#pw2025

Power Week 2025

18 - 19 - 20 novembre 2025

IBM Innovation Studio Paris

IBM Flashsystem Safeguarded Copy avec IBM i

20 novembre

Antoine Maille
IBM France
amaille@fr.ibm.com

Ludovic Menard
IBM France
ludovic_menard@fr.ibm.com

Guillaume Legmar
IBM Techzone
guillaume.legmar@fr.ibm.com

IBM

common FRANCE

La Cyber Criminalité
est déjà bien organisée … et vous ?

59% des organisations frappées par une attaque ransomware en 2024*

94% des victimes précisent que les attaquants ont d'abord ciblé **leur sauvegarde***

70% des attaques consistent au chiffrement des données*

78% Des victimes ont mis plus de 100 jours pour s'en remettre**

$4.88M Cout moyen d'une attaque**

56% Payent pour récupérer leurs données*

* Source: Sophos The State of Ransomware 2024
** Source: IBM Cost of a Data Breach 2024

Comment/Pourquoi aborder le sujet maintenant ?

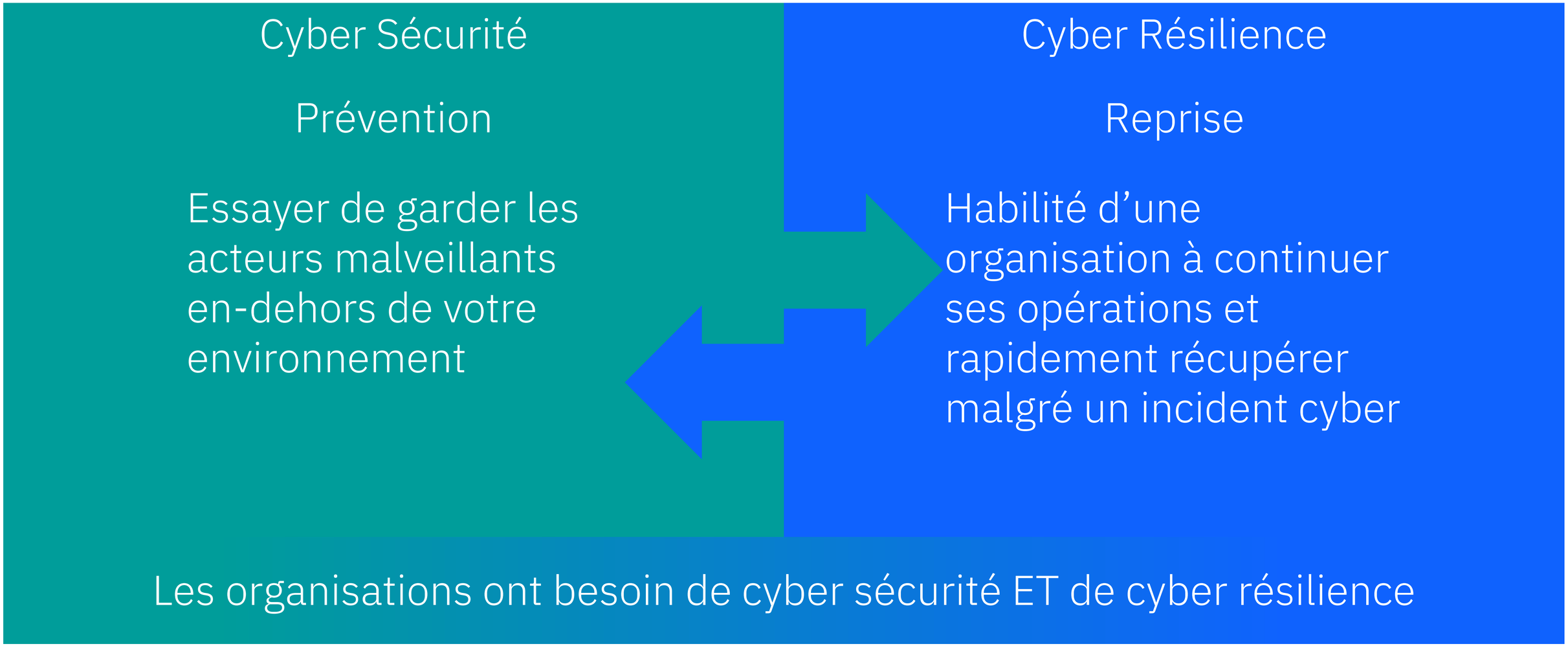
La survie de votre entreprise peut en dépendre

ANSSI :
https://cyber.gouv.fr/publications/les-regles-dor-de-la-sauvegarde
https://cyber.gouv.fr/publications/fondamentaux-sauvegarde-systemes-dinformation

NIS-2 :
https://cyber.gouv.fr/la-directive-nis-2
https://monespacenis2.cyber.gouv.fr/simulateur

DORA : Digital Operational Resilience Act
https://www.ibm.com/topics/digital-operational-resilience-act

Cyber Sécurité and Cyber Résilience



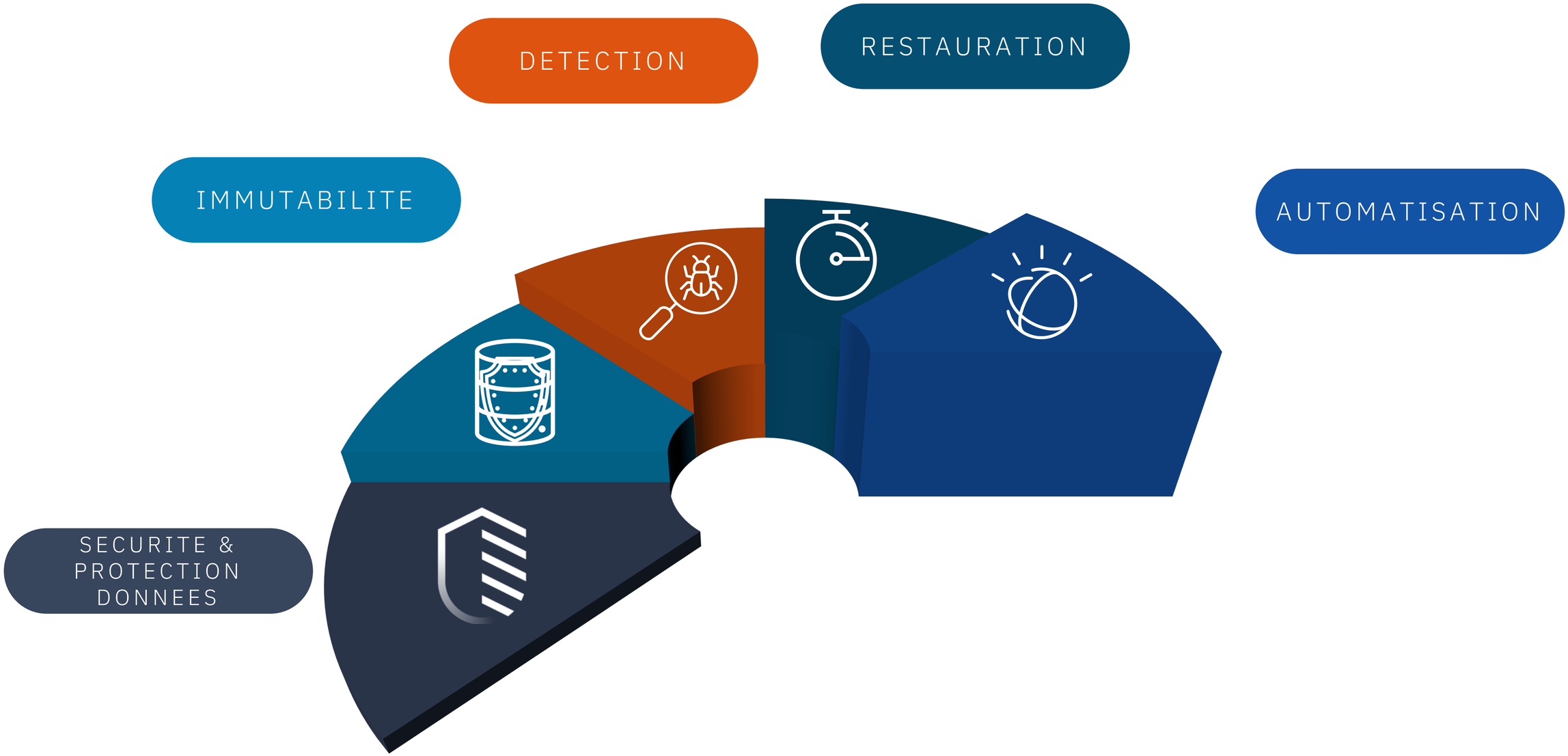
Changement de paradigme : PCA vs Cyber PCA

Categories	Traditional Recovery	Cyber Recovery
Nature de l'impact	Aléatoire Ex: catastrophe naturelle	Ciblé pensé pour faire un maximum de dégâts
Périmètre de l'impact	Local / Régional	Global Peut atteindre tous systèmes connectés
Infrastructure de Sauvegarde impactée ?	Pas spécifiquement	Une des premières cibles !
Point de restauration	Connu	Inconnu Besoin de restaurer la dernière copie "saine"
Remise en état	RPO/RTO	RPO/RTO + Restauration de données saines
Durée de la remise en état	Heures/Jours	Jours/Semaines
Probabilité d'occurrence	Faible	Elevé

Besoin de détection au plus tôt

Besoin de données saines & restaurable rapidement

Comment se preparer à la resilience des données ?



Comment se preparer à la resilience des données ?

SECURITE & PROTECTION DONNEES

01

Prévoir, prévenir et réagir
Intégration SOC
Protection contre les pannes d'infrastructure et les catastrophes naturelles

Comment se preparer à la resilience des données ?

IMMUTABILITE

02

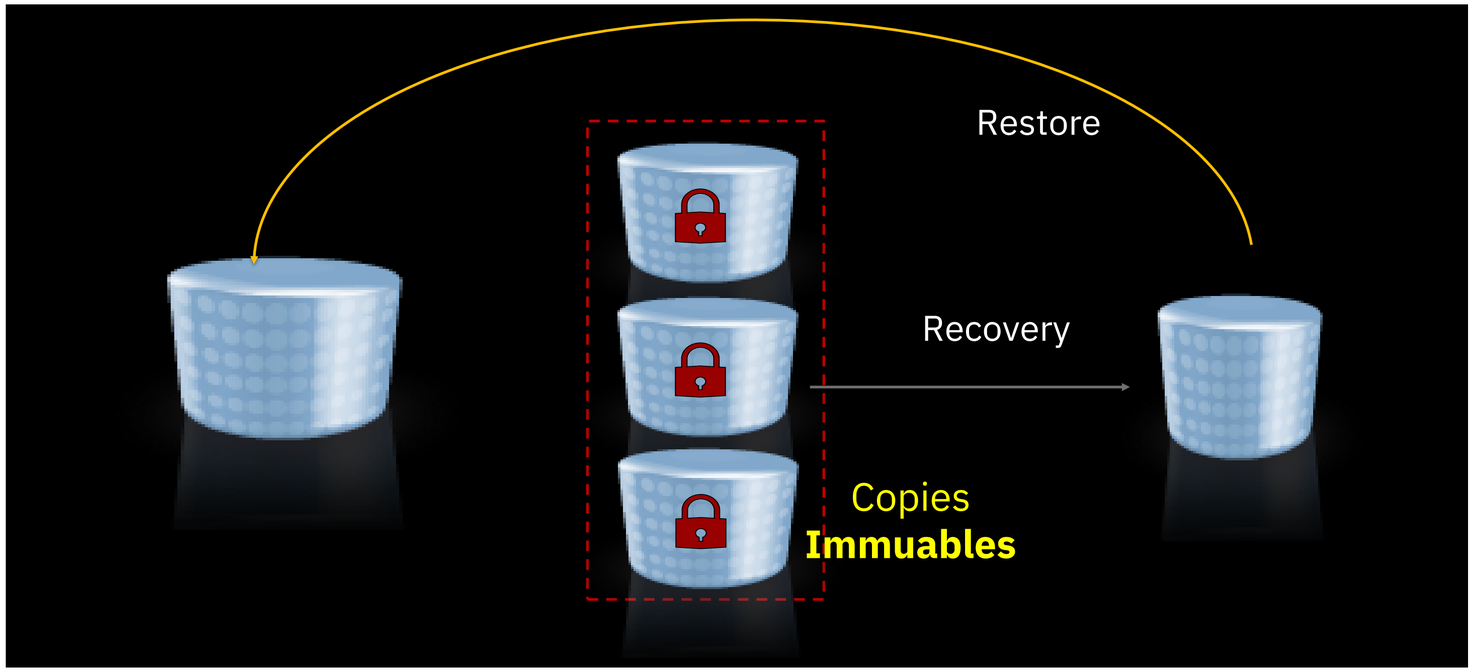
Points de données récupérables immuables, les données ne peuvent pas être supprimées

SECURITE & PROTECTION DONNEES

01

Prévoir, prévenir et réagir
Intégration SOC
Protection contre les pannes d'infrastructure et les catastrophes naturelles

Cyber Résilience des données avec Safeguarded Copy



Les copies sont stockées dans un **entrepôt sécurisé :**

Séparation logique avec les autres volumes
Restriction des accès

Les copies protégées ne peuvent **pas** être :

- ✓ Mappées à un host,
- ✓ Ecrites ou lues par une application,
- ✓ Supprimées par l'administrateur qui gère le stockage au quotidien.

Des **règles** sont définies pour des **groupes de volumes cohérents,** au niveau de chaque baie de stockage :

- ✓ **Fréquence** du programme de copie : en minutes, heures, jours, semaines, mois
- ✓ **Durée** de rétention définie en jour : maximum = 365 jours

Modification de la durée de rétention **non rétroactive**.

Comment se preparer à la resilience des données ?

DETECTION

03

Trouver les menaces actives
Détecter et prévenir les menaces dormantes

IMMUTABILITE

02

Points de données récupérables immuables, les données ne peuvent pas être supprimées

SECURITE & PROTECTION DONNEES

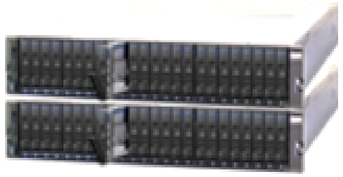
01

Prévoir, prévenir et réagir
Intégration SOC
Protection contre les pannes d'infrastructure et les catastrophes naturelles

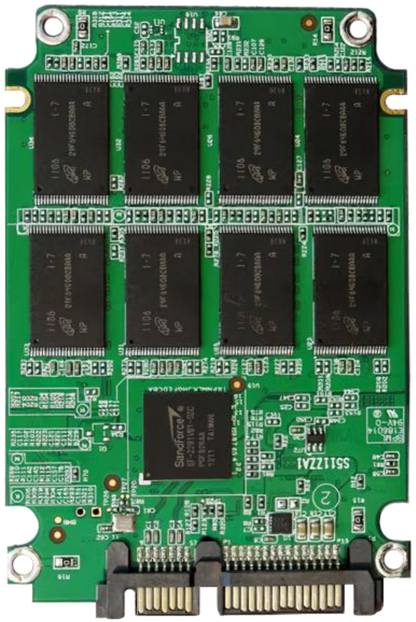
Les baies de disque IBM Flashsystem utilisent des Flash Core Modules

FlashSystem 5300

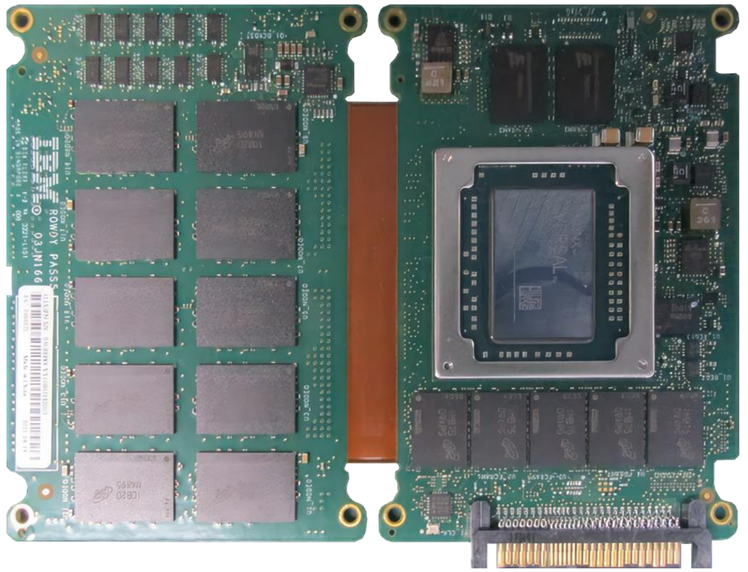
FlashSystem 7300



FlashSystem 9500



Un SSD « normal »



Un FlashCore Module

Capacités utiles (physiques) / effectives (max adressables) :

- **4.8TBu** / **22TBe** (ratio 4.5:1)
- **9.6TBu** / **29TBe** (ratio 3:1)
- **19.2TBu** / **58TBe** (ratio 3:1)
- **38.4TBu** / **116TBe** (ratio 3:1)

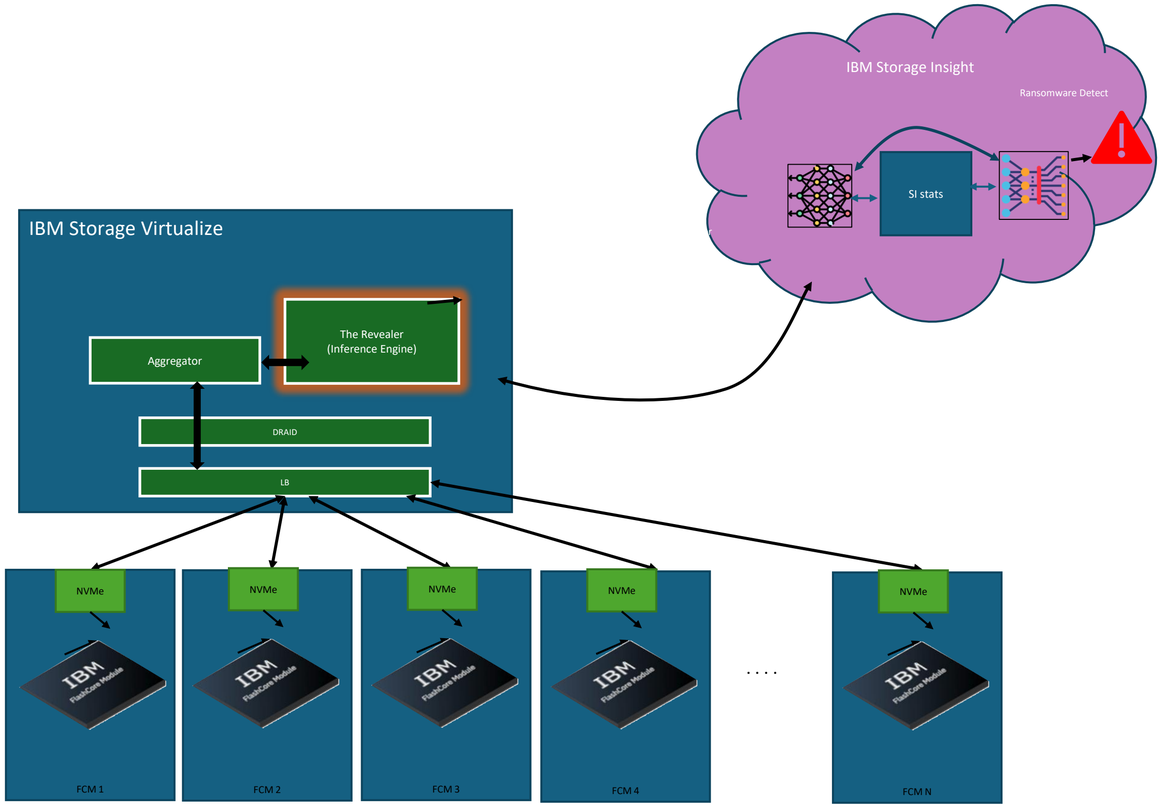
Note : valeurs en décimal (base 10)

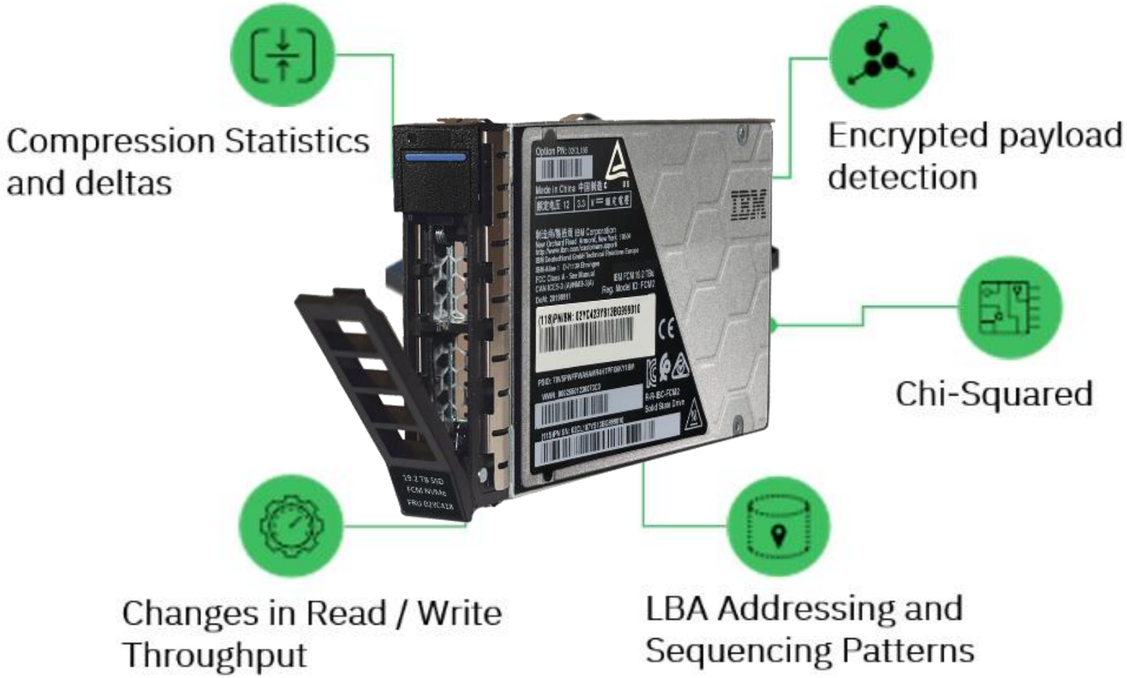
Endurance
Performance

Sécurité
Efficience

« Inline data corruption detection » avec IBM Storage **Virtualize**

Amélioration avec la génération FCM4





- Les mesures sont collectées à l'aide de FPGA installés dans les modules FlashCore Gen 4 (FCM4)
- Cette collecte est effectuée sur chaque FCM4 sans impact sur les performances.
- Les données sont transmises en temps réel à IBM Spectrum Virtualize.
- Les statistiques sont agrégées et transmises à Storage Insights PRO qui les analysera à l'aide de modèles d'apprentissage automatique (IA).
- Une alerte est transmise en cas de détection d'une anomalie ou d'une attaque RansomWare.

Comment se preparer à la resilience des données ?

DETECTION

03

Trouver les menaces actives
Détecter et prévenir les menaces dormantes

RESTAURATION

04

Récupération opérationnelle rapide en quelques secondes, minutes ou heures
Éviter le paiement de rançons

IMMUTABILITE

02

Points de données récupérables immuables, les données ne peuvent pas être supprimées

AUTOMATISATION

05

Simplification des opérations et possibilité de tester et de prouver la capacité de récupération
Intégration de la cybersécurité et de la cyber résilience

SECURITE & PROTECTION DONNEES

01

Prévoir, prévenir et réagir
Intégration SOC
Protection contre les pannes d'infrastructure et les catastrophes naturelles

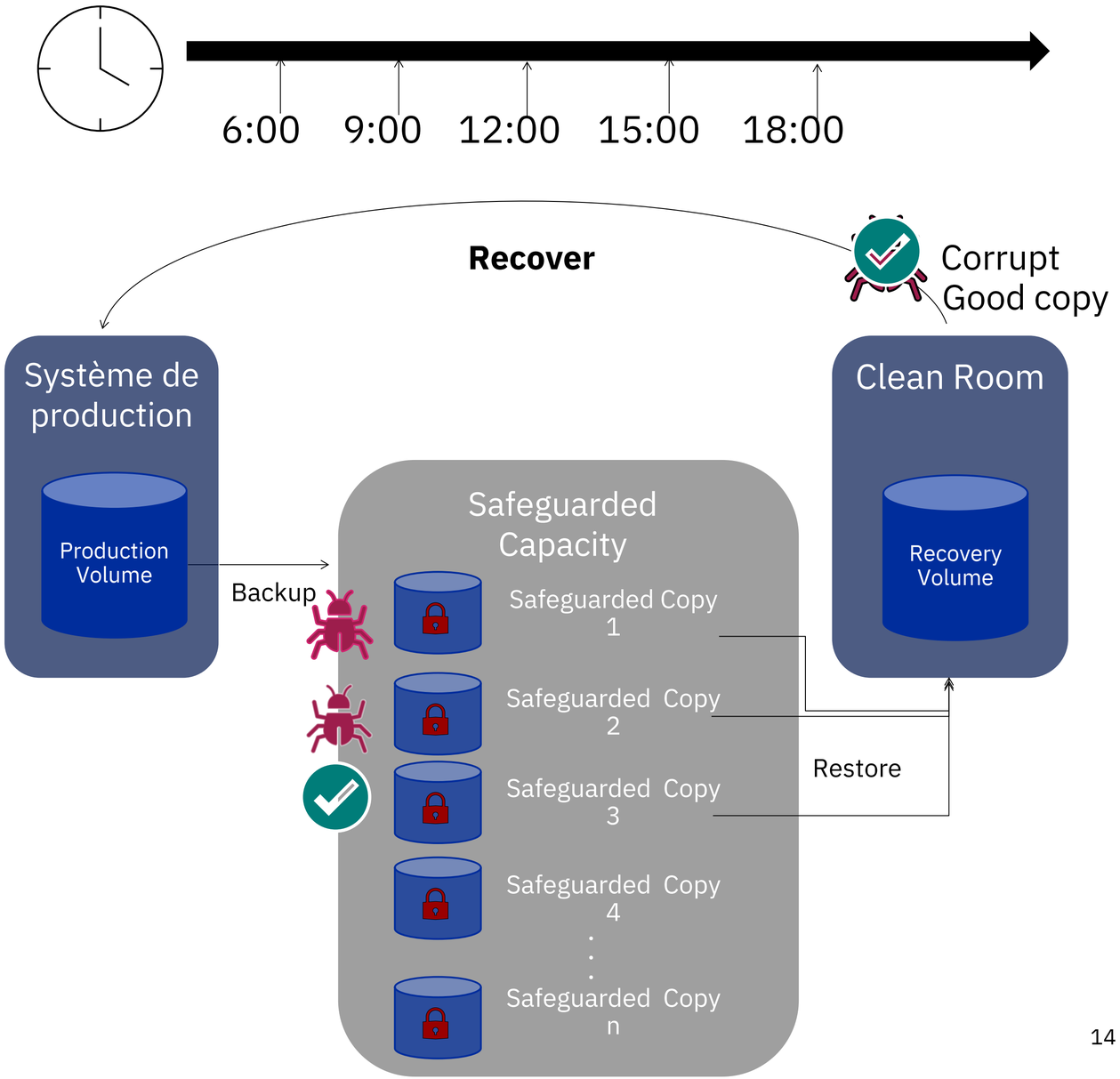
Cyber Résilience des données avec Safeguarded Copy

Les copies sont stockées dans un **entrepôt sécurisé :**
- Séparation logique avec les autres volumes
- Restriction des accès

Les copies protégées ne peuvent **pas** être :
- ✓ Mappées à un host,
- ✓ Ecrites ou lues par une application,
- ✓ Supprimées par l'administrateur qui gère le stockage au quotidien.

- Pas directement accessible à un serveur ou à une application
- Les données ne sont accessibles qu'après la récupération d'une copie protégée sur un volume de récupération distinct

Les volumes de récupération sont utilisés pour :
- Validation des données sur la baie
- Analyse Post incident
- Restauration des données de production



Pour aller plus loin:

Evaluation autonome

En 30 minutes, déterminez le degré de préparation de votre entreprise aux cyberattaques et assurez la conformité avec un maillage complexe de réglementations telles que DORA UE (Digital Operational Resilience Act), GLBA (Gramm-Leach-Bliley Act), FISMA (Federal Information Security Modernization Act), DPDP (Digital Personal Data Protection Act), NIS-2, ainsi que des cadres réglementaires similaires dans différentes régions du monde

IBM Cyber-resilience Assesment

Atelier immersif

En l’espace de quelques heures vous profiterez d’une évaluation personnalisée, des conseils et des démonstrations de nos experts, vous participerez à une session d’idéation et repartirez avec un plan d’action adapté à votre situation.

Atelier immersif

Merci pour votre attention

#pw2025

IBM

common
FRANCE