

Résilience opérationnelle à l'ère de la connectivité

Nouvelles recherches sur la cybersécurité dans les environnements de fabrication connectés

Rockwell Automation

La nouvelle réalité de la sécurité OT

Les entreprises industrielles connectent davantage de systèmes, accélèrent le déploiement de l'IA et poussent les opérations à fonctionner en temps réel. Ces investissements créent de la rapidité et de la flexibilité. Ils augmentent également le risque opérationnel.

De nouvelles données recueillies par Rockwell Automation révèlent un décalage entre la confiance et l'exposition opérationnelle.

Près de la moitié des entreprises (4 %) ont connu un incident de cybersécurité au cours de l'année écoulée, pourtant 90 % d'entre elles affirment être confiantes dans leur capacité à maîtriser un tel incident. Plus d'un tiers (34 %) considère la cybersécurité comme l'un des principaux obstacles externes à la croissance au cours des 12 prochains mois.

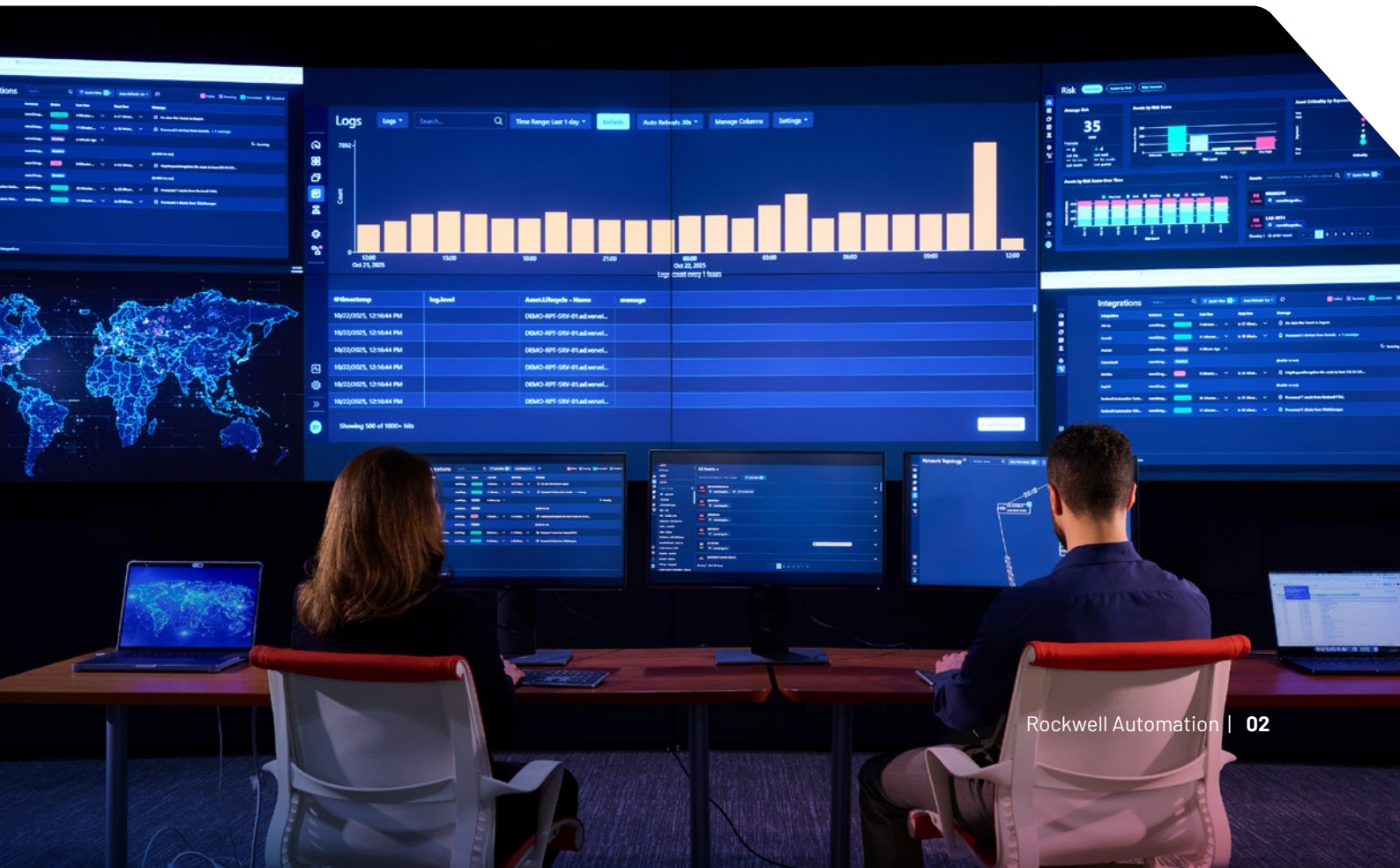
Malgré cela, les entreprises comprennent les enjeux et prennent des mesures pour renforcer leur résilience, et leur confiance. 62 % ont déjà investi dans des plates-formes de cybersécurité telles que l'inventaire des actifs, les systèmes de détection d'intrusion et l'accès à distance sécurisé. La cybersécurité figure également parmi les principales technologies ayant généré un retour sur investissement au cours des 12 derniers mois.

Le problème n'est pas la sensibilisation. Les entreprises industrielles savent que le risque cyber affecte la disponibilité, la continuité, la productivité et la croissance. Le défi est lié au fait qu'il faut sécuriser des opérations qui deviennent de plus en plus connectées et complexes.

L'adoption de l'IA se poursuit. Les environnements IT et OT continuent de converger. Les données opérationnelles circulent entre toujours plus d'actifs, d'utilisateurs, d'appareils et d'applications que jamais auparavant. Chaque connexion crée une nouvelle dépendance. Chaque dépendance crée un nouveau point d'exposition.

La bonne nouvelle, c'est que les entreprises relèvent le défi. Elles ne considèrent plus la cybersécurité comme une initiative IT distincte, mais la voient de plus en plus comme faisant partie de la performance opérationnelle.

Les entreprises qui seront à l'avant-garde de la prochaine phase des opérations industrielles sont celles qui développeront la visibilité, une architecture sécurisée et des capacités de réponse permettant de maintenir la production en cas de perturbation.



Une confiance croissante grâce à l'investissement. Mais est-ce suffisant ?

Les entreprises ne restent pas immobiles. Elles investissent dans les technologies, les architectures et les capacités nécessaires pour renforcer la résilience face aux cybermenaces. L'étape suivante consiste à regrouper ces investissements dans un programme de cybersécurité qui améliore en continu la visibilité, réduit les risques et s'adapte à l'évolution des besoins opérationnels. Les données montrent où les entreprises concentrent leurs efforts aujourd'hui.

Voici la principale conclusion :

- Les points d'intégration IT/OT sont classés parmi les plus vulnérables aux incidents de cybersécurité, juste derrière les systèmes informatiques et les réseaux d'entreprise. Les investissements en cybersécurité ont généré l'un des meilleurs retours sur investissement au cours des 12 derniers mois.
- La cybersécurité est le deuxième facteur de retour sur investissement parmi les investissements technologiques.

Cette conclusion indique un changement clair : les entreprises intègrent la cybersécurité dans des stratégies de transformation numérique plus larges, aux côtés de l'IA, de l'automatisation, des technologies cloud et des opérations connectées. Mais à mesure que les environnements deviennent plus interconnectés, la résilience dépend de la capacité des entreprises à transformer les investissements en actions coordonnées.

62%

Entreprises ayant déjà investi dans des plates-formes de cybersécurité

45%

Entreprises qui prévoient d'utiliser l'IA et l'apprentissage automatique pour la cybersécurité au cours des 12 prochains mois

35%

Plus d'un tiers des entreprises industrielles considèrent la cybersécurité comme l'un des plus grands obstacles externes à la croissance, juste après la pénurie de main-d'œuvre, pour les 12 prochains mois.

37%

Les entreprises qui déclarent que la sécurisation de l'architecture IT/OT favorisera des résultats commerciaux positifs au cours des cinq prochaines années.



Renforcer la résilience des opérations OT

Les entreprises industrielles ont réalisé des progrès significatifs en investissant dans la cybersécurité. Le prochain défi consiste à transformer ces investissements en résilience opérationnelle.

Une sécurité OT résiliente nécessite plus que des outils et des solutions ponctuelles. Cela nécessite une approche proactive et globale, alignée sur des cadres et des normes reconnus internationalement tels que le NIST, la NIS2 et l'IEC 62443. Cela donne aux entreprises une méthode structurée pour améliorer leur maturité en matière de sécurité tout en répondant aux exigences réglementaires.

Les capacités suivantes mettent en avant les actions menées par des entreprises de premier plan et illustrent concrètement ce à quoi cela ressemble en pratique.



Conseil stratégique

Élaborer une stratégie de cybersécurité basée sur les risques.

La résilience en cybersécurité commence par la compréhension des risques dans le contexte des priorités opérationnelles, des objectifs commerciaux et de la réalité organisationnelle. Avant de pouvoir réduire efficacement les risques, améliorer leur résilience ou répondre aux exigences de conformité, les entreprises doivent avoir une vision claire de leur posture de cybersécurité actuelle et des lacunes qui présentent les risques les plus importants. Sans cette base, les investissements en cybersécurité peuvent devenir fragmentés, réactifs et difficiles à mettre en œuvre.

Les entreprises qui mettent en œuvre des services de conseil stratégique peuvent :

- Identifier les risques, établir des priorités et aligner les investissements sur les résultats commerciaux
- Remplacer les décisions de sécurité réactives et ponctuelles par une feuille de route des priorités basée sur les risques et alignée sur les objectifs opérationnels et commerciaux.
- Comprendre les niveaux d'exposition actuels posés par les actifs, les vulnérabilités, les procédés et les pratiques de gouvernance, afin de concentrer les ressources là où elles auront le plus grand impact.
- Améliorer la préparation à la conformité en identifiant les lacunes en matière de sécurité et en alignant les efforts de remédiation sur les normes et exigences applicables.
- Établir une cohésion interne entre les équipes IT, OT et de direction autour d'une compréhension commune des risques, des priorités et des résultats de sécurité mesurables.

Infrastructure et réseaux industriels

Les entreprises continuent de moderniser l'architecture IT/OT à mesure que les opérations deviennent plus connectées. Bien que chaque nouvelle connexion augmente le risque de cybersécurité, une architecture défendable permet d'éviter que la complexité ne se transforme en une surface d'attaque élargie. Les entreprises de premier plan qui intègrent la cybersécurité dès la conception de leurs opérations sont mieux placées pour réduire les risques, améliorer leur résilience et consacrer moins de temps à réagir aux incidents, tout en se concentrant davantage sur l'atteinte de leurs objectifs opérationnels.

Les entreprises proactives peuvent :

- Faire progresser les initiatives de transformation numérique en toute confiance tout en contribuant à la protection des systèmes opérationnels critiques.
- Réduire la probabilité et l'impact des perturbations grâce à la segmentation du réseau, afin de contenir les menaces avant qu'elles n'affectent la production.
- Activer un accès à distance sécurisé qui favorise la flexibilité opérationnelle, la productivité et la collaboration, sans créer de points d'entrée non supervisés.
- Mettre en œuvre des architectures sécurisées dès la conception qui réduisent les risques tout au long du cycle de vie des actifs.
- Réduire le coût de la sécurité à long terme en abordant les risques de manière proactive au travers de l'architecture et de la conception, plutôt qu'en procédant à des corrections réactives.

Gestion de l'inventaire et du cycle de vie des actifs

Avoir une visibilité sur les actifs et les risques

La visibilité limitée est l'un des obstacles les plus courants à l'atteinte de la résilience. Sans une vue complète de l'environnement, y compris les systèmes existants, les dispositifs connectés en série ou les connexions temporaires, les entreprises n'ont pas le point de départ nécessaire pour planifier et mettre en œuvre une réduction significative des risques.

Une visibilité complète des actifs permet aux entreprises de :

- Comprendre et hiérarchiser les risques de cybersécurité dans l'ensemble de l'environnement opérationnel
- Réduire les angles morts pouvant créer des risques opérationnels, de sécurité et de cybersécurité.
- Prendre de meilleures décisions plus rapidement en comprenant quels actifs sont connectés, lesquels sont exposés aux risques et lesquels sont les plus critiques pour la production et les opérations commerciales.
- Accélérer les efforts de réduction des risques en priorisant les activités de remédiation en fonction de leur impact opérationnel, et pas seulement de la gravité des vulnérabilités.
- Améliorer la résilience opérationnelle grâce à une gestion continue du cycle de vie des actifs, qui permet de maintenir un environnement sécurisé et pris en charge dans la durée.
- S'appuyer sur la base du programme pour développer des mesures compensatoires et d'autres composants afin d'assurer une cybersécurité de bout en bout.

Gestion des risques et des vulnérabilités

Prioriser et corriger les risques les plus importants.

Les entreprises ne peuvent pas éliminer tous les risques liés à la cybersécurité, mais elles peuvent améliorer leur posture de sécurité en renforçant la rapidité avec laquelle elles identifient, priorisent et réagissent aux menaces avant qu'elles n'affectent leurs opérations. À mesure que les opérations industrielles deviennent plus connectées, une gestion efficace des risques dépend de la visibilité contextuelle, de la prise de décisions fondées sur les risques et du maintien de la continuité opérationnelle face aux perturbations.

Un programme de gestion des vulnérabilités basé sur les risques aide les entreprises à :

- Donner la priorité à la remédiation en fonction de l'impact opérationnel, et pas seulement des niveaux de gravité.
- Réduire le temps moyen de remédiation sur l'ensemble des actifs OT
- Démontrer des progrès mesurables en matière de conformité par rapport aux normes IEC 62443, NIST CSF et NIS2.
- Permettre de prendre des décisions d'investissement éclairées en alignant les investissements en cybersécurité sur la tolérance au risque de l'entreprise et les objectifs opérationnels.

Détection et réponse gérées

Maintenir une vigilance continue sur l'ensemble des opérations

À mesure que les environnements IT et OT deviennent de plus en plus interconnectés, les entreprises sont confrontées à une difficulté croissante pour distinguer les événements de sécurité courants des menaces susceptibles de perturber leurs opérations. La surveillance continue permet d'identifier les risques les plus importants avant qu'ils ne provoquent des perturbations.

Un programme de détection et de réponse proactif aide les entreprises à :

- Accélérer la détection et la réponse en assurant une surveillance 24h/24 et 7j/7, ainsi qu'une visibilité continue sur les environnements IT et OT.
- Permettre de prendre de meilleures décisions plus rapidement grâce à des informations contextualisées qui aident les équipes à identifier quelles menaces nécessitent une action immédiate.
- Combler le déficit de compétences en renforçant les capacités internes grâce à une expertise dédiée en sécurité OT, sans avoir à supporter les coûts de création et de maintenance d'un SOC interne complet.
- Renforcer l'efficacité du programme en intégrant la détection des menaces à la gestion des vulnérabilités, à la réponse aux incidents, à la gouvernance et aux efforts d'amélioration continue.

Réponse aux incidents et reprise

Contenir, restaurer et améliorer

Lorsqu'un incident de cybersécurité survient, une réponse rapide est essentielle pour déterminer l'ampleur des dommages, la durée d'interruption et les coûts auxquels une entreprise pourrait être confrontée. Contenir un incident n'est qu'une partie du défi. Les entreprises doivent comprendre l'importance de la préparation à la reprise en ce qui concerne la résilience opérationnelle. Lorsque le pire se produit, elles doivent être en mesure de rétablir rapidement les services et de reprendre leurs activités normales.

Un programme mature de réponse aux incidents permet aux entreprises de :

- Réduire l'impact des incidents de cybersécurité grâce à des procédures de réponse et de confinement prédéfinies et testées.
- Accélérer la reprise opérationnelle en coordonnant la réponse et la récupération entre les équipes IT, OT et opérationnelles.
- Minimiser les temps d'arrêt en améliorant la préparation à la reprise pour les systèmes critiques.
- Renforcer la confiance des parties prenantes grâce à une communication claire, une bonne gouvernance et une gestion efficace des incidents pendant et après un événement.
- Mener une enquête détaillée sur l'incident afin d'identifier la cause première et d'appliquer les leçons apprises pour renforcer en continu la cyberrésilience.



La résilience devient un avantage concurrentiel.

Les entreprises industrielles investissent massivement dans la cybersécurité, l'intelligence artificielle et les opérations connectées. Ces investissements renforcent la confiance, mais la technologie à elle seule ne crée pas la résilience.

Les entreprises qui tireront le plus de valeur de la cybersécurité seront celles qui adopteront une approche proactive et structurée. En intégrant dès le départ la visibilité, la prise de décision basée sur les risques, des architectures sécurisées, la surveillance continue et la préparation à la reprise dans leurs opérations, elles peuvent réduire les risques opérationnels, maintenir la production et permettre à l'entreprise d'avancer en toute confiance.

Dans un environnement industriel plus connecté, la cybersécurité ne se résume plus seulement à protéger les actifs. Il s'agit de permettre des opérations résilientes capables de s'adapter, de se rétablir et de continuer à apporter de la valeur à l'entreprise.

Pour en savoir plus, contactez votre représentant Rockwell Automation.

Rockwell Automation

Suivez-nous.

rockwellautomation.com — expanding **human possibility**®

AMÉRIQUES : Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 États-Unis, Tél. : +(1) 414.382.2000
EUROPE / MOYEN-ORIENT / AFRIQUE : Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgique, Tél. : +(32) 2 663 0600
ASIE PACIFIQUE : Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tél: (65) 6510 6608
CANADA : Rockwell Automation, 3043 rue Joseph A. Bombardier, Laval, Québec, H7P 6C5, Tél: +1 (450) 781-5100, www.rockwellautomation.ca
FRANCE : Rockwell Automation SAS – 2, rue René Caudron, Bât. A, F-78960 Voisins-le-Bretonneux, Tél: +33 1 61 08 77 00
SUISSE : Rockwell Automation AG, Av. des Baumettes 3, 1020 Renens, Tél: 021 631 32 32, Customer Service Tél: 0848 000 278

Allen-Bradley et expanding human possibility sont des marques commerciales de Rockwell Automation, Inc.
Les marques commerciales n'appartenant pas à Rockwell Automation sont la propriété de leurs sociétés respectives.

Publication GMSN-SP043A-FR-P - Août 2026

Copyright © 2026 Rockwell Automation, Inc. Tous droits réservés. Imprimé aux États-Unis.