Les menaces de sécurité ne respectent pas les horaires de bureau

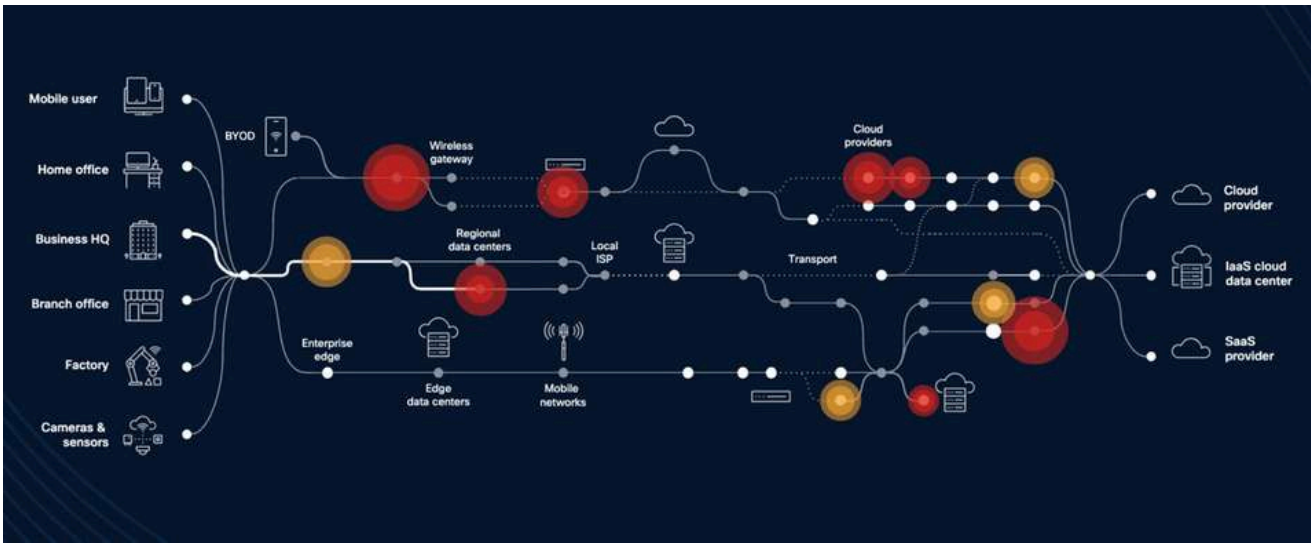
La surveillance de votre sécurité ne devrait pas non plus

Le monde du travail a changé, mais les lieux de travail ne se sont pas adaptés

Votre entreprise ne se limite plus à un seul bureau : elle se trouve partout où vous et votre équipe travaillez. Mais à mesure que vous ajoutez des appareils et des points d'accès à distance, assurer la sécurité de votre entreprise peut finir par ressembler à un travail à plein temps à part entière.

Vous ne devriez pas avoir à choisir entre sécurité et productivité. Gérer une douzaine d'outils de sécurité différents prend du temps, coûte cher et laisse souvent des failles que les pirates informatiques ne manquent pas de repérer. Vous avez besoin d'un moyen simple et fiable de protéger votre entreprise, sans entraver votre croissance ni ralentir vos collaborateurs.

Pour vous protéger contre les cybermenaces, les temps d'arrêt et les mauvaises expériences utilisateur, le besoin de visibilité et d'informations exploitables n'a jamais été aussi grand. Vous ne pouvez pas vous préparer pour l'avenir avec des solutions cloisonnées et une approche fragmentée de l'informatique ; la complexité engendre tout simplement trop de risques.



Ce dont vous avez besoin, c'est d'une sécurité qui protège vos données d'entreprise 24 h/24, 7 j/7 : une protection cohérente et une stratégie unifiée qui couvre tous les lieux où le travail s'effectue réellement.

Une sécurité unifiée et surveillée est essentielle pour un environnement de travail à l'épreuve du temps

Le travail et les risques se déplacent désormais partout, sur des appareils que vous ne gérez pas et des réseaux qui ne vous appartiennent pas. Les équipes sont débordées, jonglant entre les relais et réagissant trop tard lorsqu'une exposition se transforme en incident.

Quel est le défi ?

L'un des problèmes les plus difficiles à résoudre est le facteur humain : les utilisateurs et leurs appareils exposent l'entreprise. Lorsque les contrôles d'identité varient selon l'application ou le réseau, les utilisateurs trouvent des moyens de les contourner. Le facteur humain est à l'origine d'environ 60 % des violations[1] et 65 % des employés contournent les politiques de cybersécurité[2] dans les environnements hybrides.

En matière de protection sur site, les équipes peinent à colmater les failles de défenses déconnectées. Les solutions ponctuelles et les consoles supplémentaires créent des failles ; les équipes réduites passent leur journée à jongler entre les consoles et à être submergées par les alertes - une recette pour la dérive, la lenteur des réponses et les risques manqués.[3]

De plus, à mesure que l'utilisation du SaaS et du cloud se développe, la sécurisation des données transitant par le cloud devient plus complexe. Les données sensibles des employés ou des clients empruntent des chemins que vous n'avez pas prévus : 61 % des organisations ont signalé une violation dans le cloud au cours de l'année écoulée[4] et 75 % ont subi un incident de sécurité lié au SaaS.[5]

[1] Verizon — 2025 Data Breach Investigations Report (Executive Summary): human element ~60% of breaches.
[2] CyberArk — 2024 Employee Risk Survey: Harmful Employee Behaviors: 65% bypass policies in hybrid environments.
[3] 2024 SME Security Workload Impact Report: teams average 11+ tools; ~5 hours/day juggling them.
[4] Check Point & Cybersecurity Insiders — 2024 Cloud Security Report: 61% reported a cloud breach in the past year.
[5] AppOmni — State of SaaS Security 2025: 75% had a SaaS-related security incident in the last year.

Le défi : la complexité de la sécurité engendre trop de risques

68%

des entreprises disposent d'au moins 10 solutions ponctuelles dans leur infrastructure de sécurité ; 25 % en ont 30 ou plus.[1]

59%

des équipes de sécurité informatique déclarent consacrer trop de temps et d'efforts à la maintenance des outils et des workflows associés.[2]

80%

des entreprises admettent que la multiplicité des solutions ponctuelles ralentit leur capacité à détecter les incidents et à y répondre.[1]

54%

des entreprises ont subi un incident de cybersécurité au cours des 12 derniers mois ; pour la majorité d'entre elles, cela leur a coûté 300 000 dollars ou plus.[1]

78%

des équipes de sécurité informatique déclarent que leurs outils de sécurité sont dispersés et déconnectés.[2]

61%

des entreprises de taille moyenne estiment que la sécurité native du cloud n'est pas suffisante.[3]

Combler les lacunes en matière de sécurité

Il est facile de considérer la plupart de ces problèmes comme des lacunes à combler à l'aide de nouveaux outils ou de ressources supplémentaires. Mais le problème fondamental réside dans la fragmentation de la protection, des politiques et de la visibilité, ainsi que dans l'absence de surveillance - tant au niveau de ce qui vous appartient que de ce qui ne vous appartient pas -, ce qui rend difficile d'identifier les menaces, de prendre des décisions et d'agir de manière coordonnée.

1. Cisco Cybersecurity Readiness Index, April 2024;
2. Splunk, State of Security report, 2025;
3. Techaisle SMB and Midmarket Security Adoption Trends Report, 2024

Sans une approche unifiée et une surveillance active et continue de vos solutions de sécurité, il devient difficile d'identifier les menaces et d'y répondre rapidement. Pour protéger efficacement votre entreprise, vous devez consolider vos politiques de sécurité, bénéficier d'une visibilité totale sur vos chemins réseau et vous assurer que vos solutions de sécurité sont surveillées 24 h/24, 7 j/7. Cela vous permet de voir, de décider et d'agir en une seule fois, garantissant ainsi que votre entreprise reste protégée où que le travail soit effectué, à tout moment de la journée

D'une défense fragmentée à une posture unifiée

Pour de nombreuses petites et moyennes entreprises (PME), la gestion de la sécurité dans un environnement de travail hybride peut s'apparenter à un combat de titans. Lorsque les contrôles d'identité et des appareils manquent de cohérence, la sécurité devient un obstacle que les employés peuvent tenter de contourner. Au cours des 12 à 24 prochains mois, votre objectif devrait être de passer de ces défenses fragmentées et rigides à une posture de sécurité unifiée et « invisible » qui protège votre équipe sans la ralentir.

Offrez une expérience fluide qui réduit les risques pour l'entreprise

Des contrôles unifiés de l'identité, des accès et des terminaux facilitent l'adaptation des politiques

Les opérations de sécurité centralisées avec SSE et MFA intégrés réduisent les changements de console

Les informations sur les menaces optimisées par l'IA réduisent le temps, le coût et l'exposition aux attaques potentielles

La base : la surveillance comme point de départ

Avant d'ajouter de nouvelles couches de protection, il est essentiel d'établir une surveillance continue comme fondement de votre stratégie. Vous ne pouvez pas vous protéger contre des menaces que vous ne voyez pas. En maintenant une visibilité constante sur votre réseau et l'activité des utilisateurs, vous pouvez identifier les menaces en temps réel et prendre des décisions éclairées, transformant ainsi la sécurité d'une tâche réactive en un processus proactif et automatisé.

Une approche unifiée avec les solutions Cisco

Pour construire une base de sécurité résiliente, vous pouvez intégrer ces trois solutions clés afin de créer un modèle de protection homogène et « omniprésent » :

Cisco Umbrella
la première ligne de défense

Protégez vos utilisateurs quel que soit l'endroit d'où ils se connectent. Umbrella offre une sécurité au niveau de la couche DNS qui bloque les requêtes vers des domaines et des adresses IP malveillants avant même qu'une connexion ne soit établie, stoppant ainsi les menaces au stade le plus précoce possible.

Cisco Duo
sécurité axée sur l'identité

Allez au-delà des simples mots de passe. Duo garantit que l'accès est accordé en fonction du rôle de l'utilisateur, de l'état de santé de l'appareil et du contexte situationnel. Il agit comme une « ombre » au « privilège minimal » qui suit vos employés vers n'importe quelle application, garantissant que seuls les utilisateurs autorisés ont accès à vos données.

Cisco Secure Endpoint
protection des appareils

Vos terminaux constituent la ligne de front de votre entreprise. Secure Endpoint offre une protection avancée en détectant, prévenant et répondant aux menaces sophistiquées directement sur vos appareils, garantissant ainsi que même si une menace contourne les autres couches, l'appareil reste sécurisé.

L'avenir : une sécurité qui fonctionne pour vous

Conformité intégrée

La sécurité ne dépend plus du réseau ou de l'application que l'utilisateur utilise en premier ; elle est cohérente dans l'ensemble de votre entreprise.

Réduction des demandes d'assistance

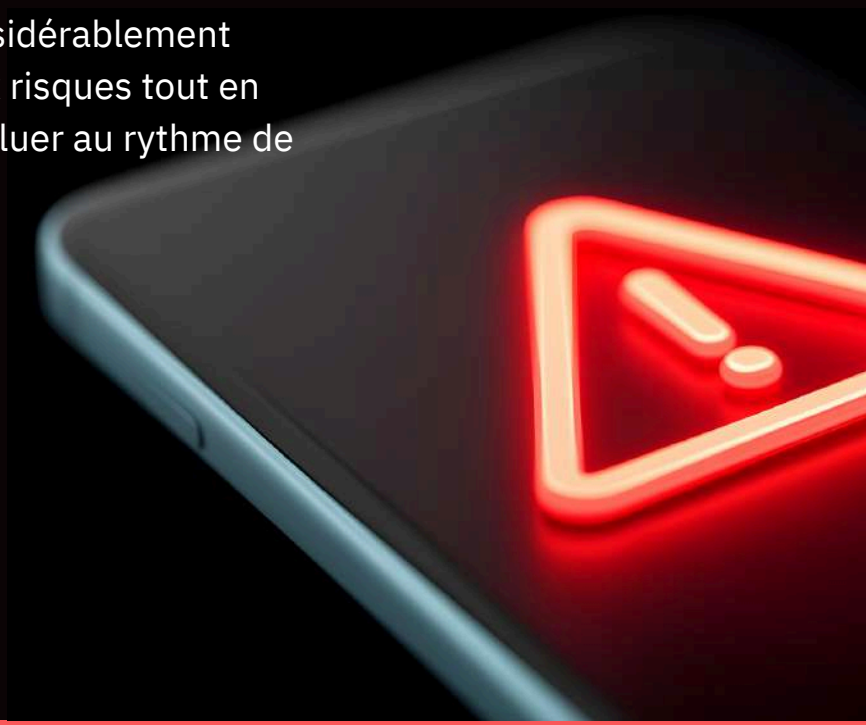
En automatisant les contrôles de sécurité et en vérifiant les identités de manière transparente, vous réduisez le volume de tickets d'assistance liés à la sécurité.

Autonomie accrue du personnel

Vos employés peuvent travailler de n'importe où, sur n'importe quel appareil, tout en restant dans leur « flux de travail » sans être interrompus par des protocoles de sécurité complexes.

Pourquoi c'est important :

En surveillant votre état de référence et en unifiant vos défenses grâce à Umbrella, Duo et Secure Endpoint, vous pouvez réduire considérablement l'exposition de votre entreprise aux risques tout en établissant une base capable d'évoluer au rythme de votre croissance.

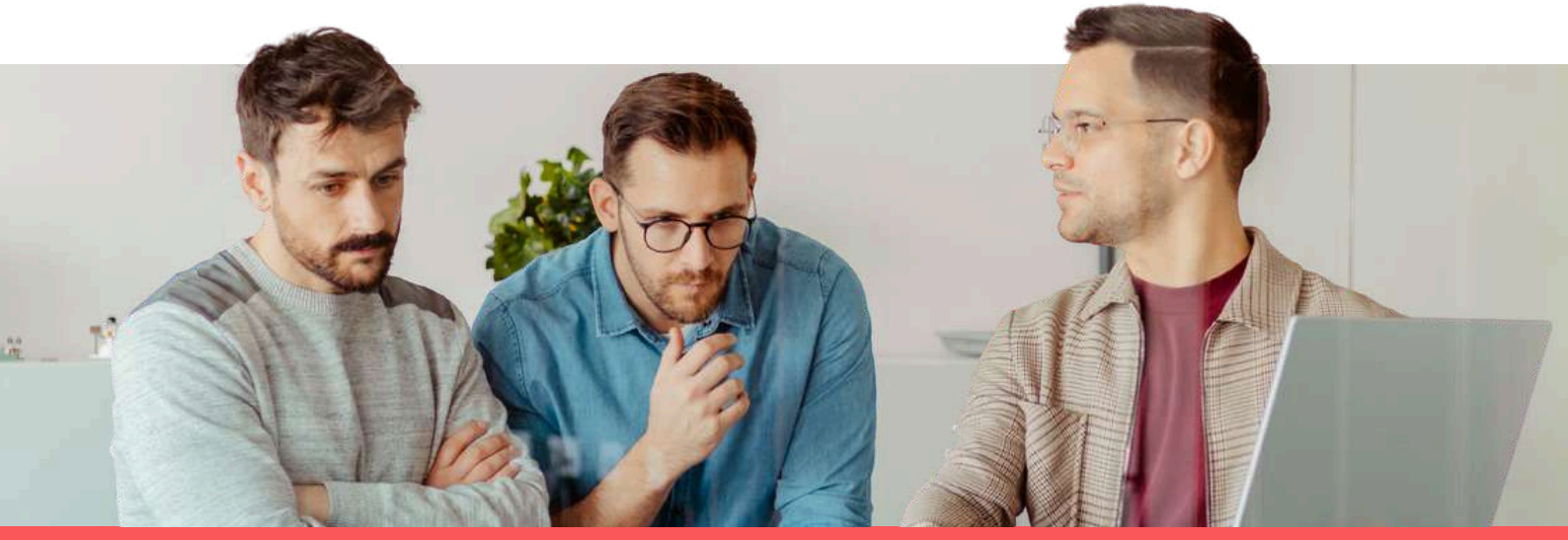


Ne vous laissez pas intimider par la complexité des outils et des opérations de sécurité ; nous nous en chargeons pour vous.

Alors que les enjeux en matière de cybersécurité sont extrêmement élevés, de nombreuses entreprises, en particulier les petites et moyennes, peinent à mettre en place une approche efficace de la sécurité. Elles achètent constamment de nouveaux outils de sécurité pour se protéger contre des modes d'attaque toujours plus nombreux, ce qui conduit à une multitude d'outils de sécurité. Par conséquent, les organisations ont du mal à gérer des ensembles d'outils fragmentés qui manquent de corrélation des données et de visibilité unifiée. Cette situation augmente les risques et fait grimper les coûts. Une étude récente de l'EMA a révélé que 45 % des entreprises considèrent la consolidation des outils comme un facteur prioritaire lorsqu'elles investissent dans des solutions de sécurité.

De plus, les entreprises ont du mal à recruter, à fidéliser et à former du personnel de sécurité, d'autant plus que les besoins augmentent et qu'il leur est toujours impossible d'assurer elles-mêmes la surveillance de ces solutions.

Les entreprises ont besoin de solutions qui répondent aux menaces de sécurité en constante évolution, consolident la prolifération des outils et comblent les lacunes en matière de compétences et de connaissances en cybersécurité. Une solution XDR gérée joue un rôle central pour relever ces défis.



EXTENDED DETECTION & RESPONSE

Qu'est-ce que le XDR ?

eXtended	Collecte et corrèle automatiquement les données télémétriques provenant de multiples outils de sécurité
Detection	Applique des analyses pour détecter les activités malveillantes
Response	Accélère la réponse aux menaces et la remédiation

Le XDR est une technologie de cybersécurité qui offre une corrélation et une automatisation de la sécurité inter-domaines. Il corrèle les données issues de l'ensemble des outils de cybersécurité en collectant des données télémétriques provenant à la fois de points de contrôle de sécurité natifs et tiers. La technologie XDR intègre généralement les données issues des technologies de sécurité suivantes : solutions de gestion des identités et des accès, sécurité des e-mails, pare-feu, solutions de détection d'intrusion, détection et réponse réseau (NDR) et détection et réponse au niveau des terminaux (EDR).

La plateforme enrichit et corrèle les données qu'elle collecte à partir de divers systèmes afin de permettre une analyse efficace et performante. Les solutions XDR intègrent l'analyse des données, les renseignements sur les menaces, le contexte des actifs et des utilisateurs, ainsi que le cadre MITRE ATT&CK pour détecter et interpréter les activités malveillantes.

Une solution XDR efficace permet des opérations de sécurité performantes en rationalisant les enquêtes pour un délai de résolution accéléré. Les solutions XDR génèrent des incidents classés par priorité qui aident le personnel de sécurité à se concentrer sur les menaces les plus préjudiciables à l'entreprise. Elles offrent également des workflows automatisés que les analystes peuvent exécuter efficacement pour le confinement et la correction des activités malveillantes.

Cas d'utilisation critiques de l'XDR

EMA a interrogé les utilisateurs de solutions XDR afin d'identifier leurs principaux cas d'utilisation de cette technologie.

1 Amélioration de la détection des menaces avancées (61 %)

Le XDR aide les entreprises à détecter les attaques sophistiquées en réduisant le bruit des alertes. Dans les architectures de sécurité traditionnelles, un seul incident cybernétique peut déclencher des alertes provenant de plusieurs outils. Le XDR élimine ce bruit en consolidant les alertes connexes en un seul incident exploitable que les équipes de sécurité peuvent traiter rapidement. Cette capacité est particulièrement utile pour détecter des menaces complexes telles que les ransomwares. En effet, 29 % des entreprises ont déclaré à l'EMA que le XDR faisait partie de leur stratégie de lutte contre les ransomwares, et beaucoup ont indiqué que le XDR les avait aidées à détecter plus rapidement les attaques de ransomware.

---

2 Visualisation simplifiée des attaques complexes (22 %)

Les plateformes XDR incluent des visualisations de la progression d'une attaque, basées sur les multiples points de vue à partir desquels les solutions XDR collectent des données. Cette visualisation aide les analystes de sécurité à comprendre rapidement la nature et l'ampleur d'une attaque.

---

3 Consolidation des outils (11 %)

Certaines entreprises voient dans le XDR une opportunité de rationaliser leur infrastructure de sécurité. Au lieu d'intégrer leurs outils de sécurité existants à la plateforme XDR, elles choisissent de les remplacer par les contrôles de sécurité et les analyses natifs de la plateforme. Cette approche permet non seulement de réduire les coûts, mais aussi de diminuer les frais généraux opérationnels, rendant ainsi la gestion de la sécurité plus simple et plus efficace.

---

[1] EMA, "Why Should Organizations Consider Extended Detection and Response?" July 2023.

Pourquoi votre entreprise a besoin d'un service XDR géré

Le XDR est une solution puissante, mais toutes les entreprises ne sont pas en mesure de l'exploiter efficacement. Bien que le XDR offre des capacités d'analyse et d'automatisation puissantes, cette technologie nécessite un niveau minimal d'expertise et de connaissances de la part des analystes SOC pour fonctionner efficacement. Aujourd'hui, la plupart des entreprises peinent à recruter du personnel possédant les compétences requises. Elles font plutôt appel à des équipes informatiques composées de généralistes qui ne disposent pas de la spécialisation nécessaire pour exploiter correctement une solution XDR.

La pénurie d'expertise en sécurité dans de nombreuses équipes informatiques devient de plus en plus risquée, car les cybercriminels se tournent vers les petites entreprises. L'automatisation et l'IA ont permis aux acteurs malveillants, y compris aux attaquants soutenus par des États, de cibler plus facilement les petites entreprises et certains secteurs spécifiques. Auparavant, les petites entreprises bénéficiaient d'une relative obscurité, car le coût de les cibler était plus élevé que le gain potentiel. Cependant, l'automatisation et l'IA réduisant le coût des attaques, les petites entreprises constituent désormais des cibles plus attrayantes.

Si ces entreprises doivent renforcer leur posture de sécurité, elles manquent souvent du personnel et des capacités organisationnelles nécessaires. Une solution gérée peut aider à combler ces lacunes, en répondant aux défis en matière de personnel et de ressources auxquels les petites entreprises sont confrontées aujourd’hui.

Avec une solution XDR gérée, vous bénéficiez non seulement d’une équipe de professionnels de la sécurité hautement qualifiés travaillant 24 heures sur 24 et 7 jours sur 7, mais vous recevez également des conseils sur les failles de sécurité de votre entreprise et les mesures à prendre pour protéger vos données et votre réputation.

Renforcer la puissance des services de sécurité gérés existants

Une solution XDR gérée peut renforcer l'efficacité des autres services gérés qu'une entreprise utilise déjà. Par exemple, les MSP qui supervisent les pare-feu et l'infrastructure réseau d'une entreprise peuvent ajouter une solution XDR intégrée à ces services. Le XDR géré offre une intégration plus poussée, permettant une meilleure orchestration de la sécurité et l'accès à un ensemble de données plus complet à partir des solutions de sécurité gérées existantes. Cette approche rationalisée permet une réponse automatisée aux incidents, en orchestrant les changements à travers d'autres services gérés pour isoler ou bloquer efficacement les menaces.

De plus, un service XDR géré aide les entreprises à tirer le meilleur parti de leurs ressources internes. Grâce aux conseils d'experts des fournisseurs de services gérés, les généralistes informatiques reçoivent des informations exploitables pour mieux protéger l'entreprise. Les services XDR gérés offrent également une flexibilité financière, car les entreprises ne paient que ce dont elles ont besoin, quand elles en ont besoin. Ils soutiennent la transformation numérique en gérant l'approvisionnement, les opérations et les ajustements continus de la plateforme XDR. À mesure que les entreprises adoptent le cloud et les technologies définies par logiciel, le MSP assure une protection de bout en bout tout au long du parcours de transformation.

zenconnect

Fondée en 2012, Zenconnect est spécialisée dans l'intégration de réseaux informatiques, WiFi, télécom & SD-WAN, cybersécurité, IoT, et Cloud.

Zenconnect accompagne ses clients dans leurs projets de modernisation et digitalisation, afin qu'ils puissent se concentrer sur leurs métiers, baisser leurs coûts en rationalisant leur IT, et augmenter leur volant d'affaires grâce à des solutions innovantes. Les solutions et services de Zenconnect sont destinés à tous les secteurs d'activité, en tête desquels on peut citer les secteurs Franchises / Retail, Industrie & Transports, Tertiaire, French Tech, Enseignement, et Collectivités.

zenconnect.fr