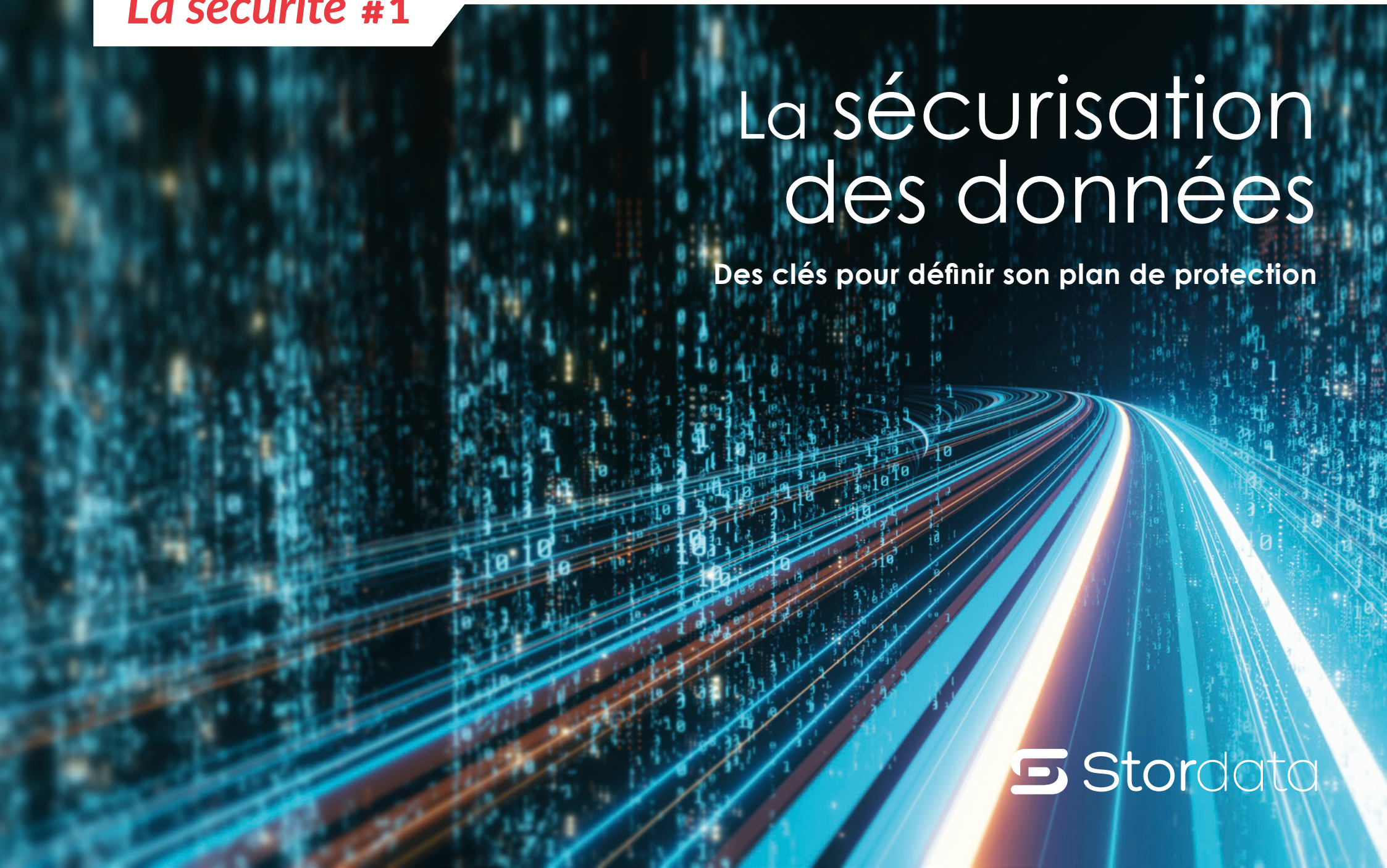
LES CAHIERS THÉMATIQUES
DE STORDATA

La sécurité #1



La sécurisation des données

Des clés pour définir son plan de protection

Stordata

éditorial

Joël Thouvenin
Directeur commercial

Entre idées reçues et système d'informations atomisé

dans le temps et l'espace, la sécurisation des données en gestion finit par relever du concept. En cause, une infrastructure construite principalement par projet, n'offrant qu'une vision parcellaire des données détenues, produites comme collectées. L'informatique de projet, c'est aussi prendre le risque de multiplier les possibles failles et les menaces. C'est enfin devoir composer avec un historique d'entreprise qu'on ne maîtrise pas forcément et un patrimoine informationnel protéiforme.

Ce cahier thématique n'a évidemment pas pour finalité de tirer à boulets rouges sur le principe même de projet informatique, qui a pour lui de savoir répondre à la complexité technologique de notre époque et aux besoins versatiles des équipes. Il faut en revanche garder en mémoire que la sécurité de la data ne peut pas se satisfaire de cette fragmentation.

Aussi est-il indispensable de couvrir ces éléments disparates d'une toile tissée serré, composée de solutions, d'outillages et de méthodes ayant tous pour vocation de protéger la donnée et par conséquent l'entreprise.

Deux mises en garde nous paraissent indispensables :
si la protection des données personnelles s'intègre pleinement dans la sécurisation des données de l'entreprise, au sens Data Protection by Design du RGPD, l'application du règlement européen reste insuffisante au regard du plan de protection.

Par ailleurs, les enjeux relevés dans ce cahier thématique sont d'ordre organisationnel, technique et technologique. Si nous ne l'abordons pas ici, il va de soi qu'en matière de sécurité, les efforts de sensibilisation et de prévention auprès des collaborateurs doivent être prodigués très régulièrement.

L'inventaire

L'objectif d'un plan de protection est d'une grande simplicité. Il s'agit de tout mettre en œuvre pour que les données d'entreprise ne soient ni corrompues ou modifiées, ni détruites, ni copiées, ni espionnées.

C'est un enjeu économique, de croissance et de compétitivité.

La Donnée a de la Valeur. Que ce soient des données commerciales et marketing, des données de recherche, des données organisationnelles, des données statistiques, des données sociétales ou bien des données de gestion, elles sont toutes porteuses de valeur, immédiate pour que l'entreprise puisse exercer son activité, ou dans un futur proche à lointain, quand il sera possible d'analyser les données collectées précédemment,

C'est un enjeu d'image et de confiance.

De plus en plus, les entreprises, les entreprises partenaires ou les entreprises sous-traitantes sont évaluées à l'aune de leur capacité à protéger leurs données et celles de leurs relations quand elles évoluent dans un même écosystème. C'est aussi l'engagement de l'entreprise dans la démarche de confiance numérique à destination des citoyens, des gouvernements, des utilisateurs ou des clients.

Si l'objectif à atteindre est entendu, sa mise en œuvre semble parfois requérir quelque talent d'architecte-funambule-visionnaire-medium. Il suffit pour s'en convaincre de dresser une liste, même sans exhaustivité, des menaces et des risques pesant sur la donnée d'entreprise : panne matérielle et logicielle, erreur humaine, malfaisance interne, attaque extérieure par déni de service, intrusion, accident et catastrophe naturelle, événements sociétaux… peuvent tous impacter la donnée.

> “C'est un enjeu économique, de croissance et de compétitivité.”

Quelle donnée et combien ?

Dès cette étape, le bât blesse. Et déjà la DSI se trouve démunie devant l'étendue de la problématique à couvrir. De l'entreprise multisites à la prolifération des solutions Cloud, l'état réel de la donnée détenue, à protéger, est inconnu.

L'étape n° 1 dans le cadre de l'élaboration d'un plan de protection est donc bien entendu d'établir l'inventaire de la donnée numérique à traiter et d'en évaluer la criticité. C'est une démarche fondamentale, qui exige du temps, de la minutie et une bonne dose de savoir-faire. C'est pourquoi les entreprises ont tendance à repousser l'échéance.

L'inventaire (suite)

L'inventaire de la donnée... à la loupe

Réaliser un inventaire, c'est pénétrer dans un historique d'entreprise largement méconnu et découvrir une organisation qui a évolué dans le temps. Savoir se poser les bonnes questions est un avantage dans ce type d'exercice.

> "Un historique d'entreprise largement méconnu."

1 Répertorier et classifier la donnée

- Inventorier de façon exhaustive toutes les données informatiques, quel que soit leur type, et où qu'elles soient stockées ou utilisées : datacenter, Cloud, site distant, filiale, partenaire, fournisseur, sous-traitant, etc.
- Comprendre et maîtriser l'usage de ces données, la nature du traitement appliqué et leur cycle de vie (durée de vie, rétention).
- Mesurer la criticité de ces données, y compris les données légales et l'impact sur l'entreprise en cas de blocage, de destruction, de corruption ou d'accès indésiré.
- Détailler les règles de protection appliquées, pourquoi et comment.

2 Collecter les règles et les contraintes métiers

- *Via* des interviews des propriétaires de données, par application.
- *Via* des interviews des entités internes : direction générale, directions vente/commerce, achats, légal, recherche et développement, industrialisation/production, marketing et communication, ressources humaines, sites, relations partenaires/fournisseurs, etc.

Des règles spécifiques, des contraintes règlementaires

Ce travail de maîtrise du parc informationnel ne sera pas complet tant que les règles spécifiques applicables à certains types de données n'auront pas été prises en compte. Et elles peuvent être nombreuses, en particulier quand elles relèvent du règlement. RGPD/GDPR (protection données personnelles), PCI-DSS (protection des transactions monétaires), ISO 27001 (norme de certification de la sécurisation d'un système d'information), HDS (protection des données de santé), autant de sigles pour autant de domaines d'activités et de types de données. La CNIL rappelle à ce titre qu'un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal sont tous des données personnelles, même publiques, tant qu'ils n'ont pas été anonymisés.

3 Rapprocher et compléter

- Croiser les données inventoriées avec les règles de protection à respecter
- Déterminer ce qui n'est pas couvert et en mesurer l'impact
- Créer les stratégies de protection manquantes, le cas échéant.

À cette étape, l'entreprise dispose maintenant d'une première photographie de son parc informationnel et des mesures de sécurité à mettre en place.
Ces dernières concernent la protection à appliquer à la donnée, sa durée de rétention et le chiffrement possible de cette donnée.
Comprenons-nous bien : **une faille dans la construction de ce filet de protection pourra totalement fragiliser l'ensemble.**

Concevoir l'outillage du plan de protection

Un outillage conçu pour la sécurisation des données en gestion est composé de logiciels, de matériels, de méthodes, de procédures et de tests. Ce canevas doit être appliqué à l'ensemble de l'écosystème de production de données de l'entreprise. Chaque application, chaque élément d'infrastructure, chaque organisation, chaque site physique ou non, présent à et venir, est concerné par le plan de protection et son outillage.

Abordons ce plan dans le détail, au regard des bonnes pratiques à respecter.

1 LOGICIELS

En administration, monitoring, supervision, logs et audits, l'outillage minimal doit alerter de tout dysfonctionnement d'un des composants, générateur potentiel de dégradation des données ou de dégradation du service rendu.

L'habitude doit être prise de tracer à la fois tous les événements qui concernent le système d'information, toutes les actions réalisées par l'équipe d'exploitation et d'administration du système d'information et toutes les actions réalisées par les utilisateurs sur les fichiers ou les bases de données.

La possibilité de rejouer ces actions permet de détecter les erreurs, les malveillances, les activités et comportements anormaux.

2 MATÉRIELS

— Le stockage primaire de la donnée en production

Le SAN pour les données structurées
Architecture de stockage en réseau la plus courante pour les applications stratégiques qui demandent un débit élevé et une faible latence, le SAN est conçu pour supprimer les points de défaillance uniques, ce qui les rend hautement disponibles et résilients.

Le NAS pour les données non structurées fichiers
Basés sur Ethernet, les NAS se démarquent par leur simplicité d'utilisation et de gestion, leur évolutivité et un meilleur coût total de possession (TCO).

Le stockage objet S3 pour les données non structurées multi-type
Le stockage S3 est la meilleure façon de gérer d'importants volumes de données non structurées.

Il simplifie les déploiements sur site et assure le déplacement fluide des données dans un contexte MultiCloud.

En termes de bonnes pratiques, optez pour des baies de stockage à double contrôleur, avec gestion de la redondance des médias de stockage, basée sur du Raid ou de l'Erasure Coding. Elle doivent embarquer l'utilisation des snapshots et la mise en place de clusters permettant la **continuité d'activité.**

— Les serveurs et le réseau

Les serveurs, les postes de travail et les OS : les consommateurs de données
C'est au niveau des serveurs que s'exécutent les traitements des données. C'est donc lors du transport des données, depuis le lieu de stockage (baie de disque ou Cloud) jusqu'aux serveurs, que des logiciels malveillants peuvent s'installer. Le cœur du système d'exploitation devient alors un point de vue privilégié pour corrompre, chiffrer et supprimer des données. Des boucliers de protection à différents points du système et jusque dans les serveurs doivent être intégrés. C'est également vrai pour les postes de travail et les applications bureautiques.

Le réseau : le transport
Parce que le réseau transporte les flux de données, il y a lieu de surveiller en permanence qui parle à qui et pourquoi. L'observation continue de la nature des flux et des canaux utilisés permet d'identifier assez rapidement des comportements inappropriés et suspects. Ils déclencheront, de façon automatique ou pas, l'action des outils de sécurisation tels des alertes, une coupure du trafic ou le détour, la fermeture de ports, la prise de traces pour analyse et le déclenchement de contre-mesures, le cas échéant.

L'outillage (suite)

3 MÉTHODES, PROCÉDURES, TESTS ET MISE EN ŒUVRE

Un plan de protection… se rédige. Cela va sans dire mais seule une rédaction exhaustive permet de clarifier le schéma, en toute transparence.

C'est avec une approche méthodique de l'inventaire et de la collecte des règles et des contraintes que l'entreprise peut définir l'ensemble des procédures de sécurité à mettre en œuvre, du chiffrement à l'authentification des utilisateurs, hommes, machines et réseau.

Le traçage systématique des actions et des résultats reste de mise pour mieux comprendre les comportements du sytème et des utilisateurs.

Enfin, la vérification régulière de la tenue des objectifs passe aussi par des tests des procédures de bascule, d'escalade et de reprise à la récurrence, afin de s'assurer de l'efficacité du plan.

Il est nécessaire d'introduire au protocole un rythme de contrôle correspondant à l'activité du SI. Un système qui n'évolue que peu se satisfera d'une vérification de l'efficacité du plan une à deux fois par an, quand d'autres exigeront des contrôles mensuels.

4 LA SAUVEGARDE

La brique de base

Incontournable, seule la sauvegarde est en mesure de remédier à la perte définitive des données, en autorisant une restauration à un moment précis du cycle de vie du patrimoine informationnel. Ni les snapshots, ni les réplications n'offrent ce degré de complétude et de précision.

Pour une sauvegarde conforme et efficiente, il est recommandé de **respecter la méthode fiable des 3-2-1 :**

- Maintenir **3 copies des données** (les données originales stockées sur le stockage d'entreprise et deux sauvegardes) ;
- Sauvegarder les données sur **2 types de supports** différents : le choix est vaste entre bandes magnétiques, stockage NAS secondaire, stockage externe sur un autre site ou dans le Cloud, stockage objet S3, etc ;
- Conserver **1 copie de sauvegarde** hors-site (hors du datacenter, voire de l'entreprise).

PORTER UNE ATTENTION PARTICULIÈRE AU CLOUD

Le Cloud, public, en particulier, reste un sujet d'inquiétude auprès des entreprises traditionnelles. Alors que les Startups s'y lancent tête baissée puisque c'est leur modèle et que les grandes entreprises l'adoptent sans toujours en mesurer tous les risques, les ETI et PME évoquent encore beaucoup de freins. Le Cloud est vraiment intéressant à plus d'un titre et s'en priver est dommageable. C'est pourtant compréhensible.

La nébuleuse Cloud renforce le sentiment d'insécurité et de non maîtrise du risque. C'est à la fois vrai et faux. C'est vrai parce que les Cloud Providers, malgré un taux de perte de données négligeable, ne s'engagent jamais contractuellement sur la sécurité. La sauvegarde du patrimoine informationnel reste et restera de la responsabilité des entreprises. C'est faux parce que les entreprises peuvent remédier à l'incertitude en créant leur plan de protection. Bien informées en volume, comme en nature de leurs datas et conscientes des règles, mesures et procédures à appliquer, elles peuvent éprouver le Cloud avec l'assurance d'une entreprise avertie.

Le choix Stordata

Les solutions de stockage primaire NetApp

Désigné Leader 2019 pour le stockage primaire par le Gartner, NetApp garantit la protection des données stockées sur ses baies par :

la redondance de tous les éléments ;

la technologie RAID embarquée de haut niveau, ou Erasure Coding, réduisant notablement le risque de perte de données, et facilitant la reconstruction des médias de stockage ;

la multiplication des prises de snapshots sans dégradation des performances ni consommation excessive de place ;

la réplication intégrée, en miroir, ou en historisation, vers d'autres baies, sur d'autres sites.

— Baies de stockage SAN et NAS full Flash ou hybrides : baies FASXXXX, baies AFFXXXX. Ces baies, Scale-Up et Scale-Out, offrent différents niveaux de performance et de capacité. Elles embarquent simultanément plusieurs protocoles d'accès aux données, ce qui leur permet d'être multiusage.

— Baies de stockage S3 (objets) : solutions StorageGrid de différentes capacités et qui sont Scale-Out.

Les solutions de sauvegarde et de restauration CommVault

CommVault propose un système de sauvegarde et de restauration à la fois simple, économique et moderne. Commvault est une solution unique et efficace pour la protection des données, quels que soient leur nature et leur emplacement. CommVault est noté parmi les leaders de la protection des données par le Gartner, et ce, depuis 9 ans maintenant.

La solution CommVault est 3 Tier :

— CommServe : chef d'orchestre de la solution, gère les stratégies de sauvegarde et l'orchestration, fonction haute disponibilité.

— MediaAgent : gère la collecte des flux de sauvegarde et le stockage sur les médias de sauvegarde (disques, S3, bandes, site distant, Cloud), et porte le référentiel de déduplication, fonction haute disponibilité.

— Agents applicatifs : serveurs NAS, postes clients, bases de données, virtualisation, messagerie, applications SaaS, gestion des snapshots, clones et réplication.

Les solutions serveurs et réseau Cisco

Cisco a développé de nouvelles technologies qui agissent de concert pour optimiser la détection des menaces grâce à une visibilité sur l'ensemble des utilisateurs, des équipements, des réseaux, des applications, des workloads et des processus.

La microsegmentation et les listes blanches d'applications empêche les hackers de se déplacer de manière latérale (est-ouest) sur le réseau. Les capteurs de menace multicouche détecte et identifie les failles, les bloquent et les traitent rapidement pour empêcher le vol de données et les interruptions.

Cisco UCS :

— Jusqu'à 20 châssis de 8 lames maximum, soit 160 lames : gestion centralisée de l'ensemble, administration et supervision du hardware et du firmware.

— Notion unique de Service Profil : paramétrage total des lames et gestion des mises à jour.

— Ports virtualisés sur les lames : fournit et associe ports virtuels et machine virtuelles.

— Éléments actifs réseau centralisés : Fabric Interconnect, hauts débits et unification des ports IP et FC.

En partenariat avec :

Depuis sa création, Stordata protège la donnée, où qu'elle soit. Son entité Conseil aide les entreprises à mieux cerner les périls qui menacent leurs données et à établir ou parfaire leurs stratégies de protection.

Son expertise data, rare sur le marché, profite aux entreprises qui entendent se doter des solutions matérielles, logicielles et méthodologiques les plus adaptées aux contrôles et au renforcement de la sécurité des données numériques, On Premise comme dans le Cloud.

Les équipes Stordata et les moyens logistiques à leur disposition garantissent le maintien en conditions opérationnelles et le suivi des infrastructures, prérequis incontournable de la protection des données.

Stordata est un partenaire privilégié des constructeurs et éditeurs majeurs d'infrastructures informatiques.

Agence Île-de-France & Nord
28, rue Saint-Honoré - 78000 Versailles
Tél. : +33 1 30 21 42 42

Agence Sud-Est
28, rue Louis Guérin - 69100 Villeurbanne
Tél. : + 33 4 78 48 09 47

Agence Sud-Ouest
82, rue Maubec - 31300 Toulouse
Tél. : + 33 5 34 50 49 00

Agence Sud-Ouest Méditérannée
Tél. : + 33 5 34 50 49 00

Agence Ouest
34, quai Magellan - 44000 Nantes
Tél : +33 2 28 08 09 93

Agence Est
9, rue Icare - 67960 Entzheim
Tél. : +33 3 88 76 47 64

www.stordata.fr

Stordata
vos données, notre engagement