypto-actifs, les émetteurs de jetons….
(f)les dépositaires centraux de titres,
(g)les contreparties centrales,
(h)les plates-formes de négociation,
(i)les référentiels centraux,
(j)les gestionnaires de fonds d'investissement alternatifs,
(k)les sociétés de gestion,
(l)les prestataires de services de communication de données,
(m)les entreprises d'assurance et de réassurance,
(n)les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire,
(o)les institutions de retraite professionnelle,
(p)les agences de notation de crédit,
(q)les contrôleurs légaux des comptes et les cabinets d'audit,
(r)les administrateurs d'indices de référence d'importance critique,
(s)les prestataires de services de financement participatif,
(t)les référentiels des titrisations,
(u)les tiers prestataires de services informatiques.

koesio Corporate IT

DU CONTEXTE … AUX BONNES PRATIQUES

Hewlett Packard Enterprise

Cybermalveillance.gouv.fr cf. Fiche - Prévention du risque numérique : les bonnes pratiques de sauvegardes

CNIL cf. Fiche CNIL : Sécurité Sauvegarder et prévoir la continuité d'activité

ANSSI - Etat de la menace rançongiciel (ransomware)

Vos 10 résolutions

1. 90 % des failles sont le produit d'une erreur humaine : culture, sensibilisation aux risques, formation, simulation, vigilance collective
2. Ne pas payer de rançon : 68 % des entreprises qui payent subissent de nouveau une attaque peu de temps après.
3. Adopter le modèle « Zero trust » : Essor du « secure by design », et fin de la « confiance implicite » (réseaux, systèmes, apps, emails, API)
4. Mettre à jour votre SI : applications des fix FW / OS / Applicatifs …
5. Protéger son système d'information par des sauvegardes extérieures aux réseaux pour ne pas être complètement paralysé par une cyberattaque.
6. Effectuer des sauvegardes Régulières en appliquant a minima la règle du 3-2-1
7. Rendre les dispositifs de sauvegarde hermétiques et « inviolables » isolation réseau & authentification, chiffrement & immuabilité des données
8. Déployer des approches en amont de la Sauvegarde "classique" : protection des données continue, solution spécialisée DR.
9. Mettre à jour, programmer et simplifier le plan de reprise et de continuité d'activités.
10. Contrôler, tester et optimiser régulièrement l'application du plan de continuité ou de reprise de l'activité, la restauration des sauvegardes.

koesio Corporate IT

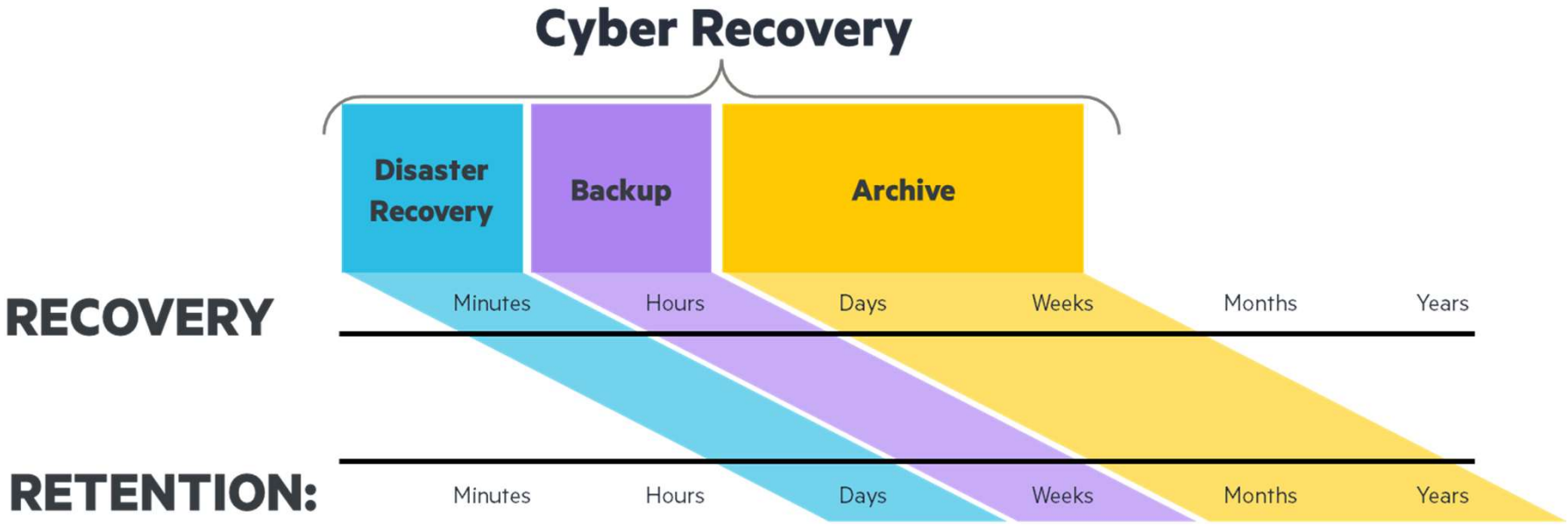
PRÉVENIR LES IMPACTS DES RISQUES CYBER EN 2024 ?

Implémenter une solution DISASTER RECOVERY dédiée est désormais une approche privilégiée

ANSSI Agence nationale de la sécurité des systèmes d'information

DORA Regulation

NIS 2 DIRECTIVE



koesio Corporate IT

PROTECTION DES DONNEES DE BOUT EN BOUT AVEC HPE

Hewlett Packard Enterprise

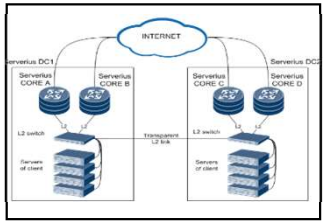
Reprise Ransomware	Reprise après sinistre	Sauvegarde & récupération	Rétention à long terme	Multi-cloud mobilité
• Récupération à grande échelle • Récupérez quelques secondes avant une attaque • Analyse des données	• Pannes matérielles • Catastrophes naturelles • Des pannes de courant • Tests automatisés	• Erreurs utilisateur • Suppressions de fichiers • Corruptions	• Exigences légales • Rétablissement de la conformité	• Migrations • Hybride, multi-cloud • Consolidations de centres de données • Modernisation des infrastructures

koesio Corporate IT

6 niveaux de protection des données par HPE

NIVEAU DE SÉCURITÉ DES DONNÉES

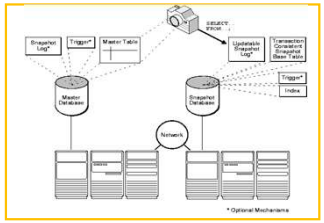
1 Haute disponibilité



Strectched Cluster / Métrocluster

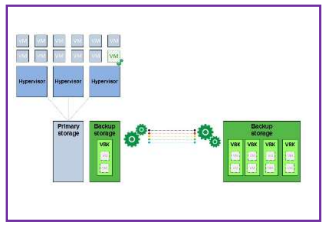
Peer Persistence

2 Copie primaire cyber-résiliente



Snapshot
Immuabilité

3 Sauvegarde sur site



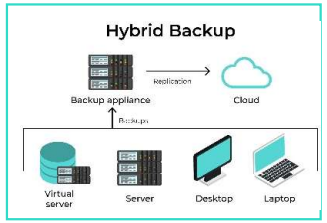
HPE GreenLake for Backup & Recovery

Appliance StoreOnce

Stockage Disque

Partenariat HPE avec Veeam…

4 Sauvegarde sur le Cloud

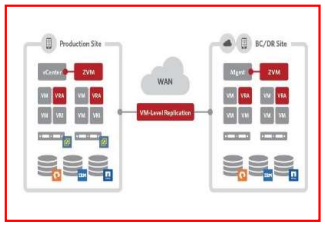


HPE GreenLake for Backup & Recovery

StoreOnce CloudBank

Partenariat HPE avec Veeam…

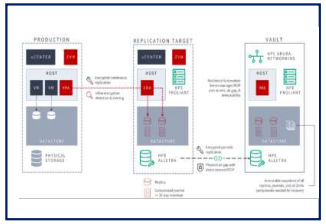
5 Reprise après sinistre



HPE GreenLake for Disaster Recovery

Zerto

6 Copie secondaire cyber-résiliente



Offres « Zerto cyber resilience Vault*

Stockage Objet S3 immuable

Tape HPE (StoreEver / LTO)

DISASTER RECOVERY

Sécurisez, migrez, gérez vos applications & données à travers les hyperviseurs, infra, cloud…

Zerto

a Hewlett Packard Enterprise company

Protection continue des données

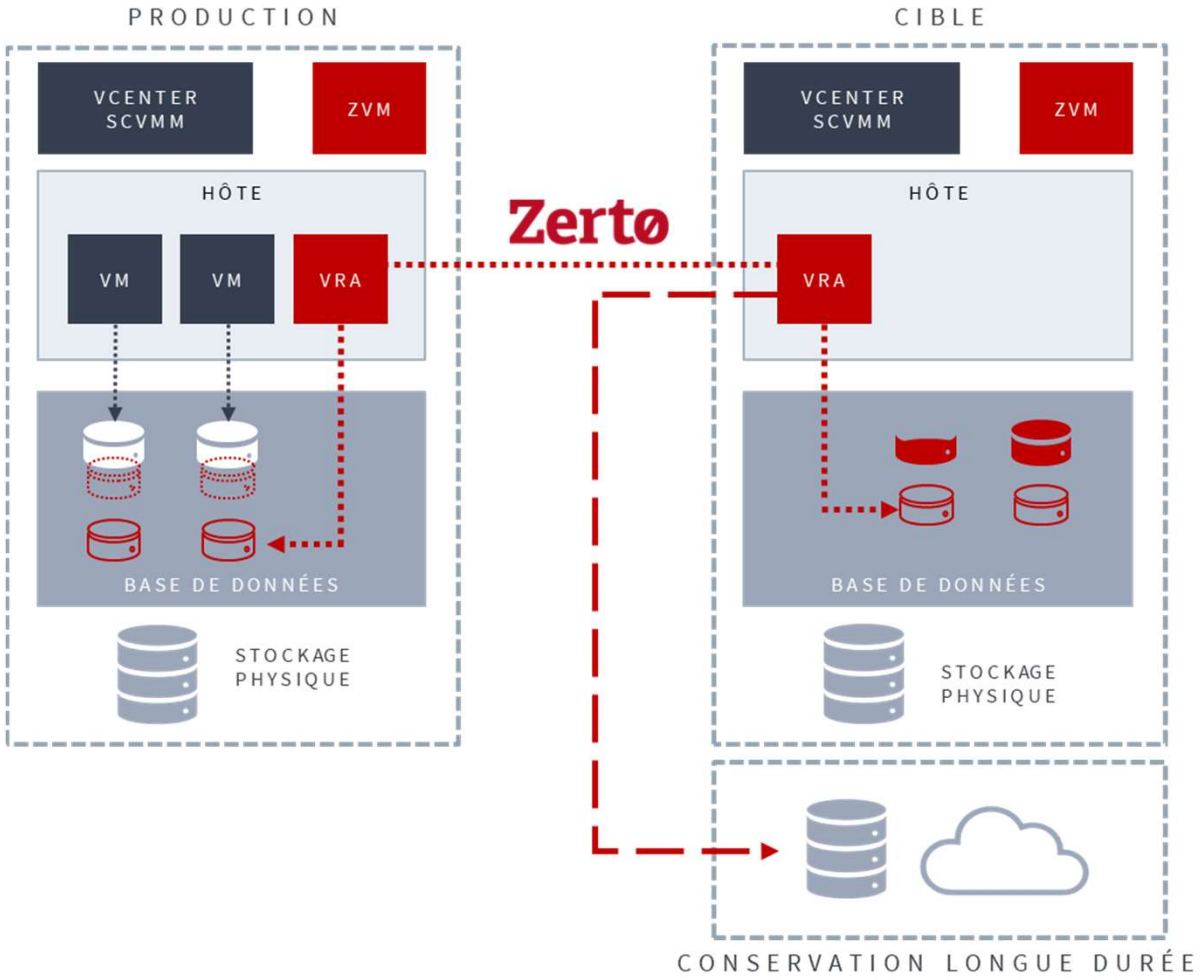
Reprise après ransomware | **Reprise après sinistre** | **Mobilité multicloud**

Orchestration | Automatisation | Analyses

koesio Corporate IT

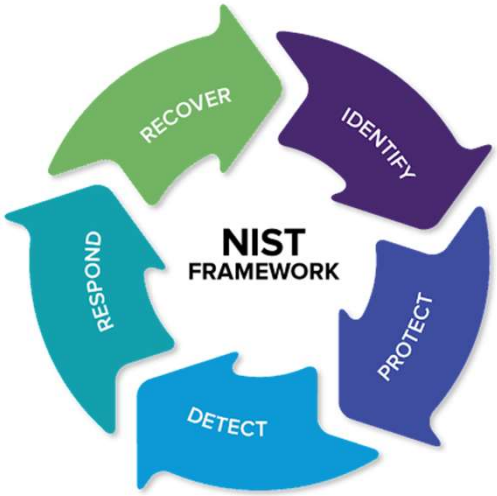
APERÇU HPE ZERTO

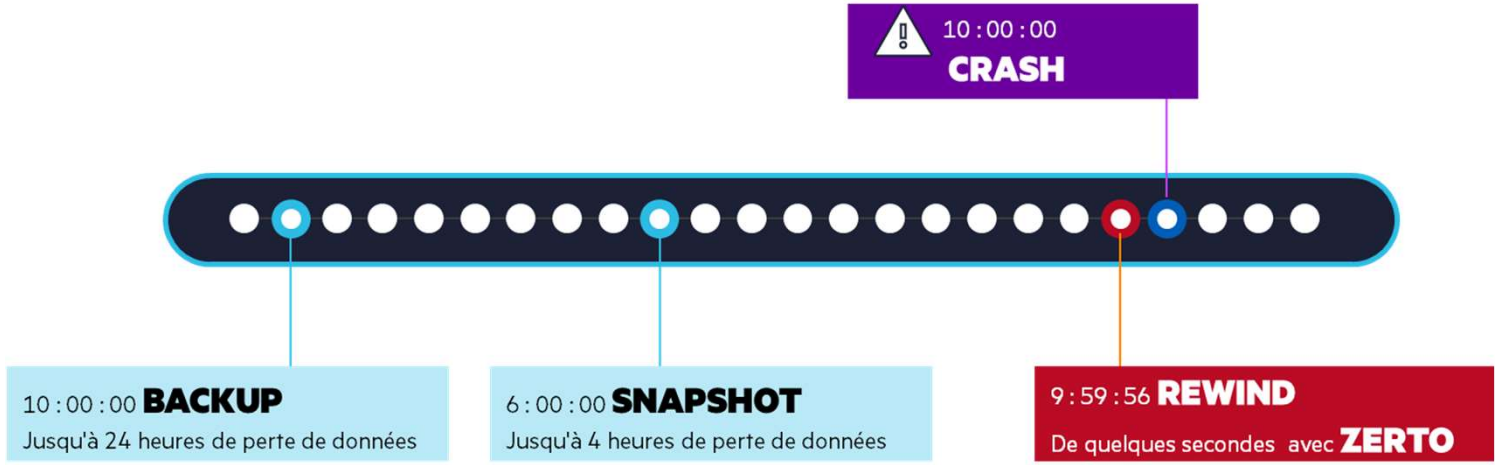
- **Protection continue** des VM / apps / data
- **Réplication** quasi Synchrone
- **Journalisation** de point de reprises
- **Zéro RTO / RPO »** (qq secondes)
- **100% Logiciel** (Indépendance HW)
- **Zéro** planification, agents
- Design & Déploiement **simples**
- **Cloud ready** : Private , Hybrid & multi



TECHNLOGIE UNIQUE DE JOURNALISATION

Tests et récupération granulaires avec le journal dynamique Zerto





DETECTER
chiffrement anormal en temps réel pour alerter d'un éventuel ransomware

REPONDRE
rapidement pour minimiser la perte de données

REPRENDRE
quelques secondes seulement avant une attaque

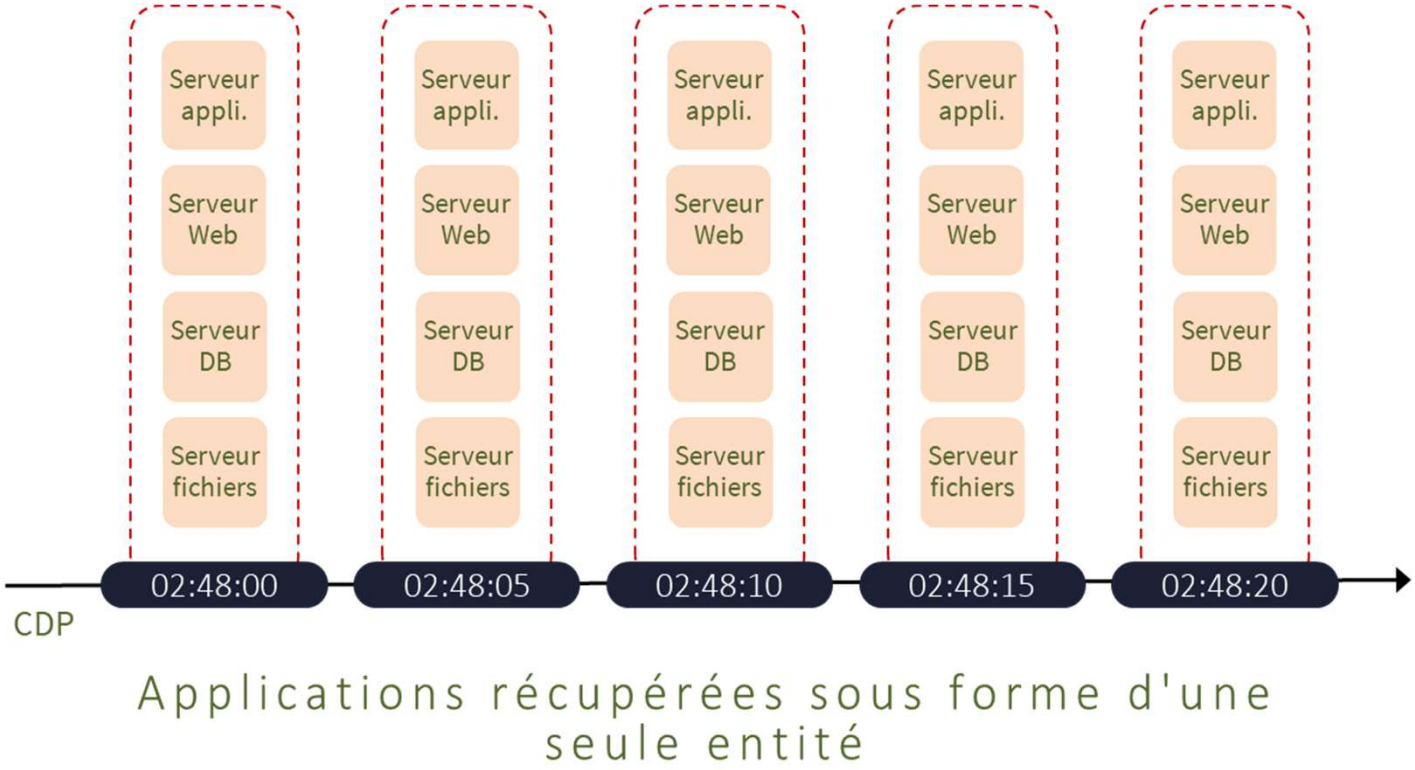
koesio
Corporate IT

HPE ZERTO – REPRISE COHÉRENTE DES APPLICATIONS

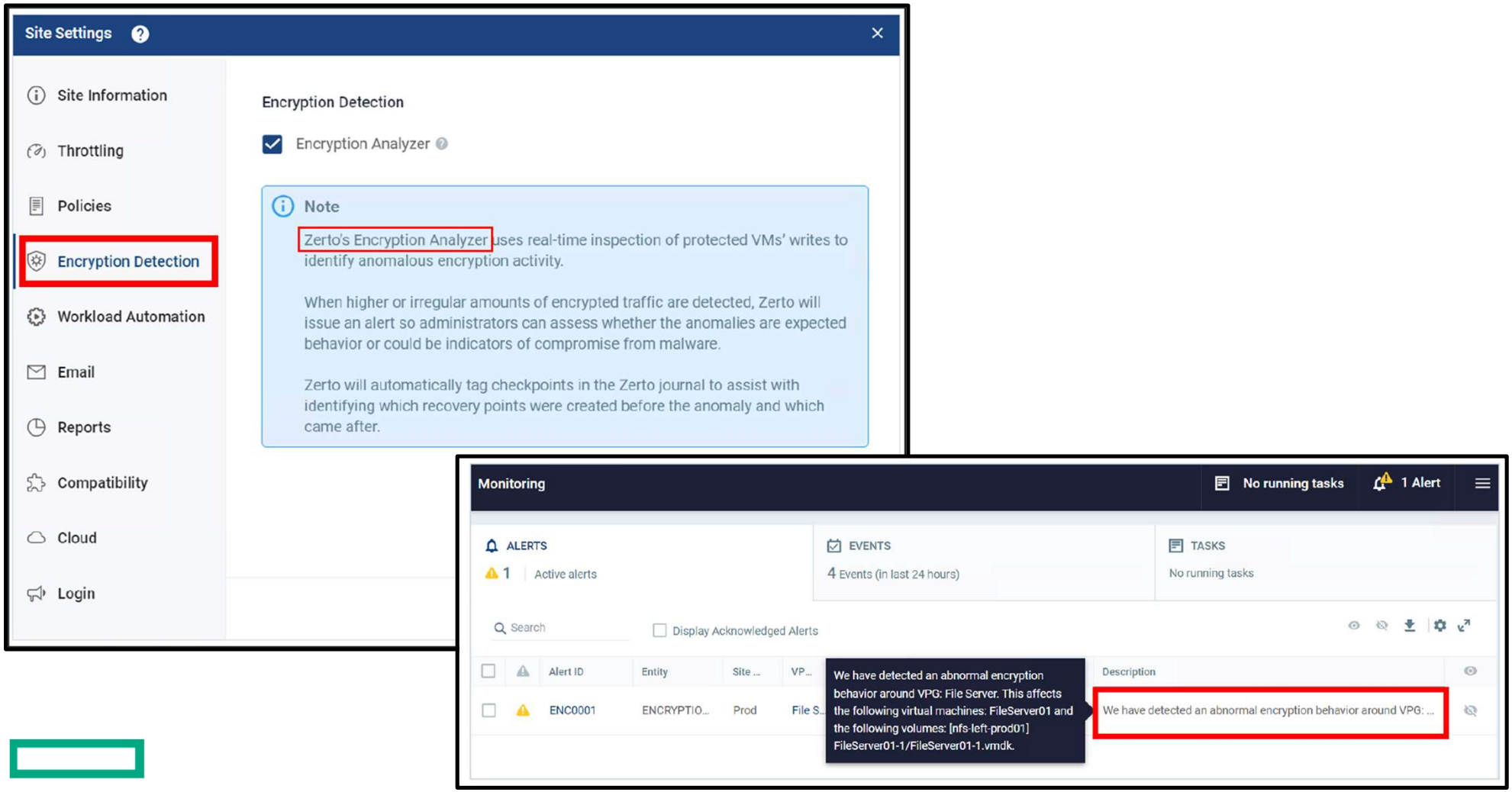
Fidélité de l'ordre d'écriture sur toutes les machines virtuelles d'une application

Points de restauration cohérents même pour les VM sur différents datastores ou hôtes

Aucune fenêtre de sauvegarde échelonnée et aucune tâche de réplication planifiée

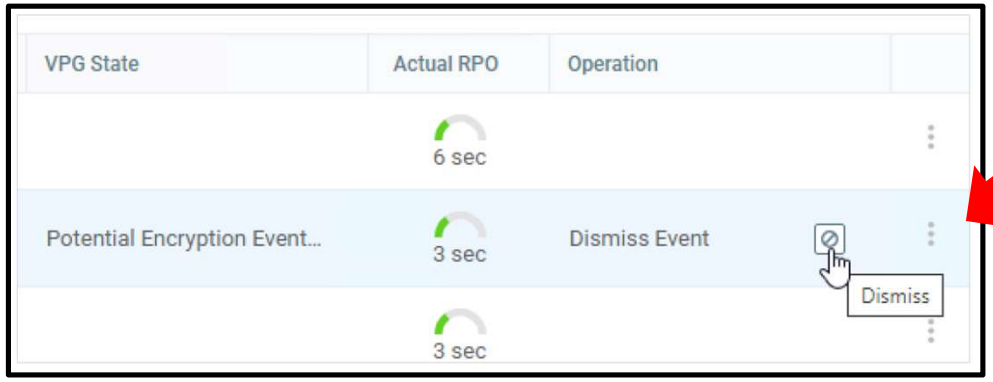


HPE ZERTO – DÉTECTION TEMPS-RÉEL ZERTO



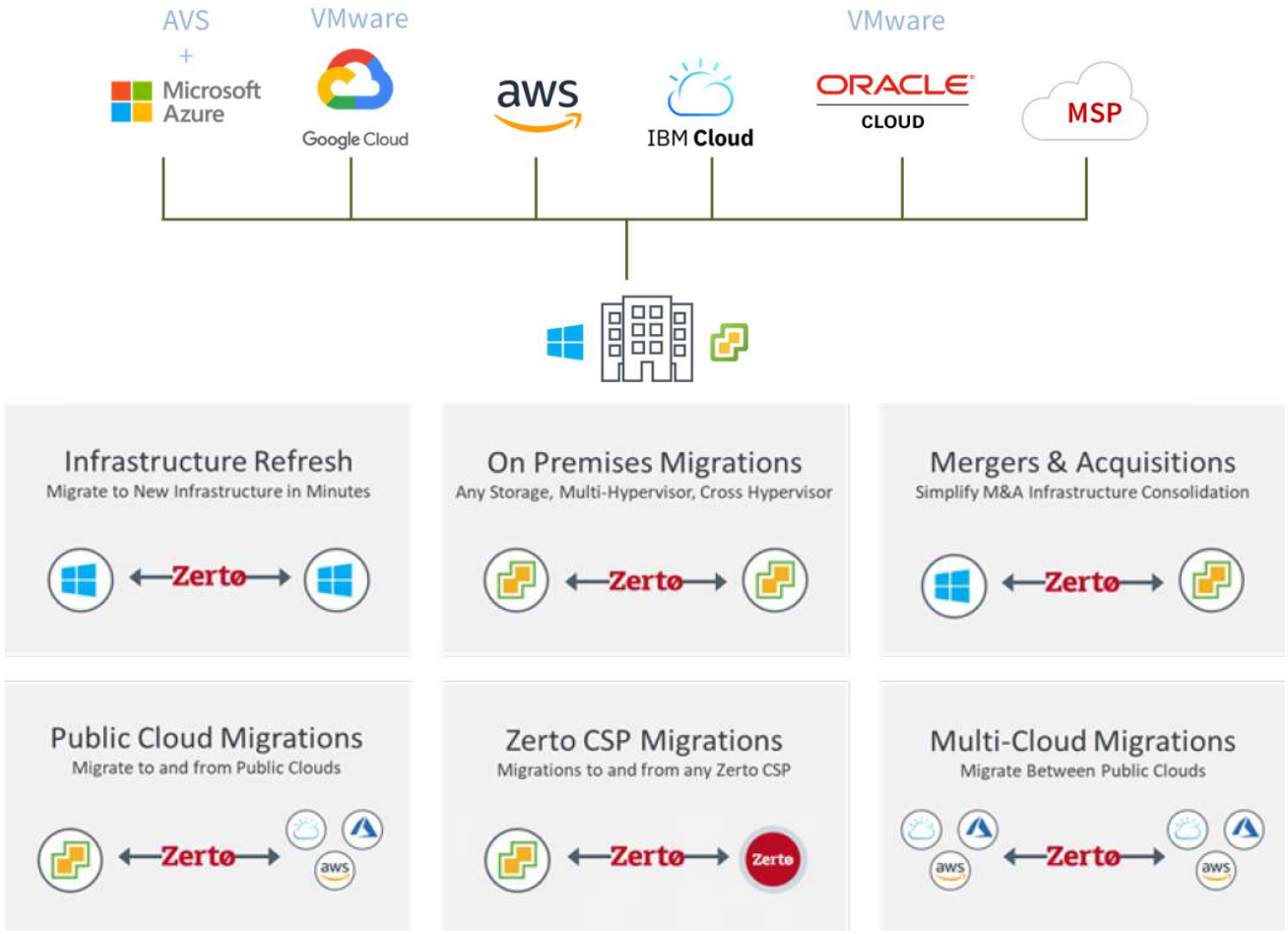
koesio Corporate IT

HPE ZERTO – DÉTECTION TEMPS-RÉEL



HPE ZERTO –LIBÉREZ L'AGILITÉ DU CLOUD

Simplicité de la mise en œuvre, mobilité et conversion transparentes des VM du site vers le cloud natif

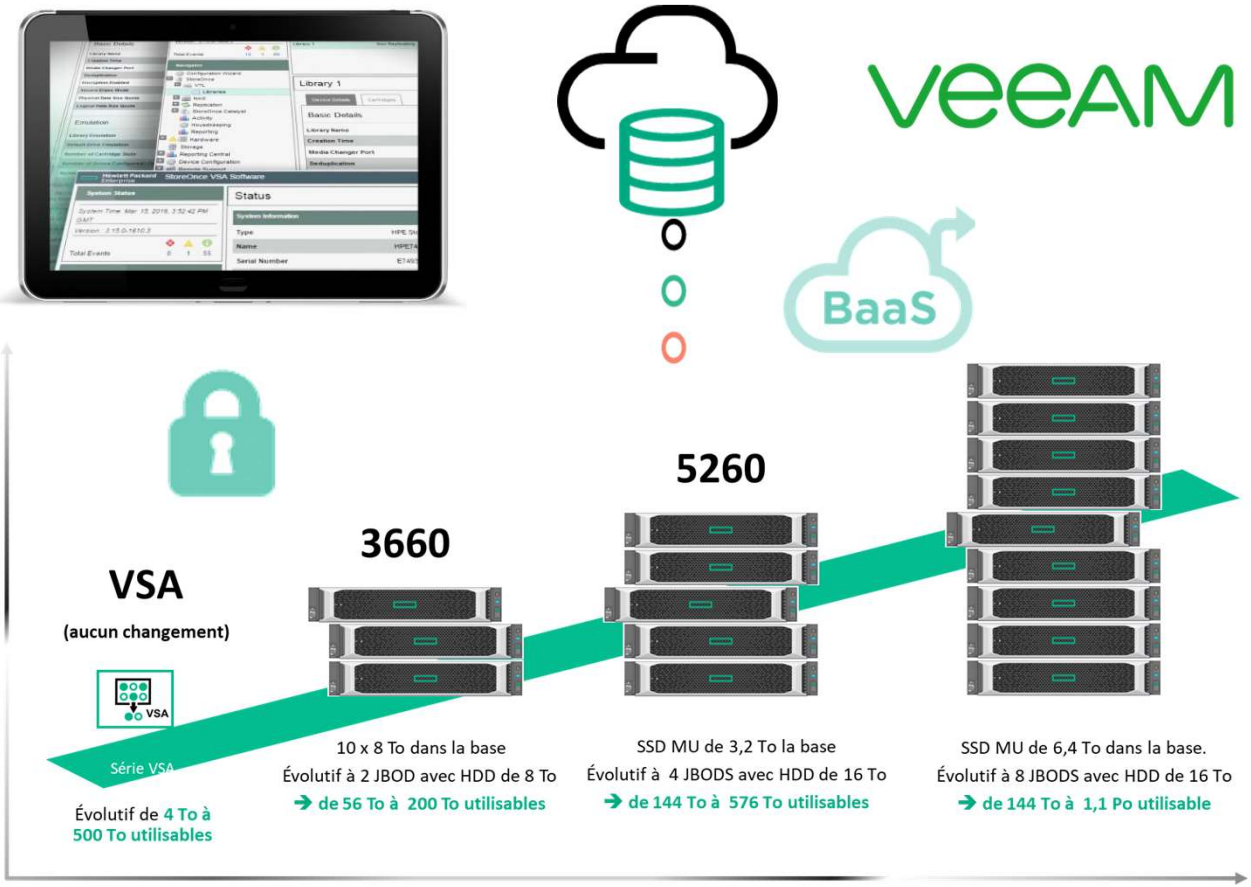


HPE STOREONCE

Éliminez la complexité en consolidant, simplifiant, accélérant les sauvegardes

INFO !

- Solutions dédiées clef-en-main & simples
- Application Matérielle, virtuelle ou Cloud
- Scalabilité : capacité & Performance
- Robustesse & disponibilité
- Déduplication
- Virtualisation (VTL, NAS, API Catalyst)
- Connexion FC / Ethernet
- Sécurité (chiffrement, MFA, immuabilité…)
- Intégration applicatives (Oracle, SAP, SQL…)
- Intégration logiciel de sauvegarde
- Copie « cloud » Object » : AWS, Azure, Scality…



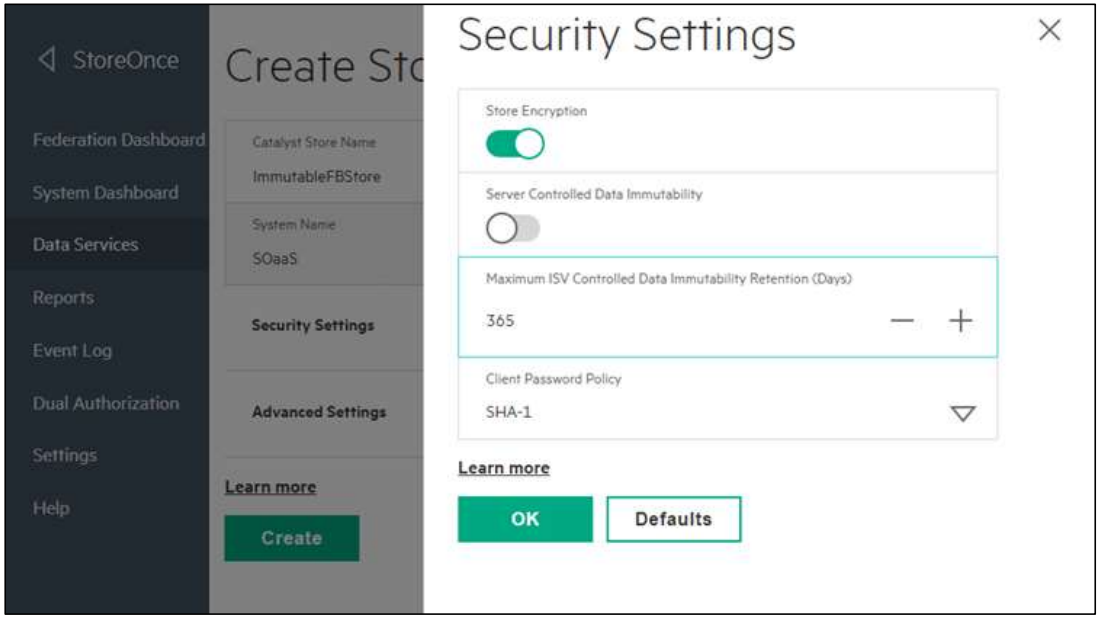
koesio Corporate IT

HPE STOREONCE : SANCTUARISER LES DONNÉES AVEC VEEAM

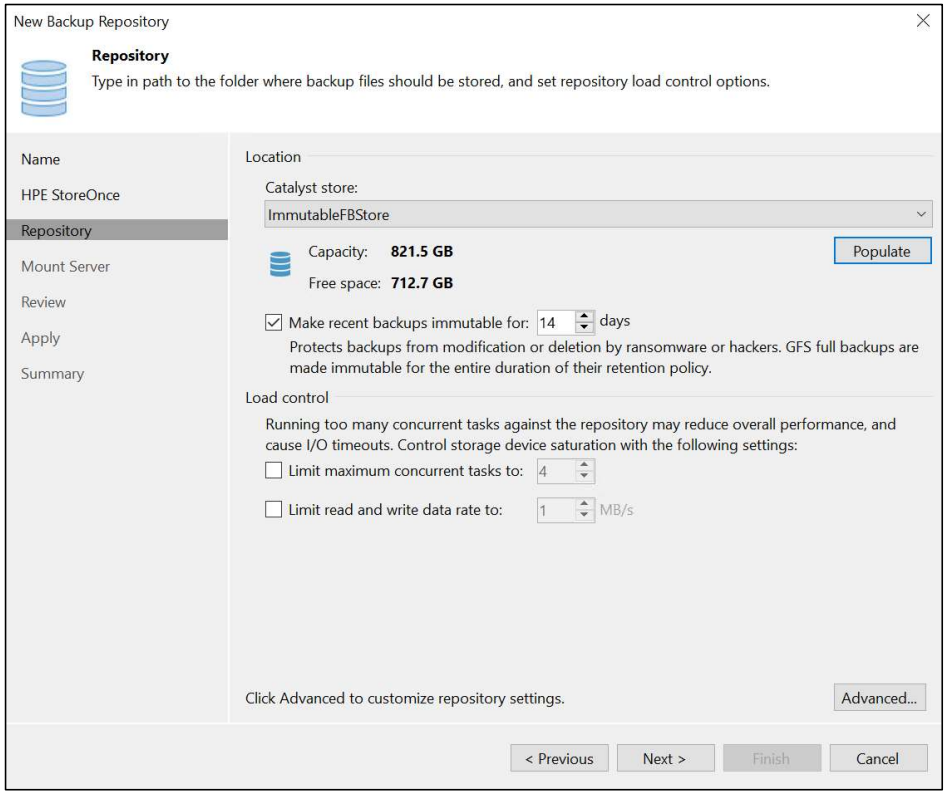
Exemple : « Data immutability » avec Veeam

HPE StoreOnce

Catalyst



VEEAM

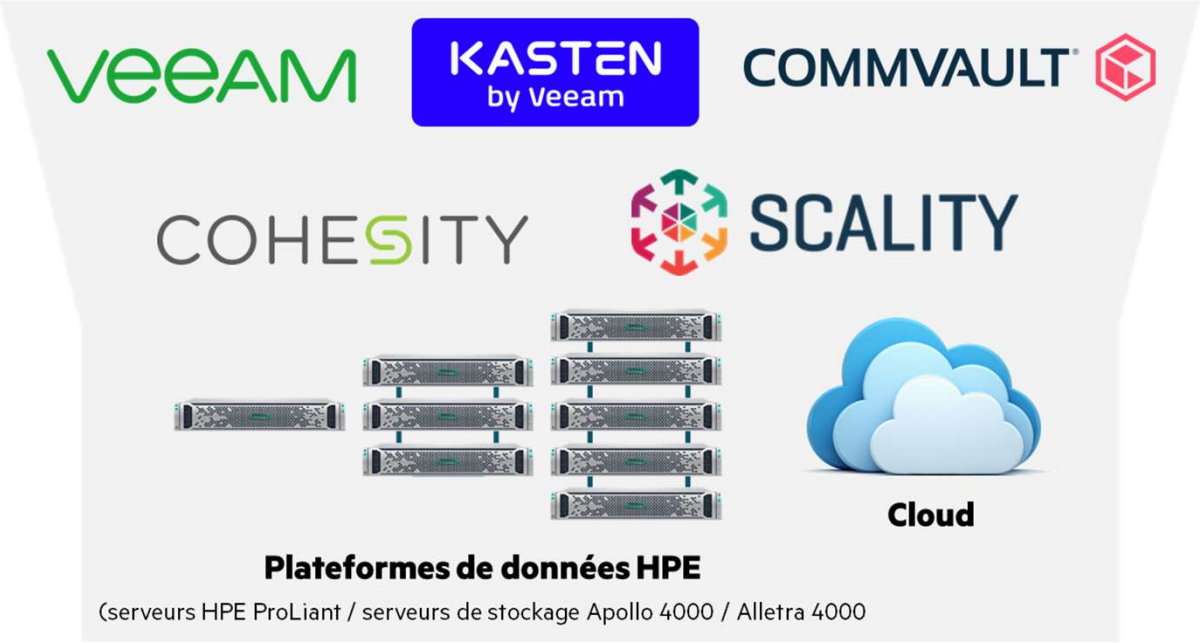


koesio Corporate IT

PROTECTION BASEE 100% SERVEUR DEFINI PAR LOGICIEL, HYPERCONVERGEE

Le meilleur du savoir-faire serveur HPE intégrant (accords OEM) les éditeurs leaders du marché

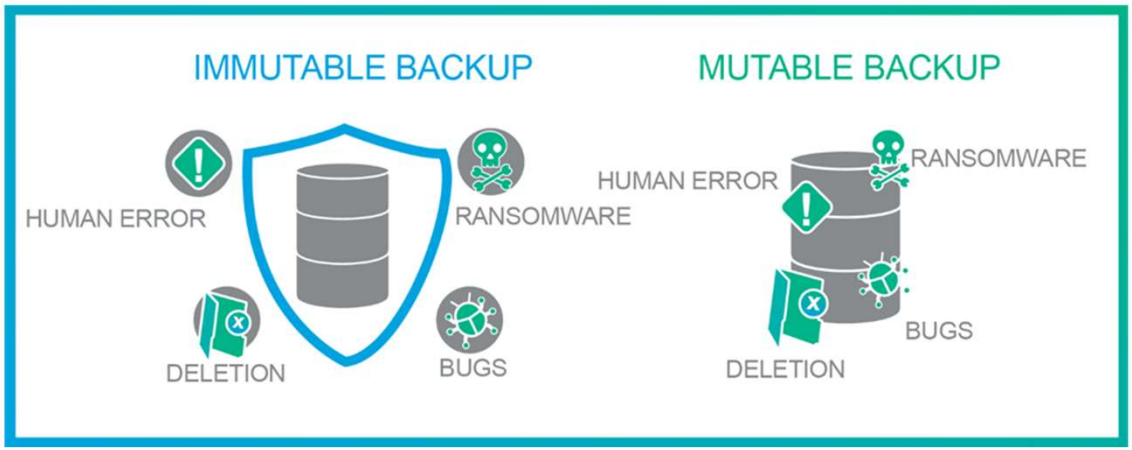
Veeam	Disponibilité & protection VM Private / hybrid / Public / multi cloud
Kasten	Disponibilité & protection des workloads conteneurs Private / hybrid / Public / multi cloud
Commvault	Disponibilité & protection 360° (device, serveurs physiques, virtuels, VM, container, clouds)
Cohesity	Stockage, disponibilité & protection & gestion 100% hyperconvergé
Scality	Stockage fichier et/ou Objet disponible, hyper-résilience, durable, immuable



koesio Corporate IT

LE CONSTAT : DES SAUVEGARDES CIBLÉES ET VULNÉRABLES

- Erreur, incident ou Cybercriminalité : le risque Zéro n'existe pas
- Les sauvegardes sont visées par les cybercriminels
- Sauvegardes indisponibles = zéro recours en cas d'attaque
- Besoin de mise en conformité (ANSSI / DORA / NIS2…)
- Besoin de solution simple , moderne, évolutive, cloud ready



SANCTUARISER LES SAUVEGARDES AVEC HPE SCALITY ARTESCA

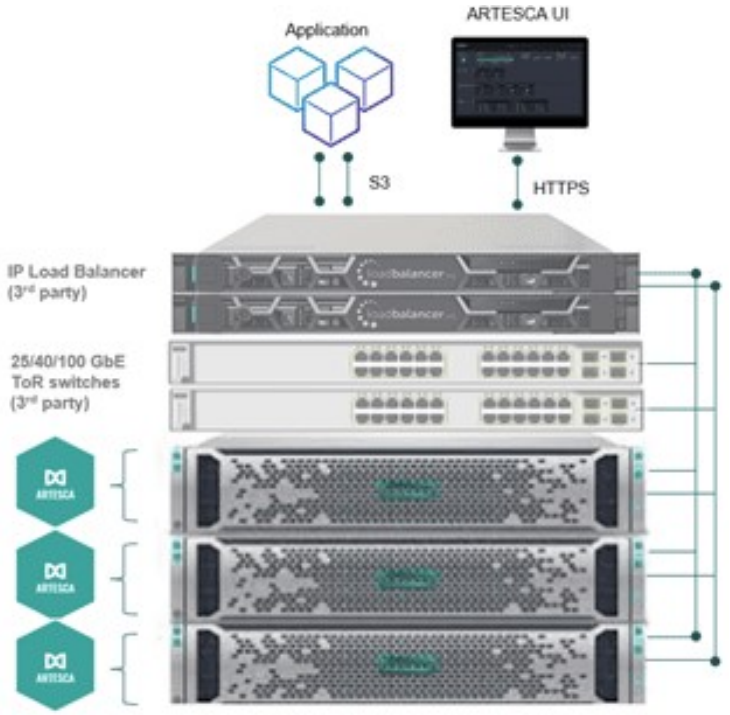
Vos applications, vos datacenters, vos edges, les clouds que vous choisissez

Avantages techniques clés :

- Ne manque jamais de **capacité**
- **Durabilité** élevée des données (11x9s)
- **Disponibilité** ~100 % et performance (6 To/h)
- sauvegarde & restauration , **SLA** .
- Sauvegardes **objet directe**
- **Zéro silo** : architectures simplifiées, élimine la complexité des bandes, élimine les migrations
- Commence à **1 nœud,** cluster **3 nœuds**
- **API S3** standardisée, prête pour le cloud

Protection ultime :

- Selon Veeam, 94 % des cyberattaques / ransomware ciblent en premier la sauvegarde. (68% réussissent)
- **S3 ObjectLock** : protection **WORM** activée au niveau du protocole
- Sauvegardes **immuables**
- **Reprise après sinistre** efficace
- **Restaurations** rapides



SOLUTIONS HPE SCALITY : SANCTUARISER LES DONNÉES AVEC VEEAM

Exemple : « Data immutability » Scality avec Veeam

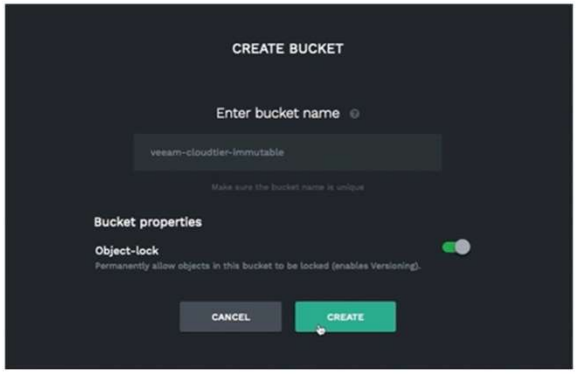
Configurez l'immutabilité en quelques clics

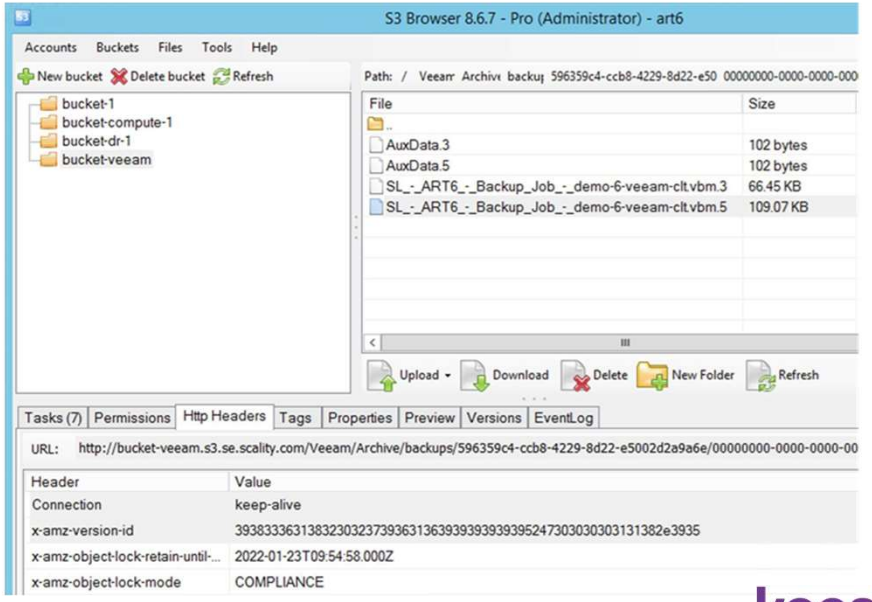
- Choisissez le bucket avec Object Lock
- Créez des préfixes au sein du bucket
- Sélectionnez l'option pour rendre immuable
- Déterminez le temps d'immutabilité

Veeam utilise la fonctionnalité **S3 Object Lock** (« Compliance mode »)

L'immutabilité n’est pas déprogrammable une fois activée.

Les sauvegardes dans des "buckets" immuables sont inviolables !

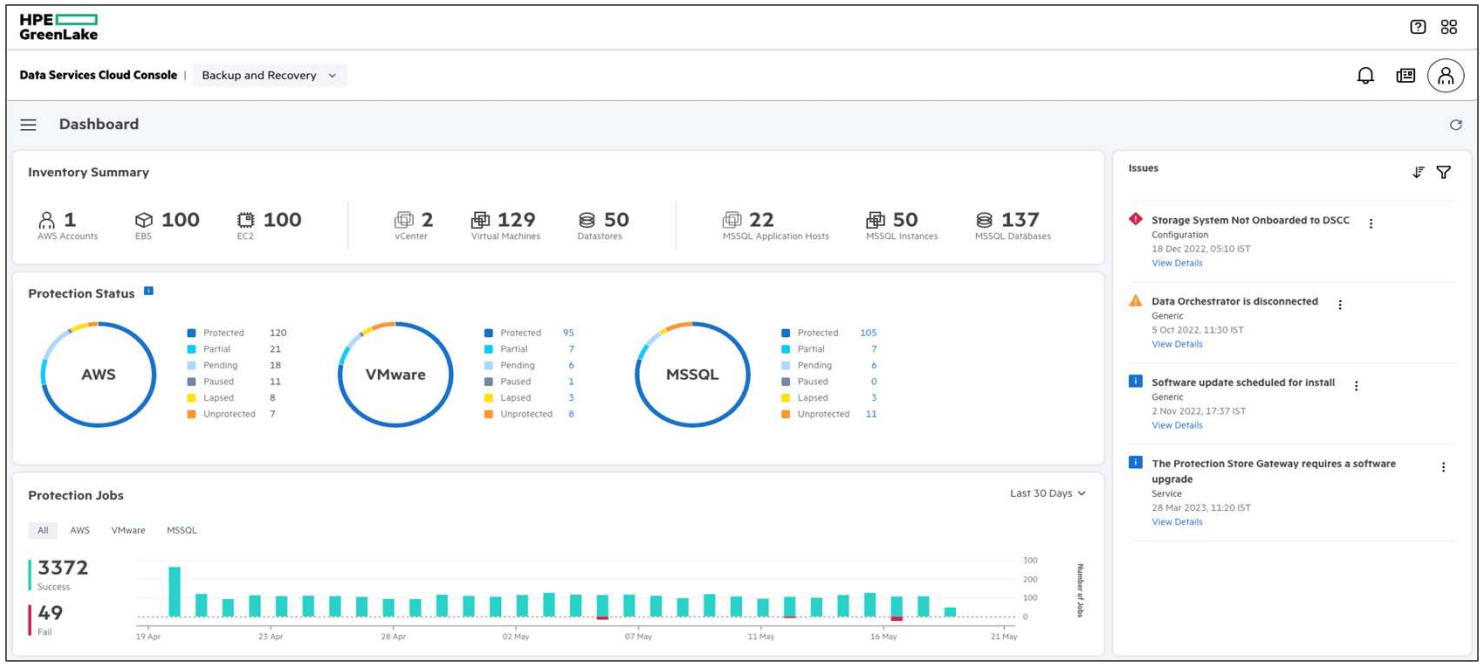




MODERNISER / SIMPLIFIER LA PROTECTION EN MODE SAAS

HPE GREENLAKE FOR BACKUP & RECOVERY

Solution de sauvegarde efficace du secteur pour VMware, la base de données MS SQL Server, Amazon EBS, EC2 , RDS et EKS (et en beta M365… et à venir Azure)



Protection automatisée sans effort sur le cloud hybride

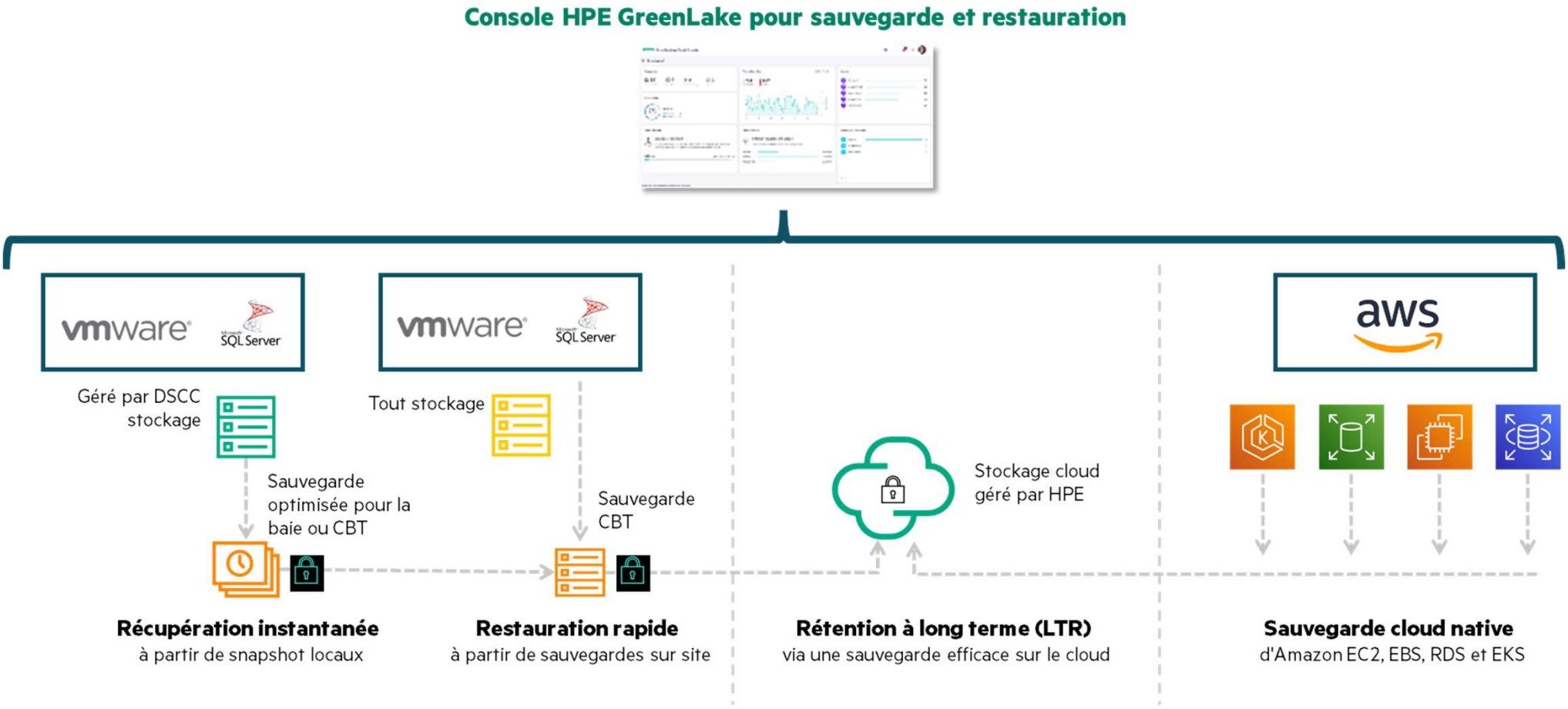
Protége contre les risques, les ransomwares

Simple, protégez en quelques mn, 5 clics

koesio Corporate IT

HPE GREENLAKE FOR BACKUP & RECOVERY

Plan de contrôle SaaS unique avec orchestration et automatisation intégrées



koesio Corporate IT

HPE GREENLAKE FOR BACKUP & RECOVERY

Avantages clés

- **BENEFICES DU SAAS :** simplicité, nouvelles fonctionnalités automatiquement disponibles (pas de MAJ SW), Edge to cloud (idéal sites distribués)
- **Chiffrement** : Toutes les données, au repos et en vol
- **Immutabilité** : Copies de données qui ne peuvent être modifiées par personne
- **Double autorisation** : Les opérations destructrices nécessitent une escalade et une approbation
- **Air Gap** : Déconnexion physique entre l'environnement de production et la copie de sauvegarde
- **Economique:** Coût à l'asset de l'ordre de 3 € / mois
- (+ « cloud storage » associé le cas échéant) , dedupe

Moderniser / Simplifier
la protection
en mode SaaS

koesio
Corporate IT

MERCI !

koesio.com

EN PARTENARIAT AVEC Hewlett Packard Enterprise