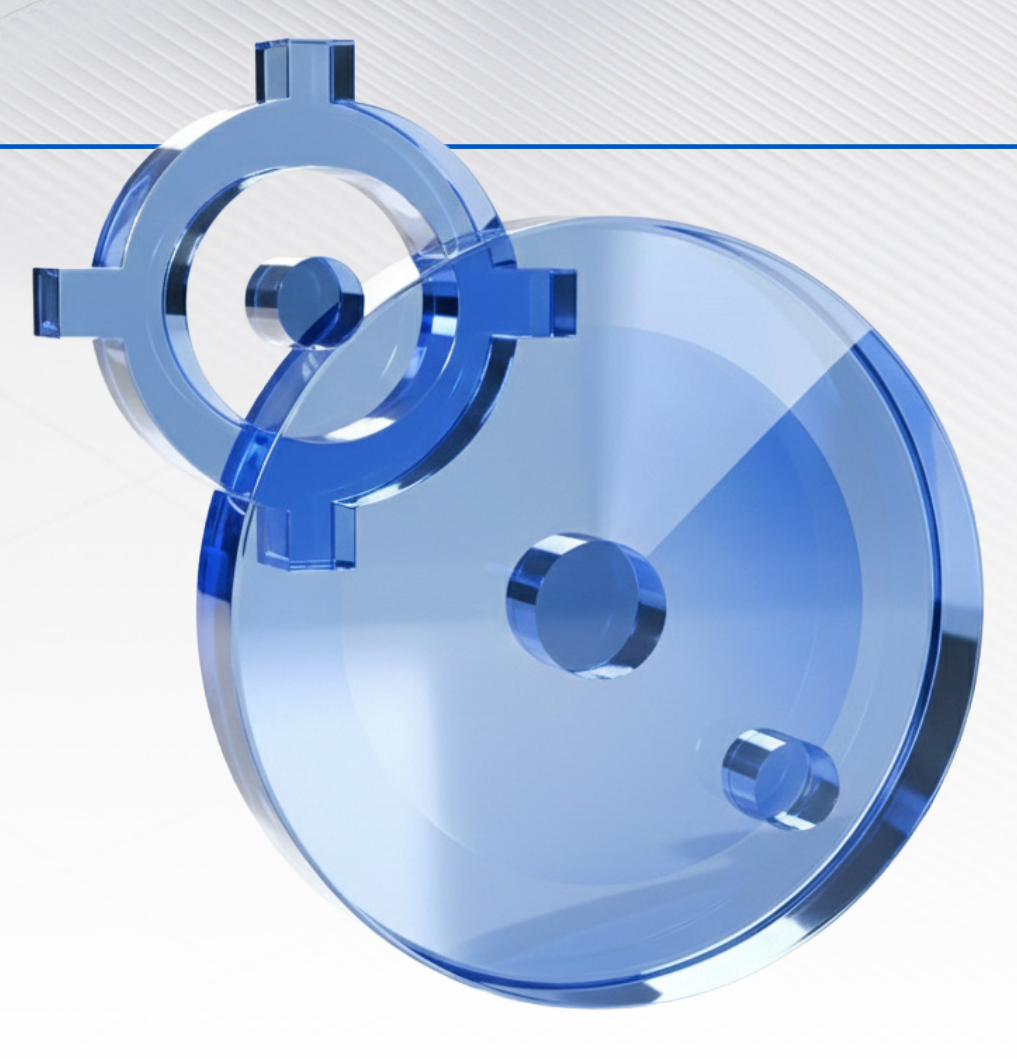
Acronis

Au-delà de la cybersécurité : intégrer la cyberrésilience pour assurer la continuité des activités

Pourquoi les responsables IT doivent se préparer aux perturbations, et pas seulement se soucier de la prévention.

Cybersécurité vs cyberrésilience



La cybersécurité vise à bloquer les attaques.
La cyberrésilience garantit la continuité des activités pendant et après une attaque.

Cybersécurité
Prévention, défense périmétrique, protection contre les intrusions

Cyberrésilience
Adaptabilité, restauration, continuité des activités

Impact de la continuité des activités selon les secteurs

Pourquoi la cyberrésilience est essentielle dans les secteurs critiques

Les interruptions et les perturbations de cybersécurité touchent tous les secteurs, mais leurs conséquences varient selon l'activité.

Santé

60 %

des établissements de santé déclarent que des incidents de cybersécurité perturbent directement la prise en charge des patients[1].

Pourquoi est-ce important ?
Les interruptions retardent les soins, redirigent les patients et compromettent la sécurité.

Retail

43 %

des distributeurs ont subi une interruption majeure due à des incidents de cybersécurité au cours de l'année écoulée[2].

Pourquoi est-ce important ?
Même de courtes interruptions impactent le chiffre d'affaires, la visibilité des stocks et l'expérience client.

Services financiers

91 %

des institutions financières ont subi au moins un incident de cybersécurité l'an dernier[3].

Pourquoi est-ce important ?
Les interruptions perturbent le traitement des transactions, la confiance des clients et la conformité réglementaire.

Logistique et transport[4]

94 %

des organisations déclarent que les perturbations de cybersécurité peuvent entraîner des défaillances en cascade de la chaîne logistique[5].

Pourquoi est-ce important ?
Les interruptions d'activité bloquent le suivi des expéditions, les opérations au sein des entrepôts et les livraisons en flux tendu.

Administrations publiques / Gouvernement

60 %

des pannes réseau coûtent aux organisations au moins 1 million de dollars en perturbations opérationnelles[6].

Pourquoi est-ce important ?
Les pannes affectent les services aux citoyens, les réponses aux situations d'urgence et la confiance du public.

Les interruptions compromettent la continuité des activités

Les interruptions d'activité affectent les revenus, les opérations et la réputation, pas seulement les systèmes informatiques.

96 %

des organisations ont subi au moins une interruption d'activité au cours des trois dernières années.

80 %

estiment que les interruptions d'activité deviennent de plus en plus graves[7].

Pourquoi la redondance traditionnelle échoue face aux ransomwares

La redondance protège contre les défaillances matérielles, pas contre des attaques intelligentes et propagées.

Les réplications peuvent propager l'infection.

Des outils fragmentés de reprise d'activité après sinistre et de sauvegarde créent des angles morts.

La multiplication des outils allonge les délais de restauration et alourdit les opérations.

La résilience moderne exige de nouveaux indicateurs de reprise des activités

La rapidité ne suffit plus : la restauration doit être fiable et répondre aux besoins de l'entreprise.

RTO
Délai maximal de reprise des opérations

RPO
Perte de données maximale acceptable

MTD
Durée maximale d'interruption avant impact critique sur l'activité

MTCR
Délai de restauration d'un environnement vérifié et exempt de malware

Une restauration fiable est désormais indispensable à la continuité des activités

Une restauration rapide n'a aucun sens si les systèmes sont compromis.

- Coût moyen d'une compromission de données : 4,45 millions de dollars.
- Les perturbations opérationnelles constituent le principal poste de dépenses liées aux intrusions[8].

Ce que les responsables IT doivent prioriser

La résilience est un choix à la fois économique et opérationnel.

Actions prioritaires (niveau stratégique)

Aligner la protection sur la criticité des ressources

Tester la restauration dans des scénarios d'attaque réels

Valider les sauvegardes avant la restauration

Réduire la complexité grâce à des plates-formes unifiées

La cyberrésilience garantit continuité, confiance et maîtrise, même lorsque les attaques sont inévitables.

De la cybersécurité à la cyberrésilience avec Acronis

La cybersécurité ne se limite pas à la protection. Elle repose sur la résilience. Découvrez comment Acronis peut vous aider à anticiper les menaces, à résister aux attaques, à restaurer vos systèmes plus rapidement et à vous adapter.

Nous contacter

---

[1] U.S. Department of Health and Human Services (HHS)
https://www.hhs.gov/about/news/2023/12/01/ransomware-cyber-attacks-threaten-patient-safety.html

[2] Uptime Institute. "Annual Outage Analysis 2023."
https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023

[3] World Economic Forum. "Global Cybersecurity Outlook 2024."
https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

[4] World Economic Forum – Global Risks Report
https://www.weforum.org/reports/global-risks-report-2024

[5] Ibid

[6] Intelligent CIO. "U.S. government organizations lose millions in an average network outage or breach."
https://www.intelligentcio.com/north-america/2021/01/26/us-government-organizations-lose-millions-in-an-average-network-outage-or-data-breach/

[7] Uptime Institute. "Annual Outage Analysis 2023."
https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023

[8] IBM. "Cost of a Data Breach Report 2025."
https://www.ibm.com/reports/data-breach

Acronis