Acronis Protected Server

Cyberprotection nativement intégrée pour les serveurs et les machines virtuelles

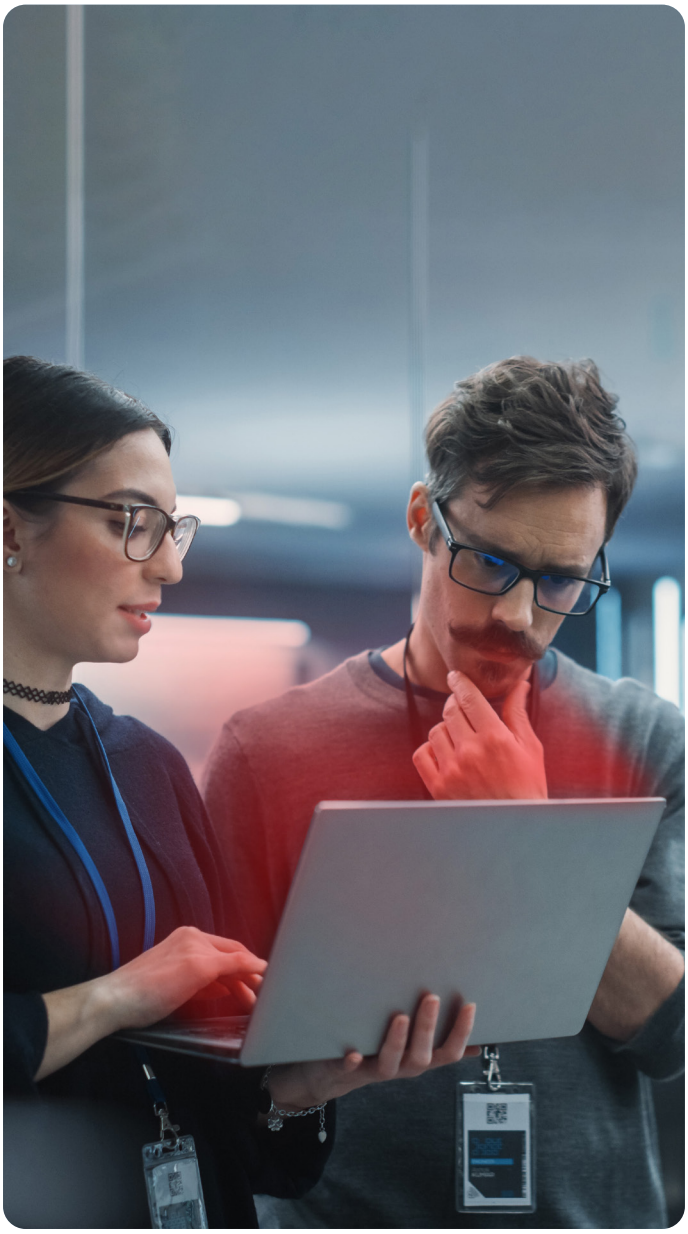
La cyberrésilience va au-delà de la cybersécurité traditionnelle. Il ne s'agit pas seulement de prévenir les attaques, mais aussi de garantir la continuité des activités des entreprises en cas d'incident. Comme le définit le NIST, « La cyberrésilience est la capacité à anticiper, à résister, à se restaurer et à s'adapter à des conditions défavorables, des contraintes, des attaques ou des compromissions des systèmes. »

Quelle est la rapidité de reprise de votre activité ? Sans guide tactique d'intervention sur incidents, sans outils, sans objectifs de délai de restauration et de point de restauration (RTO et RPO) clairement définis, chaque perturbation risque d'entraîner une perte de chiffre d'affaires, d'entamer la confiance des clients et d'entraîner des dommages de réputation durables.

Difficultés liées à la résilience

Les entreprises de toutes tailles constatent que les interruptions d'activité coûtent bien plus cher que les pertes de données. Elles sont confrontées à des pressions croissantes en matière de conformité et de surveillance réglementaire. Toute lacune en matière de préparation les expose à des amendes, des pénalités et des risques pour leur réputation.

La gestion des incidents avec des outils fragmentés crée également une complexité inutile. Sans stratégie unifiée, les équipes informatiques sont confrontées à un chaos opérationnel, car elles doivent assembler les fonctions de détection, de réponse et de reprise d'activité à partir de plusieurs consoles et agents. Ces inefficacités augmentent les coûts, ralentissent les temps de réponse et accroissent la responsabilité. L'augmentation des primes de cyberassurance risque d'ajouter des préoccupations supplémentaires, et une résilience insuffisante peut même entraîner un refus de couverture.



Les obstacles technologiques à la résilience

Avec l'accélération de la transformation numérique des entreprises, la résilience devient plus difficile à atteindre. Les environnements informatiques hybrides s'étendent sur site, dans le cloud et sur des terminaux distants, ce qui crée une surface d'attaque en constante expansion. Cela entraîne une augmentation des interdépendances et des points de défaillance uniques. Dans le même temps, les menaces deviennent plus sophistiquées. Les ransomwares, les compromissions de la chaîne d'approvisionnement et les risques internes exploitent les failles laissées par les solutions cloisonnées. Des outils ponctuels peuvent réduire des risques spécifiques, mais ils créent également des zones d'ombre, des processus manuels et des failles que les attaquants exploitent volontiers.

La voie vers la cyberrésilience

Pour atteindre une véritable cyberrésilience, il ne suffit pas de disposer de défenses solides. Il s'agit de garantir la continuité, quelles que soient les perturbations. Les entreprises peuvent atteindre la résilience en adoptant une approche structurée qui commence par **anticiper** les risques grâce à un mappage des ressources, l'évaluation des vulnérabilités et la gestion des correctifs. Elles doivent ensuite être en mesure de **résister** aux menaces en les détectant et en les contenant en temps réel grâce à des fonctionnalités avancées telles que la protection des terminaux optimisée par l'IA et la surveillance basée sur l'apprentissage automatique. Ces mesures proactives ne sont efficaces que si elles sont associées à une stratégie de restauration solide.

La restauration est l'étape critique suivante. La restauration rapide, fiable et sans malware des données et des systèmes permet de limiter au minimum les interruptions d'activité. En cas de panne grave, l'objectif premier est de maintenir la continuité des activités. Avec Acronis Cloud Disaster Recovery, les entreprises peuvent effectuer une bascule immédiate des ressources vers Acronis Cloud ou Microsoft Azure. Ce basculement immédiat garantit la continuité même en cas de panne grave et sert d'environnement de secours sécurisé jusqu'à ce que la restauration complète des systèmes principaux soit terminée.

Enfin, la résilience n'est pas statique. Les organisations doivent **s'adapter** en tirant des enseignements des incidents, en formant leurs équipes et en renforçant leurs défenses au fil du temps.

Le spectre de la reprise d'activité après sinistre

Ces stratégies ne visent pas uniquement à la reprise d'activité après sinistre, mais à la résilience opérationnelle qui permet de poursuivre les activités essentielles en toutes circonstances. La possibilité de restaurer des services en quelques minutes plutôt qu'en plusieurs jours est la clé pour minimiser les pertes financières et conserver la confiance des clients.

Les stratégies de reprise d'activité après sinistre sont généralement classées en fonction des RPO et RTO qu'elles permettent d'atteindre. Parmi les stratégies privilégiées, en voici deux :

Reprise d'activité sur site tiède

Cette approche offre un bon compromis entre coût et rapidité de restauration. Elle utilise des systèmes préconfigurés qui peuvent être mis en ligne rapidement, ce qui correspond à l'objectif de restauration des données en cas d'interruption d'activité (« recover ») selon les RPO et RTO définis.

Reprise d'activité sur site froid

La reprise d'activité sur site froid est une solution de restauration et de reconstitution des données qui repose sur la restauration complète des sauvegardes. Les temps de restauration sont plus longs, mais les coûts d'exploitation plus faibles.

En unifiant la détection, la protection et la restauration, les entreprises bénéficient d'un avantage critique : elles peuvent non seulement survivre à une crise, mais en sortir renforcées. Avec Acronis Cloud Disaster Recovery, les entreprises peuvent choisir le niveau de résilience adapté à chaque ressource, des options de basculement tiède à froid qui reconstituent les services après une panne, à une continuité quasi instantanée avec une reprise d'activité sur site chaud intégrée. Cette flexibilité renforce les défenses à chaque phase du parcours de cyberrésilience.

La solution Acronis Protected Server

La solution Acronis Protected Server unifie la sauvegarde, la restauration après sinistre, la sécurité des terminaux, l'évaluation des risques et la prévention des pertes de données en une seule plate-forme de cyberprotection intégrée de manière native. Cette approche élimine les cloisonnements, réduit la prolifération des outils et garantit la résilience sans complexité supplémentaire. La plate-forme couvre toutes les phases du parcours de résilience : Anticipation, Résistance, Restauration et Adaptation. Avec une plate-forme, un agent et une console uniques, les entreprises peuvent détecter les menaces plus rapidement, restaurer les opérations sans perturbation et s'adapter en continu aux risques en constante évolution.

ANTICIPATION	RÉSISTANCE	RESTAURATION	ADAPTATION
• Détection des terminaux • Carte de protection des données • Inventaire des ressources • Évaluation des vulnérabilités • Gestion des correctifs	• Détection des menaces en temps réel • Activez l'EDR (détection des menaces et réponse sur les terminaux) optimisé par l'intelligence artificielle • Surveillance basée sur l'apprentissage automatique • Contention rapide des menaces actives	• Restauration de données automatisée et sécurisée • Reprise après sinistre dans le cloud (CDR) • Sauvegardes immuables • Mobilité de l'hyperviseur • Restauration sur des points exempts de malware	• Surveillance et gestion des terminaux • Solution Security Awareness Training (SAT) • Modèles d'intervention sur incidents de type conseil

Pourquoi les entreprises choisissent-elles Acronis ?

Dans un environnement où les cyberattaques sont inévitables, Acronis renforce la cyberrésilience en unifiant la protection contre les menaces optimisée par l'intelligence artificielle avec la restauration après sinistre orchestrée par le cloud sur une seule plate-forme. Contrairement aux approches fragmentées et uniquement préventives, Acronis garantit que les données critiques sont à la fois protégées et récupérables grâce à des sauvegardes immuables, à la détection des ransomwares basée sur l'IA et à la validation d'une restauration adéquate.

Avec la reprise d'activité après sinistre entièrement gérée dans le cloud, le basculement instantané vers Acronis Cloud, la facturation basée sur l'utilisation ainsi que les tests et l'exécution contrôlés par le client, la solution Acronis Protected Server offre une cyberprotection professionelle sans le coût ou la complexité de l'ancienne infrastructure. Le résultat est une restauration plus rapide, un risque opérationnel réduit et une continuité des activités ininterrompue dès que nécessaire.

Demandez une démonstration avec un expert Acronis

La continuité de vos activités exige bien plus que de la protection. Cela exige de la résilience. Découvrez comment Acronis peut vous aider à anticiper les menaces, à résister aux attaques, à récupérer plus rapidement et vous adapter.

NOUS CONTACTER

Acronis

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