Acronis

LIVRE BLANC

Gestion centralisée ou distribuée de la cyberprotection pour les entreprises multisites

Comment la gestion distribuée de la cybersécurité et de la protection des données peut renforcer la cyber-résilience de votre entreprise

Les entreprises de toutes tailles peinent à protéger la disponibilité de leurs systèmes et l'intégrité de leurs données contre une multitude de menaces, des cyberattaques exploitant l'intelligence artificielle aux défaillances matérielles, en passant par les problèmes logiciels et les erreurs humaines. Si de nombreuses entreprises choisissent de centraliser leurs opérations informatiques et leur gestion de la cybersécurité, dans certains cas déléguer une partie de l'effort à des équipes informatiques et de cybersécurité sur des sites distants peut améliorer la cyber-résilience.

Ce livre blanc examine les scénarios dans lesquels une entreprise peut obtenir une disponibilité plus élevée, prévenir plus efficacement les pertes de données et réduire les coûts de gestion et de sécurisation de l'infrastructure informatique et des données en déléguant une partie du contrôle à ses sites régionaux et distants. Il évalue le pour et le contre de cette approche et examine les moyens par lesquels les entreprises peuvent atteindre leurs objectifs de conformité et de gouvernance sans une gestion entièrement centralisée de la cybersécurité et des opérations informatiques.

De nombreuses entreprises sont distribuées

Près d'un quart des entreprises américaines opèrent à partir de plusieurs sites. Bien que l'Union européenne (UE) ne rende pas spécifiquement compte des entreprises en fonction du nombre d'implantations, la prévalence des entreprises multi-implantations dans les secteurs du commerce de détail, de l'hôtellerie, des services médicaux, des services financiers et d'autres encore suggère que ces entreprises constituent une part importante de l'économie de l'UE. Les grandes entreprises sont encore plus susceptibles d'avoir plusieurs sites, notamment des bureaux régionaux, des usines de fabrication, des entrepôts et des centres de distribution.

Les entreprises qui ont recours aux fusions et acquisitions pour se développer dans leur secteur, d'autres secteurs d'activité et d'autres régions géographiques sont également susceptibles d'avoir un grand nombre de sites physiquement éloignés des équipes informatiques et de cybersécurité centralisées.

Exemples d'entreprises distribuées

Le secteur de la vente au détail est un exemple flagrant d'activité hautement distribuée. L'enseigne typique comprend des sièges sociaux mondiaux et régionaux, des entrepôts de distribution et des magasins physiques. Mais de nombreuses entreprises extérieures au secteur de la vente au détail sont également organisées physiquement comme des entreprises de vente au détail dans la mesure où elles disposent de nombreux magasins ou bureaux répartis géographiquement, comme dans les exemples suivants :

- Les soins de santé, comme les services d'optique, les cabinets de médecins de soins primaires, les cliniques dentaires, les centres de soins d'urgence sans rendez-vous, les pharmacies et les cliniques vétérinaires.
- Les services bancaires aux particuliers, d'assurance et financiers, disposant de nombreuses succursales.

- Les entreprises d'expédition/réception, de transport et de logistique avec de nombreux centres de distribution et un grand nombre de points d'expédition et de services aux entreprises.
- Les entreprises de jeux avec plusieurs sites, casinos, salles de bingo, salles de paris hors piste, salles de pachinko et installations similaires.
- Les services routiers, à savoir fourniture de carburant automobile et recharge de véhicules électriques, couplés avec commerces de proximité et restauration rapide.
- Les entreprises organisées sous une architecture fédérée, dans laquelle une équipe centralisée peut superviser les opérations informatiques, la cybersécurité et la conformité à l'échelle de l'entreprise ; cependant, les installations individuelles ont leurs propres budgets, leurs propres responsabilités de recrutement et leur propre autonomie locale pour gérer l'infrastructure informatique de l'unité commerciale.

La gestion centralisée de l'informatique et de la cybersécurité peut être difficile

Une entreprise hautement distribuée possède typiquement un mélange hétérogène de matériel, de systèmes de virtualisation et d'exploitation, ainsi que d'applications telles que des systèmes d'inventaire ou de point de vente provenant de différents fournisseurs de technologie. La combinaison de l'infrastructure technologique et des niveaux de révision des logiciels peut varier considérablement d'un endroit à l'autre. La nécessité de préserver les applications héritées, les logiciels sur mesure et les ordinateurs utilisés pour contrôler la stabilité des environnements technologiques opérationnels peut rendre difficile la normalisation informatique dans l'ensemble de l'entreprise, conduisant à une prolifération des outils informatiques et de cybersécurité.

Les collaborateurs centralisés ne sont pas nécessairement experts de tous les outils présents pour protéger, gérer et sécuriser les applications et les données dans l'ensemble de l'organisation. Parallèlement, la complexité et la diversité des applications ainsi que des outils pour les gérer et les sécuriser ne cessent de croître.

Les emplacements distants avec des exigences de sécurité élevées, par exemple les environnements d'usine, peuvent devoir être isolés physiquement du réseau de l'entreprise et de l'Internet public afin de minimiser l'exposition aux cybermenaces. Cela limite la capacité du personnel centralisé à diagnostiquer et à résoudre les problèmes par la gestion de bureau à distance et d'autres outils en réseau, nécessitant potentiellement des déplacements physiques sur des sites distants pour résoudre les problèmes.

Cela peut s'avérer extrêmement coûteux et chronophage pour les endroits difficiles d'accès, par exemple les raffineries dans le désert, les plates-formes pétrolières offshore, les installations minières et d'autres sites éloignés des centres de transport aérien et terrestre commerciaux.

La gestion de la protection et de la sécurité des données dans une grande entreprise à site unique est moins complexe et prend moins de temps que la protection du même nombre d'applications et de terminaux dispersés sur plusieurs sites éloignés géographiquement. Si les données de sauvegarde ne sont pas séparées par emplacement, une restauration ponctuelle peut avoir un impact négatif sur les performances de tous les emplacements.

La connectivité des réseaux étendus et les vitesses des réseaux dans les emplacements distants peuvent varier considérablement selon la géographie, ce qui rend les temps de restauration à la fois imprévisibles et potentiellement trop longs pour respecter les normes de temps de récupération.

La gestion des sites distants peut nécessiter que le personnel informatique se connecte aux référentiels de données locaux et aux consoles de gestion de la sécurité séparément et à plusieurs reprises, ce qui peut être inefficace, sujet aux erreurs et lent. De nombreux outils traditionnels de sauvegarde, de reprise après sinistre et de sécurité existent pour des environnements d'application particuliers, ce qui rend difficile la standardisation des outils communs à l'ensemble de l'organisation.

La prolifération des outils d'exploitation et de sécurité informatiques coûte cher et fait grimper les coûts d'intégration et de formation du personnel de support, un problème croissant dans un monde où les coûts de personnel informatique et de cybersécurité restent obstinément élevés.

La conformité peut être difficile à gérer de manière centralisée

Les exigences de conformité varient également considérablement d'un pays à l'autre et, dans certains cas, selon l'État, la province et la municipalité. Par exemple, les entreprises faisant des affaires aux États-Unis peuvent être tenues de se conformer aux réglementations de confidentialité appliquées par le gouvernement fédéral, plusieurs États américains et même certaines villes.

Le respect de la souveraineté des données constitue également un défi croissant. Ces réglementations limitent les emplacements physiques, les centres de données et les réseaux où les données sensibles peuvent être stockées ou autorisées à transiter sur un réseau, sous prétexte que certains gouvernements nationaux violeront la confidentialité des données par une surveillance secrète. Le respect de ces exigences dans une entreprise largement distribuée est complexe à gérer et peut nuire aux performances des applications.

Savoir quelles données doivent être protégées sur quels terminaux, quels éléments de l'infrastructure informatique sont certifiés conformes à diverses normes de sécurité et réglementaires et quels collaborateurs sont autorisés à accéder à ces données peut générer de la confusion et des écarts de conformité coûteux dans toute l'organisation. Ces complexités surviennent dans un contexte où les budgets sont le plus souvent stables ou en baisse pour le personnel informatique et de cybersécurité, tandis que le nombre d'applications et le volume de données à gérer et protéger augmentent.

Les autorités réglementaires prévoient désormais des sanctions importantes pour encourager le respect des règles. Par exemple, l'UE impose régulièrement des amendes allant de 2 à 4 % du chiffre d'affaires annuel d'une entreprise en cas de manquement répété à la protection des données des consommateurs.

Cela peut présenter des problèmes importants pour certaines entreprises distribuées et multisites, notamment des défis liés à la mise en réseau et des difficultés à trouver un hébergement tiers conforme et sécurisé pour les applications et le stockage avec des fonctionnalités adaptées, de contrôle d'accès sécurisé et de stockage immuable notamment.

Acronis répond aux défis de la gestion et de la sécurisation des entreprises distribuées

Acronis Cyber Protect assure la fourniture de solutions de protection et de sécurité des données dans des environnements distribués en intégrant la gestion à distance, la sauvegarde, la reprise après sinistre et la sécurité dans une plate-forme unique. Des emplacements distants peuvent être configurés et gérés séparément par le personnel local à partir d'une console dédiée, installée sur site ou hébergée dans le cloud.

Les plans de protection des données et les calendriers de sauvegarde pour chaque emplacement peuvent être personnalisés, ou standardisés et déployés sur plusieurs emplacements. La protection et la sécurité des données de toutes les ressources locales peuvent être gérées à partir d'une seule console sans avoir à basculer entre les écrans ou les applications.

Toutes les fonctions de sécurité et de protection des données sont gérées par un agent unique installé sur chaque terminal. Le chiffrement complet des données et le transfert sécurisé via la sécurité de la couche de transport (TLS) garantissent la sécurité des données pendant le transit. De plus, la compression des données, la déduplication et la limitation de la bande passante sont gérées automatiquement pour optimiser le trafic avec un débit raisonnable et un impact minimal sur les opérations actives.

Pendant ce temps, le personnel informatique et de cybersécurité du siège social peut surveiller les sites distants à partir d'un tableau de bord centralisé pour évaluer le risque global, l'état de protection des données et la conformité dans l'ensemble de l'organisation, comme le montre la figure 1.

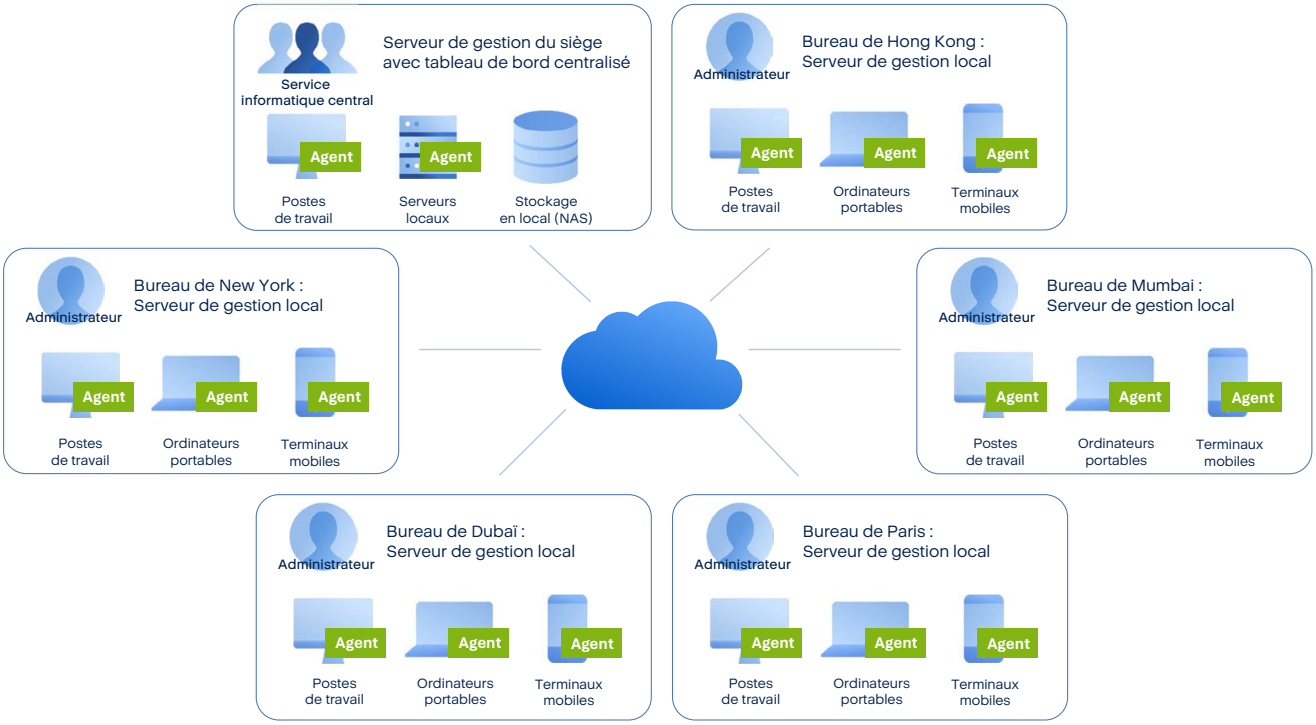

Figure 1. Gestion multisite de la cybersécurité et des opérations informatiques avec contrôle local et surveillance centralisée

Avantages d'Acronis Cyber Protect

- Isole le stockage et la sécurité des données par emplacement.
- Réduit ou élimine les problèmes de compatibilité de la cybersécurité liés au matériel, aux logiciels et à la virtualisation.
- Résout les problèmes de souveraineté des données et facilite la conformité réglementaire.
- Supprime les problèmes liés aux différentes configurations et connexions réseau.
- Réduit ou élimine la nécessité de plusieurs environnements d'hébergement pour la protection des données.
- Permet de bénéficier de coûts cohérents et prévisibles sur tous les sites physiques.
- Simplifie le déploiement du stockage géoredondant.
- Permet une surveillance centralisée pour l'évaluation des cyber-risques à l'échelle de l'entreprise, l'état de protection des données et l'état de conformité.

Les solutions Acronis sont basées sur des images et des fichiers, via un agent multiplate-forme compatible avec la plupart des environnements informatiques utilisés dans les entreprises et la fabrication industrielle. Acronis protège également les plates-formes cloud de messagerie et de collaboration, par exemple Microsoft 365 et Google Workspace, ainsi que celles sur site, comme Microsoft Exchange.

Environnements pris en charge par Acronis

VMWare vSphere 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

Microsoft Hyper-V Server 2022, 2019, 2016, 2012/2012 R2, 2008/2008 R2

Citrix XenServer / Citrix Hypervisor 8.2 – 4.1.5

Linux KVM 8 – 7.6

Scale Computing HyperCore 8.8, 8.9, 9.0

Red Hat Enterprise Virtualization (RHEV) 3.6 – 2.2

Red Hat Virtualization (RHV) 4.0, 4.1

Red Hat Virtualization (oVirt) 4.2, 4.3, 4.4

Virtuozzo 7.0.14 – 6.0.1.0

Virtuozzo Infrastructure Platform 3.5

Oracle Linux Virtualization Manager (Oracle LVM) 4.3

Nutanix Acropolis Hypervisor (AHV) 20160925x – 20180425x

Virtuozzo Hyper Server 7.5

Virtuozzo Hybrid Infrastructure 4.3 – 3.5

Souveraineté et conformité des données pour les environnements distribués

Acronis exploite un réseau mondial de centres de données indépendants implantés partout dans le monde industrialisé. Les entreprises distribuées disposent ainsi d'une grande flexibilité de stockage sécurisé de leurs données, de performances de protection supérieures et de garanties de conformité en matière de souveraineté des données. Les sites distants individuels peuvent gérer la protection et la sécurité de leurs données par emplacement et conserver les données de leurs serveurs, terminaux, e-mails et d'applications de collaboration au sein de chaque pays lorsque c'est nécessaire à des fins de conformité.

L'intégration de la gestion des terminaux, de la protection des données et de la cybersécurité dans une seule plate-forme avec des consoles locales peut réduire les coûts d'opérations informatiques jusqu'à 60 %. Les entreprises réaliseront des économies supplémentaires grâce à la réduction des frais généraux liés à la formation du personnel et à la maintenance de multiples outils informatiques et de cybersécurité, ainsi qu'aux coûts de stockage et de transit de données tierces selon les obligations géographiques de conformité.

Les entreprises distribuées et multisites sont confrontées à des défis uniques en matière de déploiement et de maintenance de solutions de sécurité, de sauvegarde et de reprise après sinistre. Il s'agit notamment de gérer des solutions sur plusieurs sites, de naviguer et de maintenir des services à travers d'innombrables combinaisons de technologies matérielles et logicielles, de garantir la conformité aux réglementations de confidentialité et de souveraineté des données, et de fournir ces services dans un environnement aux ressources et au budget limités. Ces défis sont amplifiés pour les entreprises à dimension internationale.

Avantages de la gestion multisite

Consoles locales pour sites distants avec agents indépendants

- Console unique sur site ou hébergée dans le cloud pour chaque emplacement, service, unité commerciale ou marque.
- Limitation de la bande passante, compression et déduplication des données, toujours incrémentielles, avec transport de disque physique en option.
- Agent à la source avec chiffrement des données et transfert sécurisé via TLS ; pas besoin d'utiliser le réseau d'entreprise.

Tableau de bord centralisé au siège social pour surveiller toutes les consoles Acronis des sites distants

- Surveillez toutes les consoles Acronis des sites distants collectivement ou individuellement.
- Obtenez une vue consolidée de tous les terminaux distants, des alertes et des activités.
- Téléchargez des données à partir des widgets de la console Acronis du site distant.
- Accédez à des terminaux spécifiques sur n'importe quelle console Acronis distante.

Consolidation de plusieurs outils

Un seul agent et console pour gérer :

- Sauvegarde et reprise après sinistre.
- Sécurité des e-mails et des terminaux avec détection et réponse sur les terminaux (EDR).
- Correctifs, inventaire, assistance à distance, scripting et surveillance.

Ressources protégées

- Serveur, VM, VM cloud et postes de travail.
- Ordinateurs de bureau, ordinateurs portables et terminaux mobiles.
- Windows (depuis 2003 / XP), Mac, Linux.
- Microsoft 365 et Google Workspace.

Amélioration de la conformité locale

Plus de 50 centres de données mondiaux.

- 11 centres de données européens.
- 2 centres de données allemands.

Données chiffrées à la source via AES-265 avec des mots de passe détenus par l'entreprise.

Données chiffrées en transit via SSL / TLS.

Stockage immuable.

Authentification multifactorielle.

Accès basé sur les rôles.

Certifications de conformité mondiales.

Réduction des coûts et de la complexité liée aux fournisseurs

La consolidation sur Acronis peut faire économiser jusqu'à 60 % par rapport à la coexistence d'outils de plusieurs fournisseurs.

Atténuation des limitations de ressources

Console unique, gestion unique.

L'IA et l'apprentissage automatique (ML) pour aider dans les tâches quotidiennes.

- Surveillance des terminaux et correctifs automatisés.
- Enquête et résolution des incidents de sécurité optimisées par l'IA.
- Sauvegarde automatisée et tests de reprise après sinistre.
- Bibliothèque de scripts automatisés pour les tâches de maintenance.

Pistes de réflexion finales

Alors que la plupart des entreprises gèrent les opérations informatiques et la cybersécurité avec des équipes centralisées, certaines constateront que la délégation de certaines fonctions de gestion informatique et de sécurité à des équipes régionales et/ou distantes peut améliorer la cyber-résilience.

La distribution de la gestion des défenses d'une entreprise contre les cybermenaces et autres causes de temps d'arrêt et de perte de données, ainsi que sa capacité à restaurer rapidement les données et la disponibilité en cas d'incidents, peuvent réduire les risques commerciaux plus efficacement que le contrôle centralisé.

Dans ces scénarios multisites gérés localement, les entreprises doivent équiper leurs équipes régionales et distantes d'outils qui intègrent nativement la cybersécurité, la protection des données et la gestion des terminaux. L'ajout d'une surveillance centralisée des consoles utilisées au niveau régional et sur site distant peut aider les équipes informatiques et de cybersécurité du siège social à auditer et à appliquer les normes de gouvernance et de conformité informatiques de l'entreprise.

Cette surveillance centralisée couplée à la gestion distribuée des opérations informatiques et de la cybersécurité peut rationaliser la réactivité du support (en particulier pour les installations isolées et très éloignées), améliorer la conformité aux réglementations régionales en matière de sécurité et d'informatique et réduire le risque commercial global.

Pour en savoir plus

Pour un entretien gratuit avec un ingénieur en solutions Acronis afin de déterminer si une topologie de contrôle distribuée et surveillée de manière centralisée pour la cybersécurité et la gestion des opérations informatiques est judicieuse pour votre entreprise, contactez Acronis ici.

Bénéficiez gratuitement de 30 jours d'essai d'Acronis Cyber Protect ici.

À propos d'Acronis

Acronis est une entreprise mondiale de cyberprotection qui propose des solutions intégrées de cybersécurité, de protection des données et de gestion des terminaux pour les fournisseurs de services managés (MSP), les petites et moyennes entreprises (PME) et les services informatiques des entreprises. Les solutions Acronis sont conçues pour identifier les cybermenaces modernes, les prévenir, les détecter et agir en conséquence, et pour corriger et restaurer les systèmes, avec un temps d'arrêt minimal, de façon à garantir l'intégrité des données et la continuité de l'activité. Acronis offre la solution de sécurité la plus complète du marché pour les MSP, grâce à sa capacité unique à répondre aux besoins des environnements informatiques variés et distribués.

Société suisse fondée à Singapour en 2003, Acronis est implantée dans 45 pays. La solution Acronis Cyber Protect Cloud est disponible dans 26 langues et dans plus de 150 pays. Elle est utilisée par plus de 20 000 fournisseurs de services pour protéger plus de 750 000 entreprises. Pour en savoir plus, rendez-vous sur www.acronis.com.

Acronis

Pour en savoir plus, rendez-vous sur **www.acronis.com**