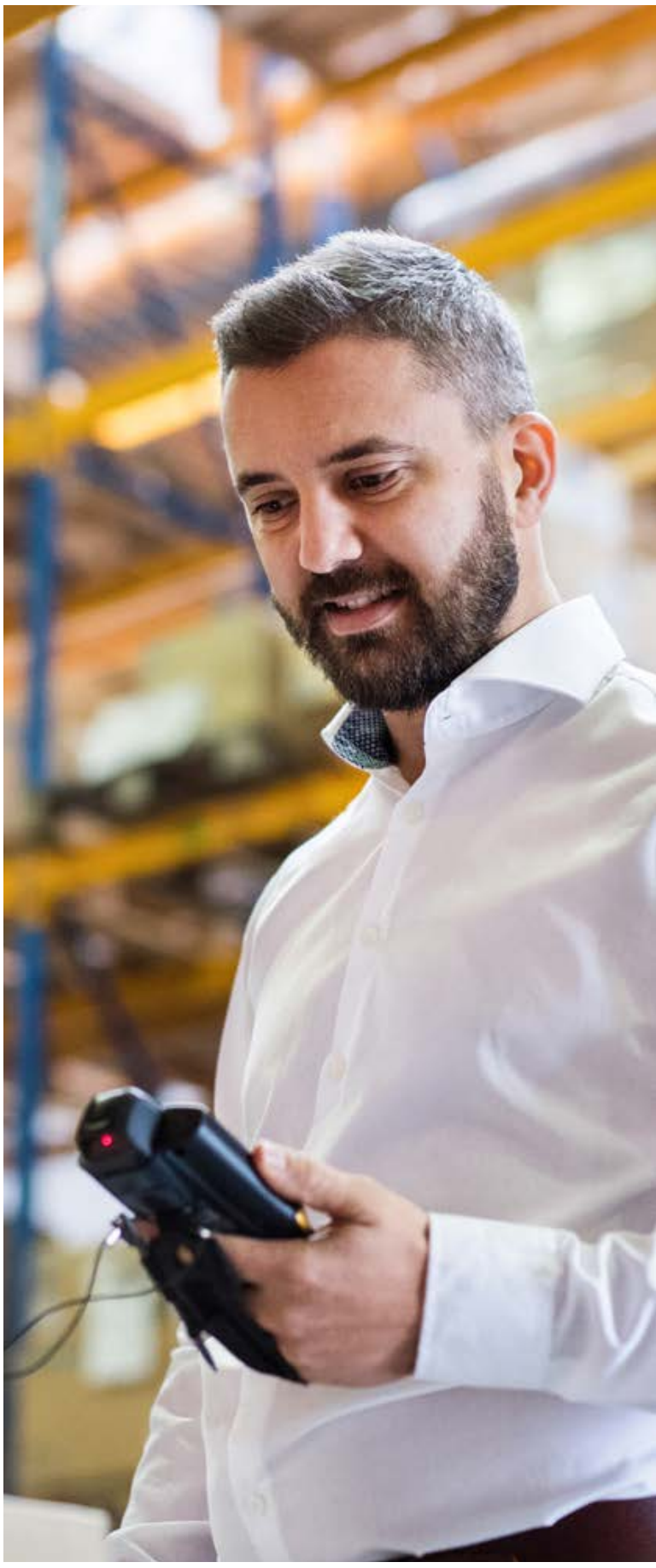
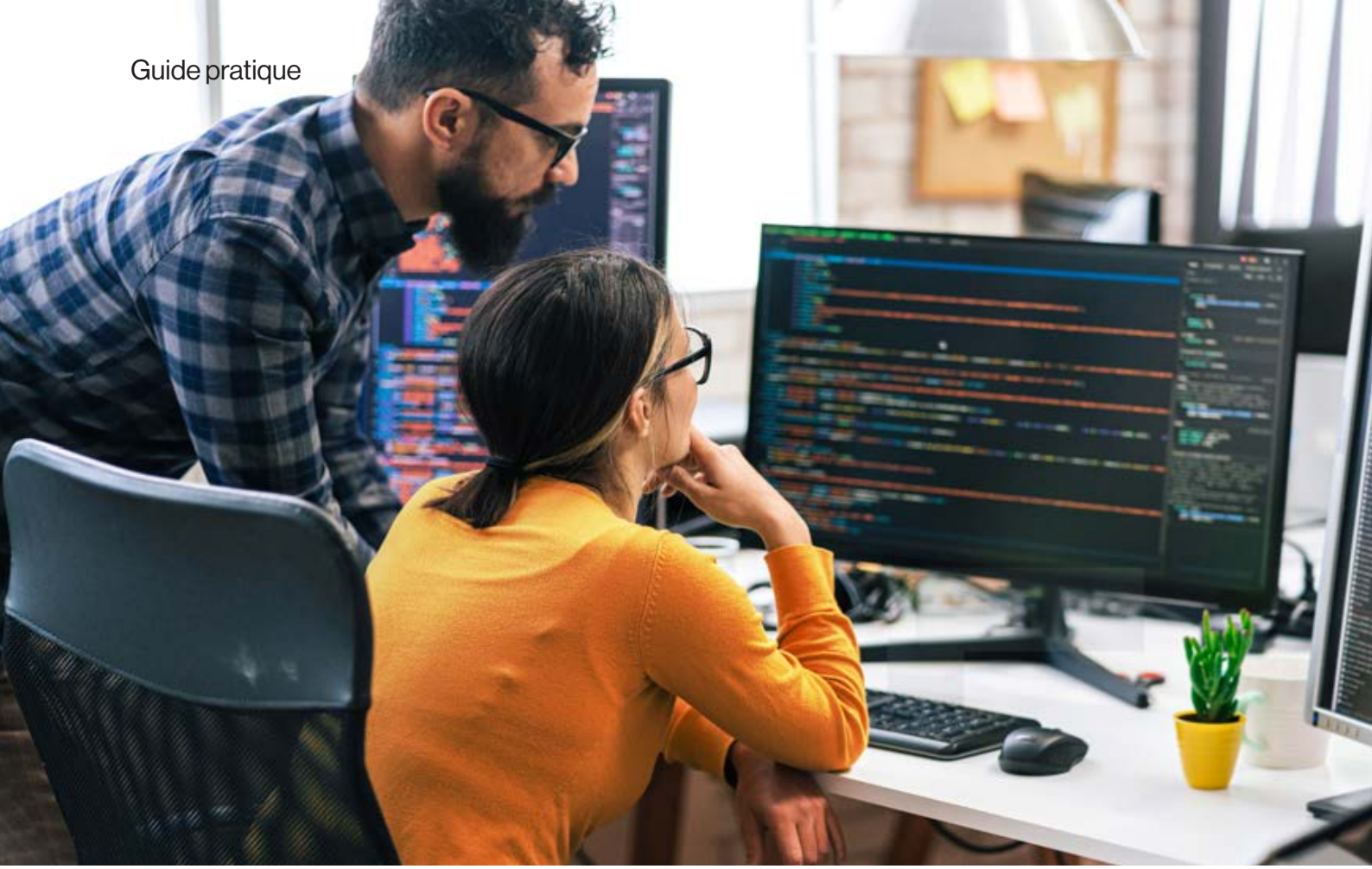
Guide pratique

Renforcer la cyber-résilience via une approche holistique

verizon business

Sommaire





Comment gagner en résilience face à la menace croissante des cyberattaques

Les acteurs cyber déploient aujourd'hui des menaces toujours plus nombreuses et sophistiquées. Pour lutter contre ces dangers, une perspective plus holistique s'impose.

En effet, à l'heure où l'innovation technologique s'accélère et où les entreprises de tous horizons sont plus connectées que jamais, le risque lié aux cybermenaces est omniprésent. Tandis que les cybercriminels mettent la barre toujours plus haut, les organisations s'appuient de plus en plus sur des outils et des processus numériques qui déplacent les données en masse vers le cloud. Résultat : leur surface d'attaque ne cesse de s'étendre.

Pour rester à l'abri, les entreprises ont besoin d'un programme de cybersécurité robuste, en phase avec leurs besoins et leurs exigences réglementaires spécifiques.

Intensification des cybermenaces

Le rapport Data Breach Investigations Report (DBIR) 2024[1] de Verizon Business a analysé :

30 458
incidents de sécurité réels

10 626
d'entre eux concernent des compromissions de données qui ont affecté des victimes dans

94
pays

Affronter la prolifération des menaces

Le rapport DBIR indique une nette augmentation des exploitations de vulnérabilités (en hausse de 180 % par rapport à l'année précédente), les applications web constituant le principal point d'entrée de ces attaques.

Près d'un tiers des incidents observés impliquent des ransomwares : une préoccupation toujours majeure pour 92 % des secteurs, car le coût d'une attaque peut être colossal. Selon les plaintes enregistrées par la cellule IC3 (Internet Crime Complaint Center) du FBI, les pertes médianes associées aux ransomwares et à d'autres techniques d'extorsion s'élèvent à 46 000 $ (dans une fourchette comprise entre 3 $ et 1 141 467 $ pour 95 % des cas)[2].

1, 2. Rapport DBIR (Data Breach Investigations Report) 2024. (non daté). Verizon Business. https://www.verizon.com/business/fr-fr/resources/reports/dbir/

Mais le volume croissant des menaces n'est pas le seul défi. En parallèle, les cybercriminels enrichissent leur arsenal pour créer des attaques plus sophistiquées, capables de neutraliser les dispositifs de sécurité et de prévention des pertes de données, tout en limitant l'efficacité des réglementations qui augmentent la diligence des entreprises. Dans son Panorama de la cybermenace 2022, l'ANSSI explique que : « Les acteurs malveillants poursuivent l'amélioration constante de leurs capacités à des fins de gain financier, d'espionnage et de déstabilisation. Cette amélioration s'illustre en particulier dans le ciblage des attaquants qui cherchent à obtenir des accès discrets et pérennes aux réseaux de leurs victimes[3]. »

Gérer la multiplication des vulnérabilités

Face à l'évolution de la technologie, des fonctionnalités réseau et des modes de travail, les entreprises doivent prendre conscience de la multitude de vulnérabilités que les cybercriminels peuvent exploiter. Selon Steven Gevers, Directeur associé, Cyber Defense Consulting Services chez Verizon Business : « L'essor du télétravail et des équipes hybrides est un élément clé qui redessine les contours de la sécurité des systèmes d'information. »

3. ANSSI (2022). PANORAMA DE LA CYBERMENACE 2022. https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf

Comme le souligne le DBIR, les compromissions imputables à des vulnérabilités ont triplé ces dernières années, principalement du fait d'attaques zero-day. Cela montre que les entreprises doivent reprendre les rênes de leur hygiène cyber et se recentrer sur des concepts clés tels que le Zero Trust et la défense en profondeur.

> Les entreprises ont besoin d'une vue consolidée des domaines qui l'exposent aux risques les plus graves, de façon à concentrer leurs investissements de sécurité là où ils seront le plus utiles.

Steven Gevers
Directeur associé, Security Consulting Services, Verizon Business

D'autres problèmes peuvent se manifester lorsque des collaborateurs décident de prendre eux-mêmes directement les choses en main. En effet, les utilisateurs ont désormais l'habitude de travailler à la vitesse du numérique. Un problème qui tarde à se résoudre les incite, parfois même de façon involontaire, à contourner les protocoles de sécurité et à utiliser des applications, des logiciels ou des équipements non autorisés et non sécurisés. Dans une étude de la Harvard Business Review, 67 % des professionnels interrogés admettent avoir déjà ignoré au moins une fois en partie les politiques de cybersécurité de leur entreprise[4]. Cette tendance au Shadow IT ouvre de nouvelles brèches potentielles dans lesquelles les groupes cyber s'empressent de s'engouffrer.

4. Verizon (2023). Mobile Security Index 2023 (livre blanc). https://www.verizon.com/business/resources/T19d/reports/mobile-security-index-report.pdf

Trouver une solution à la hauteur des enjeux

Face à la recrudescence des menaces, de nombreuses entreprises se tournent vers le Zero Trust et le SASE. Et bien que ces solutions soient efficaces pour renforcer la sécurité du réseau, il est important de prendre du recul afin de mieux en cerner les rouages.

« Les unités opérationnelles possèdent chacune leurs propres applications métiers. Et à processus uniques, besoins uniques », explique Stephen Young, Directeur, Cyber Defense Consulting Services chez Verizon Business. Il poursuit : « La sécurité repose sur des dynamiques multiples qui influent sur la capacité de l'environnement à lutter contre différents types d'attaques. La solution miracle n'existe pas. La résilience en matière de sécurité doit donc s'étendre au-delà du Zero Trust et du SASE. »

> La solution miracle n'existe pas. La résilience en matière de sécurité doit donc s'étendre au-delà du Zero Trust et du SASE.

Stephen Young
Directeur, Cyber Defense Consulting Services, Verizon Business

Maîtriser les fondamentaux

Parfois, les entreprises observent de si près les menaces les plus sérieuses qu'elles en perdent de vue les composants élémentaires de leur stratégie de sécurité. « Plus la situation est complexe et plus la menace est grande, plus les entreprises tendent à négliger les fondamentaux », note M. Young.

> Les principes de base déterminent la pertinence et l'efficacité des politiques de sécurité.
>
> **Stephen Young**
> Directeur, Cyber Defense Consulting, Verizon Business

Les entreprises doivent élargir leur vision pour prendre en compte la sécurité de leur infrastructure globale et apporter des réponses aux problèmes majeurs. Pour autant, il ne s'agit pas de faire l'impasse sur les étapes élémentaires, comme la mise à jour des systèmes et la configuration des pare-feu. En couvrant ces bases, les équipes IT empêchent l'intrusion des menaces les plus communes et évitent d'investir dans des outils de sécurité superflus.

Adopter une approche plus holistique

Devant le danger, les entreprises ont souvent le réflexe de multiplier les couches de sécurité supplémentaires. Seulement, cette approche peut en réalité devenir contreproductive, engendrant inutilement des coûts et de la complexité. Mieux vaut prendre de la hauteur pour déterminer les outils nécessaires, les lieux de déploiement stratégiques et pour quelles raisons. C'est pourquoi Verizon privilégie une approche plus holistique, fondée sur une compréhension approfondie des entreprises, de leur écosystème opérationnel aux besoins de leurs utilisateurs individuels.

Pour cela, Verizon suit les recommandations du framework de cybersécurité du NIST (National Institute of Standards in Technology), qui repose sur cinq piliers[5].

Verizon effectue des évaluations de sécurité approfondies pour cerner les besoins spécifiques des entreprises. Ensuite, nous les aidons à déployer des mesures de sécurité personnalisées en phase avec leurs exigences.

- Identification
- Protection
- Détection
- Réponse
- Reprise

5. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29 (rapport). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

> Chaque entreprise possède une culture distincte et sa propre appétence au risque. C'est pourquoi les approches de sécurité diffèrent.

Steven Gevers
Directeur associé, Security Consulting Services, Verizon Business

« Certaines entreprises considèrent que l'IA générative met en péril la propriété intellectuelle, et qu'il faut l'éviter à tout prix. D'autres estiment que cette technologie constitue un levier intéressant, à condition d'être bien encadrée. Nous aidons nos clients à améliorer la maturité de leur sécurité et à lutter contre les plus grandes menaces tout en respectant leurs besoins métiers. À ce titre, les entreprises doivent adopter une stratégie de défense en profondeur, en misant sur une panoplie de mesures de sécurité pour protéger leurs ressources. Elles peuvent ainsi bénéficier d'une certaine flexibilité, tout en gardant le risque sous contrôle : lorsqu'une composante de la sécurité est compromise, les suivantes prennent le relais pour bloquer l'attaque et en réduire l'impact ».

Munies de cette méthode, les entreprises peuvent bâtir une stratégie de sécurité IT robuste et gérer les coûts de manière plus efficace, en investissant dans des solutions réellement adaptées à leurs besoins. « Lorsque vous disposez d'une vision globale des besoins et que vous proposez des outils sur mesure, vous évitez la multiplication des solutions de sécurité redondantes, ce qui permet de mieux contrôler les coûts », conclut M. Young.

Grâce à cette approche de sécurité holistique, les entreprises peuvent trouver la solution idéale qui correspond à leurs besoins ainsi qu'à leur budget, et ainsi mieux se préparer à contrer les cybermenaces.

Découvrez comment les solutions de Verizon vous aident à éliminer les cybermenaces à l'aide d'une approche holistique taillée pour votre entreprise : verizon.com/business/fr-fr. Cliquez ici pour vous inscrire à notre newsletter et en savoir plus sur nos solutions SASE et de sécurité.

verizon business