Sécurisez votre avenir

Protéger l'appareil productif à l'heure de la transformation digitale

verizon business

Sécurisez votre avenir

Conjuguer innovation et sécurité peut parfois s'apparenter à un numéro d'équilibriste. Pour éviter la chute tout en allant de l'avant, il est important de ne jamais perdre de vue un principe fondamental.

En entreprise, les plus grandes opportunités s'accompagnent souvent des plus grands risques. La transformation digitale nous en donne le parfait exemple.

D'un côté, elle peut booster l'efficacité, améliorer la qualité des produits, optimiser l'expérience client et renforcer la résilience opérationnelle. De l'autre, elle engendre bien malgré elle des risques de cybersécurité, notamment pour les technologies opérationnelles (OT) si essentielles à la production.

La sécurité OT s'impose ainsi comme un impératif absolu dans un large éventail de secteurs, à commencer par l'industrie, le pétrole, le gaz, la distribution d'énergie, le transport, etc. Bref, elle concerne toutes les infrastructures vitales pour l'économie en général – et pour votre compte de résultats en particulier.

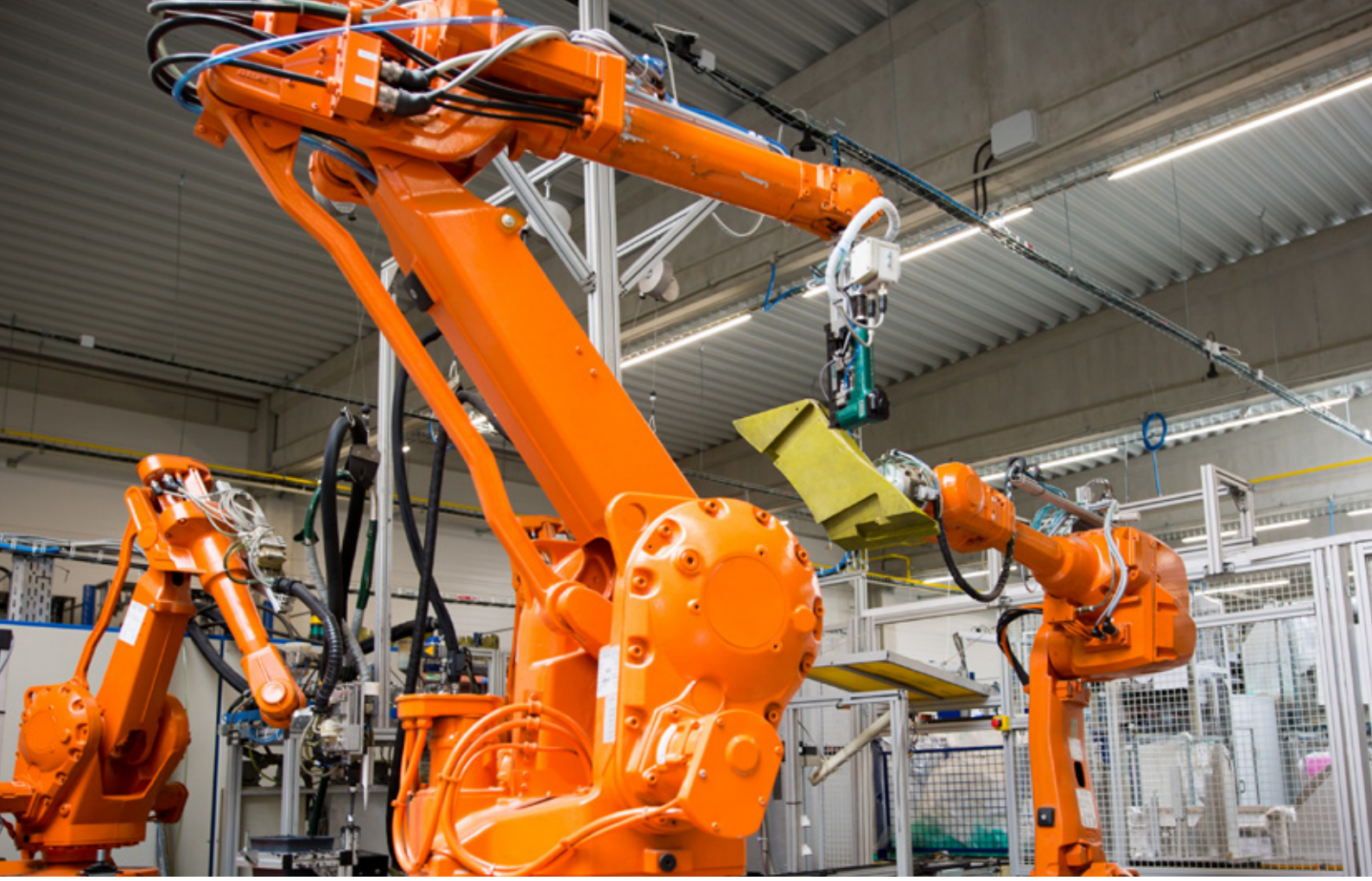
Heureusement, les leçons de la transformation digitale d'un secteur peuvent facilement s'appliquer à un autre. En d'autres termes, on peut innover sans prendre de risques inconsidérés.

Loin de nous l'idée de sous-estimer l'ampleur du défi. Les entreprises industrielles font face à des menaces de sécurité bien réelles. Partant de ce constat, ce guide s'inscrit dans une optique d'action positive, à savoir l'implémentation de solutions capables de protéger vos environnements OT tout en récoltant les fruits de l'Industrie 4.0.

Prendre conscience des problèmes de sécurité OT, c'est déjà faire un grand pas vers leur résolution. Verizon vous accompagne dans cette démarche, avec un seul objectif en ligne de mire : placer la protection au service de la croissance.

Adoptez une approche holistique de la cybersécurité avec Verizon

Verizon, c'est un portefeuille complet de solutions de sécurité IT et OT qui ont su gagner la confiance de milliers d'entreprises à travers le monde. Notre approche holistique de la cybersécurité s'articule autour de trois axes : vos besoins métiers, vos budgets et vos objectifs de transformation digitale.



La transformation digitale, un impératif absolu

Si vous lisez ces lignes, c'est que la transformation digitale figure en tête de vos priorités. C'est d'ailleurs le cas de la plupart des industriels. Dans ce secteur, le changement va en s'accélérant depuis que le concept d'Industrie 4.0 s'est généralisé.

> La transformation digitale peut augmenter le rendement de 10 % à 30 %.
>
> Source : McKinsey & Company, Preparing for the next normal via digital manufacturing's scaling potential, 2020

Dans le monde interconnecté qui est le nôtre, les supply chains doivent être à la fois résilientes, agiles et optimisées. D'où l'urgence de la transformation digitale. À l'image de l'Internet industriel des objets (IIoT) et de l'intelligence artificielle (IA), de nouvelles technologies se sont très vite imposées dans l'industrie. Ensemble, elles apportent la transparence et la coordination nécessaires à une approche proactive de la gestion des stocks, de l'amélioration de l'efficacité et de la protection des systèmes contre les pannes. L'intégration digitale s'étend aussi à l'engagement client, l'analytique en temps réel et la personnalisation, rouages essentiels à la satisfaction et la fidélisation des clients.

Au-delà des seules considérations opérationnelles, la digitalisation aide aussi à gérer la pression de facteurs exogènes. Entre instabilité géopolitique et pénurie de talents, la digitalisation des opérations permet de s'adapter à des exigences particulièrement changeantes. Elle aide également à assurer un meilleur suivi des marqueurs environnementaux, à optimiser la consommation d'énergie et à mieux respecter les exigences réglementaires.

Toutefois, la transformation digitale ne doit pas nécessairement être considérée comme un poste de coûts. Entre maintenance prédictive et réduction des gaspillages, elle peut aussi engendrer des économies significatives. Sans oublier que la digitalisation des workflows et processus génère des insights sur lesquels votre entreprise peut capitaliser pour mieux répondre aux fluctuations des marchés, aux évolutions des cadres réglementaires et aux perturbations imprévues. Autant d'avantages considérables en ces temps de changements majeurs.

Attention cependant à ne pas créer involontairement des brèches dans vos opérations.

La menace se complexifie

La généralisation des technologies digitales n'a pas que des avantages. Côté sécurité, elle a aussi ouvert de nouvelles voies aux cyberattaques.

Prolifération des équipements IIoT, multiplication des projets d'IA, intégration des systèmes IT à des environnements OT autrefois isolés… tous ces facteurs ont contribué à un élargissement significatif de la surface d'attaque.

Les systèmes OT, notamment, reposent souvent sur d'anciens protocoles de communication incompatibles avec certaines technologies de sécurité actuelles. De même, de nombreux équipements OT comportent des vulnérabilités et sont dépourvus des fonctionnalités de sécurité présentes dans les environnements IT d'aujourd'hui. Autre facteur important, les systèmes OT ont une durée de vie plus longue, si bien qu'ils peuvent fonctionner sur des logiciels et du firmware en fin de support, synonyme de failles de sécurité potentielles.

> L'intégration des systèmes IT à des environnements OT autrefois isolés a considérablement élargi la surface d'attaque.

L'arrivée de l'IA représente un nouveau vecteur de menaces susceptibles d'exposer des équipements OT et des données sensibles à toute une sphère d'acteurs humains et non humains. A minima, ce phénomène complexifie la gestion des identités.

L'entraînement et l'utilisation de vos outils d'IA doivent s'accompagner de nouvelles pratiques de sécurité visant à protéger votre infrastructure de toute intrusion et vos données de tout usage abusif. Alors que des entreprises comme la vôtre devront générer, préparer, traiter et stocker des données dans les endroits les plus divers, la question de la souveraineté de la data devra occuper une place centrale dans vos réflexions. Il en va de même pour la protection de la propriété intellectuelle et des informations personnelles face à des outils d'IA particulièrement gourmands en données.

L’improvisation peut vous coûter cher

Dans l’industrie, la tolérance aux temps d’interruption opérationnelle est proche du zéro. Les cybercriminels le savent. Et ils savent aussi que votre propriété intellectuelle recèle des trésors de valeur. On ne s’étonnera donc guère de constater une hausse très sensible des intrusions système dans l’industrie en 2025, avec un doublement des compromissions recensées par rapport à 2024 (source : Rapport Data Breach Investigations Report – DBIR – 2025).

- **Le phishing et l’ingénierie sociale** prennent des salariés au piège en les amenant à divulguer des informations ou à commettre des actes de malveillance. Les personnes dotées de droits d’accès aux environnements IT et OT sont particulièrement ciblées.
- **Les attaques de la supply chain** exploitent les vulnérabilités présentes dans le maillage complexe de fournisseurs, sous-traitants et partenaires.
- **Les systèmes de contrôle industriel (ICS)** font l’objet de menaces sophistiquées qui visent spécifiquement à perturber les infrastructures et les opérations industrielles critiques.
- **Les attaques zero-day** exploitent des vulnérabilités technologiques jusqu’ici inconnues, représentant de fait un danger insaisissable.
- **Les appareils IoT non gérés et non sécurisés** peuvent servir de point d’entrée aux attaquants pour accéder aux environnements de production.

> En 2025, les intrusions système ont connu une forte hausse qui s'est soldée par un doublement des compromissions par rapport à 2024.
>
> Source : Verizon, Data Breach Investigations Report – DBIR – 2025

Outre le coût financier direct, les attaques peuvent provoquer un préjudice beaucoup plus vaste : fortes perturbations de la production, vol de propriété intellectuelle et autres données sensibles, détérioration d'actifs matériels et infraction aux réglementations en vigueur. Chez les opérateurs d'importance vitale (OIV), ces attaques peuvent même menacer directement la sécurité des populations.

La lutte contre ces dangers pour la cybersécurité se heurte souvent à différents obstacles. Tout d'abord, il est particulièrement difficile de tenir un inventaire précis et à jour d'un parc d'équipements OT et IIoT qui s'étend rapidement. Ensuite, concernant les attaques ciblant spécifiquement ces environnements, les équipes manquent d'une Threat Intelligence semblable à ce dont elles disposent pour l'IT. Enfin, les différences culturelles et les décalages dans les priorités entre les pôles IT et industriels peuvent freiner l'implémentation de mesures de cybersécurité dans les environnements OT.

Si votre entreprise envisage un rapprochement de l'IT et de l'OT dans le cadre de sa transformation digitale, ses pratiques de sécurité doivent aussi s'aligner.

Relever les défis des industriels internationaux

Les industriels sont généralement à la tête d'environnements IT et OT composites et géographiquement dispersés. Ces systèmes complexes se composent d'un mélange de technologies d'ancienne et de nouvelle génération, sur lesquelles se superpose un très large éventail d'équipements interconnectés. Un vrai casse-tête en termes de gestion de la sécurité.

Or, l'envergure même de ces opérations impose une approche avancée et unifiée de la cybersécurité.

Des réseaux et des équipes historiquement séparés doivent aujourd'hui être intégrés. Cela passe par un rapprochement culturel et opérationnel entre l'IT et l'OT, condition essentielle à l'établissement d'une posture de sécurité homogène.

Par ailleurs, l'industrie se caractérise par des supply chains à la fois longues et sinueuses. Du fait de l'interconnexion de ces vastes réseaux internationaux, la compromission d'un seul maillon de la chaîne peut avoir des répercussions en cascade sur tous les autres intervenants. Pour limiter le risque d'exposition, les industriels doivent donc veiller à ce que tous leurs fournisseurs et sous-traitants respectent des politiques de sécurité très strictes.

Toute passivité face aux cyberattaques peut avoir des conséquences délétères dans un secteur où les enjeux ne sont pas uniquement d'ordre économique pour les entreprises, mais aussi environnemental et sociétal pour les communautés qui les entourent. Par exemple, un prestataire de services non vitaux pourra tout simplement débrancher ses systèmes informatiques pendant que ses équipes neutralisent l'attaque. En revanche, lorsque des systèmes électriques ou de refroidissement sont concernés, il est essentiel de les maintenir en état de marche pour des raisons évidentes de protection des populations. Priorité doit toujours être donnée à la prévention de catastrophes industrielles majeures.

> Un rapprochement culturel et opérationnel entre l'IT et l'OT est une condition essentielle à l'établissement d'une posture de sécurité homogène.

L'impératif économique de la continuité opérationnelle peut parfois conduire à quelques raccourcis côté sécurité. Les décideurs peuvent ainsi hésiter à donner leur feu vert à la mise à jour des systèmes ou à leur arrêt pour maintenance, augmentant ainsi leur exposition aux cyberattaques.

Côté coûts, des contraintes budgétaires peuvent limiter les capacités d'investissement dans les dernières technologies et compétences en matière de sécurité. La répartition des ressources de sécurité à travers de nombreux sites et business units à l'international peut aussi présenter de nombreuses difficultés, a fortiori lorsque les budgets de cybersécurité sont détenus par l'IT, plutôt que par les fonctions opérationnelles. D'où l'importance d'unifier les budgets IT et OT afin d'assurer une protection appropriée à chaque pan de l'activité.

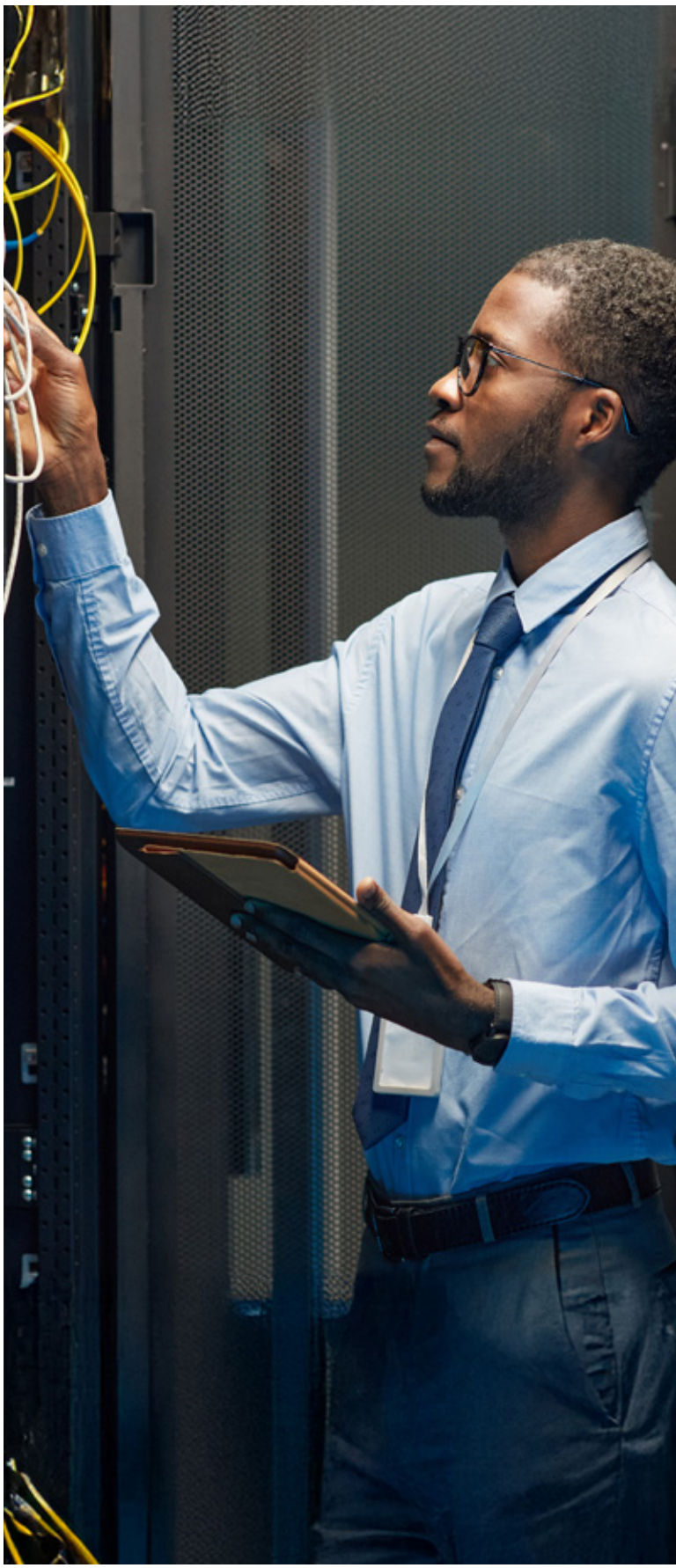
Vient ensuite la problématique des systèmes OT d'ancienne génération, souvent très profondément ancrés dans les processus de production. Le coût et la difficulté technique de leurs mises à jour les rendent particulièrement vulnérables aux attaques. Il est donc essentiel d'aborder de front le problème de la dette technique des environnements OT, tout en assurant la continuité de la production. Cela passe par une planification minutieuse, des compétences pointues et une approche échelonnée de la modernisation.

Une perspective mondiale de la cybermenace actuelle

Fruit de l'engagement de Verizon pour une sécurité pilotée par la data, notre rapport Data Breach Investigations Report (DBIR) dresse chaque année un état des lieux de la cybersécurité qui fait figure de référence dans le domaine.

Il révèle ainsi les risques et les compromissions dont sont victimes les acteurs de l'industrie et d'autres secteurs, tout en présentant les mesures correctives conseillées par ses experts. À lui seul, le rapport 2025 se fonde sur l'analyse de plus de 22 000 incidents réels, vous livrant ainsi des éclairages indispensables pour vous défendre face à une menace en perpétuelle mutation.

Téléchargez le rapport.



La cybersécurité de bout en bout, garante d'environnements OT plus sécurisés

La cybersécurité de l'OT devient beaucoup plus simple avec un expert à ses côtés.

Depuis de nombreuses années, Verizon aide des entreprises à renforcer leurs défenses. Notre approche de bout en bout assure la protection des infrastructures IT, auxquelles s'ajoutent de plus en plus d'environnements OT interconnectés.

Outre nos propres capacités étendues, nous faisons équipe avec d'autres leaders de la sécurité pour déployer des compétences spécialisées dans la sécurité OT. Ces collaborations nous permettent de proposer des solutions sur mesure, toujours en phase avec vos besoins spécifiques aux différentes étapes de votre transformation digitale.

Vous voulez protéger votre infrastructure OT critique avec une sécurité leader du marché ? Verizon peut réaliser un bilan sur site pour déterminer les axes d'amélioration les plus rentables et garants de résultats immédiats.

Votre environnement OT est le poumon de votre entreprise. À vous de bien le protéger.

Étude de cas : sécuriser les opérations high-tech d'un industriel

Pour ce producteur de vins, spiritueux et boissons non alcoolisées, le constat était sans appel : son infrastructure de sécurité n'avait pas su évoluer au rythme de son adoption des technologies connectées. L'entreprise s'est donc rapprochée de Verizon pour effectuer d'urgence une mise à jour de ses contrôles de sécurité. L'objectif : mieux s'adapter à l'évolution des exigences et rapprocher la sécurité du lieu de consommation ou de stockage des données.

Solution Verizon :

- Installation de nouveaux pare-feu on-prem et configuration de nouvelles politiques/zones de sécurité
- Gestion de ce dispositif par les experts des Verizon Managed Security Services
- Segmentation des LAN OT et IT dans plus de 20 usines à travers le monde
- Application des politiques de sécurité avec un minimum d'impact sur la production

Résultats :

- Création d'un nouvel environnement de sécurité pour accompagner la croissance future de l'entreprise
- Surveillance améliorée des équipements de sécurité
- Séparation des réseaux IT et OT pour réduire le cyber-risque
- Amélioration de la visibilité sur les équipements et les flux métiers

Envie d’approfondir la question de la transformation digitale ?

Des experts vous expliquent comment intégrer les dernières technologies pour créer une entreprise entièrement connectée.

Présentation des solutions Verizon pour l’industrie

Visitez l’un de nos centres d’innovation pour découvrir les derniers outils de transformation qui donnent l’avantage aux acteurs industriels.

Visiter un centre d’innovation

Découvrez comment protéger vos environnements OT

Lire notre livre blanc spécial protection OT

verizon business

© 2025 Verizon. Tous droits réservés. Verizon, le logo Verizon et tous les autres noms, logos et slogans identifiant les produits et services de Verizon sont des marques commerciales et des marques de service, déposées ou non, de Verizon Trademark Services LLC ou de ses filiales aux États-Unis et/ou dans d'autres pays. Les autres marques commerciales et marques de service citées sont la propriété de leurs détenteurs respectifs.