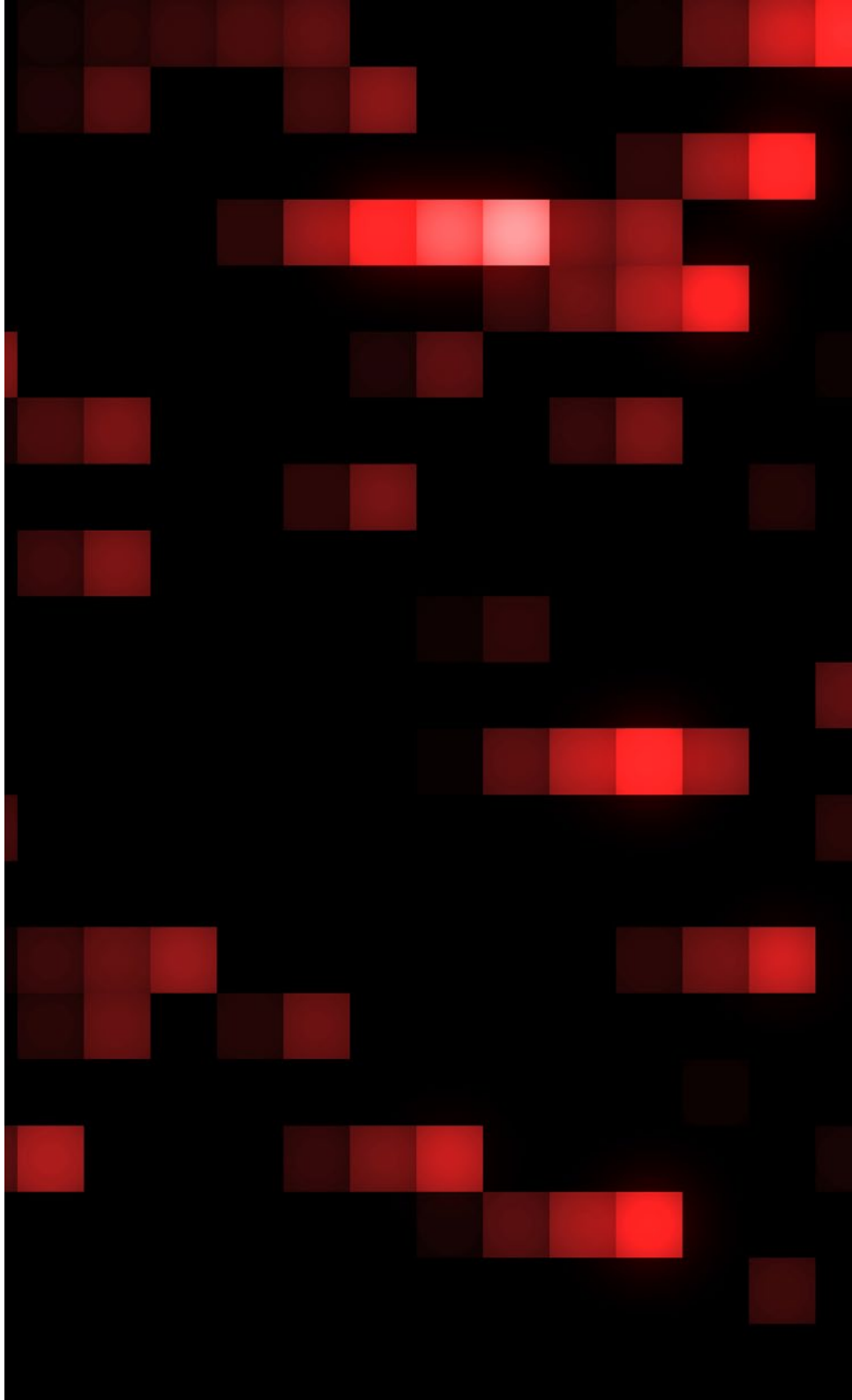
WATCHGUARD THREATSYNC®

Accéder à l'univers du XDR

Guide pour une sécurité moderne pleinement exploitée

WatchGuard®

SOMMAIRE



01 Principaux enjeux actuels liés à la cybersécurité

Les organisations de toutes tailles s'efforcent de lutter contre l'univers de plus en plus complexe de la cybersécurité. Les acteurs des menaces ne s'en prennent pas seulement aux grandes entreprises ; ils ciblent agressivement les petites et moyennes entreprises avec des cyberattaques sophistiquées.

Les entreprises ne peuvent pas se permettre de fermer les yeux et de maintenir le statu quo en matière de sécurité. Les acteurs des menaces et leurs techniques évoluent rapidement. Votre réponse se doit donc d'être à la hauteur pour protéger vos environnements, vos appareils, vos utilisateurs et vos données. Par conséquent, vous devez adopter des solutions de sécurité qui peuvent s'adapter et évoluer au rythme de votre entreprise et de la croissance de sa surface de menace.

F12.net™

« La cybersécurité n'est pas une destination, c'est un voyage – tout simplement parce qu'elle évolue constamment »

Calvin Engen
Chief Technology Officer chez F12.net

Quels sont les principaux enjeux actuels liés à la cybersécurité ?

Sécurité cloisonnée

Les équipes de sécurité sont chargées de gérer et de protéger un nombre toujours croissant de vecteurs de menaces sur les réseaux d'entreprise, les endpoints et les identités de leurs clients. Compte tenu de la multiplicité des vulnérabilités en jeu et du large éventail de cyberattaques potentielles à détecter, il est logique de mettre en place un large éventail de solutions de sécurité. Cependant, un large arsenal d'outils peut être une arme à double tranchant si chaque solution fonctionne indépendamment des autres. Augmenter le nombre de produits de sécurité ne renforce pas systématiquement le niveau de sécurité global.[1]

Un large arsenal d'outils peut être une arme à double tranchant si chaque solution fonctionne indépendamment des autres.

[1] Rapport Panaseer 2022 Security Leaders Peer

19 %

Le nombre d'outils de sécurité utilisés par les entreprises a augmenté de 19 % au cours des deux dernières années

36 %

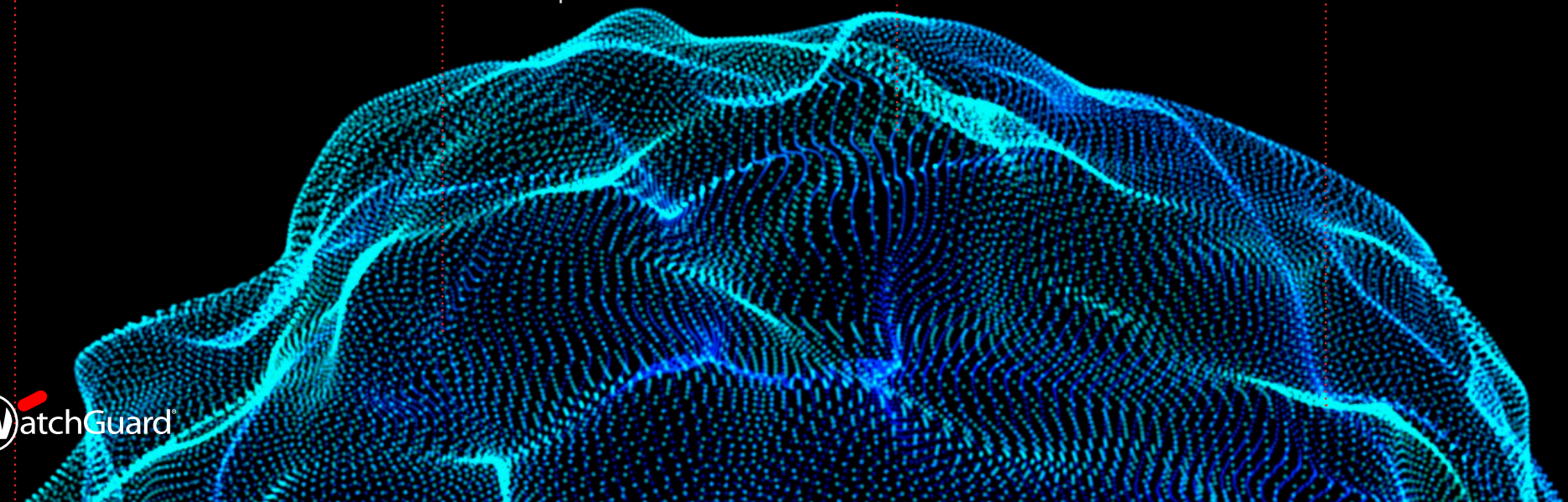
Seulement 36 % des entreprises se disent « très confiantes » lorsqu'il s'agit de s'assurer que les contrôles fonctionnent comme prévu

64 À 76

Le nombre d'outils de sécurité utilisé par les grandes entreprises est passé de 64 à 76 en moyenne

82 %

De plus, 82 % déclarent avoir été surpris par des incidents de sécurité qui ont échappé aux outils existants



WatchGuard®

Manque de visibilité

Tous ces outils cloisonnés compliquent également le développement d'une vision globale sur votre posture en matière de sécurité. Chaque outil ne fournit qu'une vue limitée sur son propre domaine de spécialité. Tous ces éléments constituent un ensemble de pièces de puzzle que vous devez classer manuellement et essayer de rassembler en une image complète.

Pire encore, en cas de cyberattaque active, le processus consistant à assembler les pièces du puzzle fait perdre un temps précieux. Si vos administrateurs de sécurité doivent se connecter à plusieurs consoles et basculer entre une demi-douzaine d'outils différents juste pour déterminer ce qui pourrait se passer, les acteurs de la menace ont déjà un avantage considérable lors du lancement de leur attaque.

> Les administrateurs de sécurité doivent briser ces cloisons pour récupérer ce temps perdu et avoir une chance de faire face à l'évolution rapide des cyberattaques.

Cependant, à moins que ces outils ne soient mis en œuvre par le même fournisseur, les solutions axées sur différents domaines de sécurité fourniront rarement l'interopérabilité requise pour une protection efficace.

Problèmes de données corrélées et contextuelles

Tous les produits de sécurité, tels que les solutions réseau et de sécurité des endpoints, les firewalls ou les outils de protection de l'identité présentent les logs, la télémétrie et les alertes de différentes façons ; ils ont chacun un format et une fréquence qui leur est propre.

En outre, la gestion manuelle de l'énorme volume de données de sécurité recueillies par ces produits peut s'avérer fastidieuse et il est complexe de les combiner et de les analyser. Il est facile de passer à côté d'indicateurs de menace importants ou de s'enliser avec de faux positifs si vous vous noyez dans des données générées par plusieurs produits disparates. Cela conduit finalement à des menaces négligées qui mettent toute l'entreprise en danger.

L'intégration de plusieurs produits de sécurité de différents fournisseurs peut être compliquée et prendre beaucoup de temps, et nécessite des connaissances et une expertise spécialisées. Même lorsque ces produits sont intégrés avec succès, leur gestion peut encore s'avérer difficile, surtout lorsqu'il s'agit de gérer des environnements informatiques complexes et diversifiés.

Manque d'automatisation de la sécurité

Vos utilisateurs vous font confiance pour protéger leurs données et les ressources de leur entreprise. Sans automatisation, la détection et la réponse aux incidents de sécurité peuvent être lentes et inefficaces, augmentant ainsi le risque de compromission des réseaux, des endpoints et des utilisateurs, sans oublier les coûts et les atteintes à la réputation consécutifs à des violations de données.

1. **Temps de détection lents et prolongés**
   Sans détection automatisée, les équipes de sécurité doivent s'appuyer sur des processus manuels qui ont un impact significatif sur le temps moyen de détection (MTTD), laissent passer des menaces, déclenchent de faux positifs et retardent les temps de réponse aux incidents. Ce retard dans la détection des menaces de sécurité peut amener vos administrateurs de sécurité à manquer des menaces critiques et à mener des enquêtes inutiles sur les alertes de bas niveau, entraînant ainsi une augmentation des coûts et laissant la porte ouverte à des violations potentielles.

2. **Manque de clarté sur les mesures d'intervention appropriées**
   Comment les administrateurs de la sécurité choisissent-ils la mesure d'intervention à prendre en premier ?

Lorsque vous êtes victime d'un incident de sécurité, la rapidité et la précision de la réponse peuvent faire toute la différence en matière d'impact et de portée de l'attaque. Cependant, sans fonctionnalités de réponse automatisées, il peut être difficile de savoir quelle action de réponse résoudra la menace et réduira le temps moyen de réponse (MTTR).

Le temps est précieux ; des temps de détection lents et des actions de réponse inexactes peuvent faciliter la propagation de l'attaque à travers l'entreprise et peuvent souvent entraîner des interruptions d'activité prolongées et une perte de données. L'automatisation de la sécurité assure des services constants et efficaces à grande échelle.

L'automatisation de la sécurité peut vous aider à fournir des services de sécurité cohérents et efficaces pour plusieurs clients et à maintenir un niveau de sécurité standard pour tous.

Complexité de la sécurité et équipes de sécurité informatique surchargées

À mesure que les technologies progressent, les environnements informatiques deviennent plus complexes. Ainsi, de nombreux systèmes, applications et périphériques nécessitent un monitoring et une maintenance constants pour assurer la sécurité. Par ailleurs, des menaces sophistiquées continuent d'apparaître rapidement, intensifiant ainsi la nécessité de suivre le rythme.

Les entreprises doivent constamment rechercher de nouveaux niveaux d'agrégation, de corrélation et d'analyse de la télémétrie de sécurité, ce qui vient s'ajouter à la charge de travail déjà importante de leur personnel. Les administrateurs doivent faire face à un déluge constant et croissant d'alertes, et protéger une surface d'attaque de plus en plus diversifiée dans laquelle les menaces sont devenues plus difficiles à détecter.

1 **Pénurie de professionnels qualifiés en cybersécurité**
Le recrutement et le maintien en poste de personnel qualifié et compétent deviennent de plus en plus difficiles en raison de la demande croissante de professionnels hautement qualifiés dans le domaine. Dans ce contexte, il se peut que vous ayez du mal à gérer un large éventail de solutions de sécurité spécialisées et à trouver le temps nécessaire pour identifier les menaces.

2 **Fatigue due aux alertes**
Généralement, la plupart des professionnels de la sécurité sont confrontés à des milliers d'alertes hebdomadaires de malware, dont seulement 19 % sont considérées comme fiables et seulement 4 % font l'objet d'une enquête. De plus, certaines solutions de sécurité traditionnelles, loin de résoudre des cas d'utilisation spécifiques, créent plus de stress et augmentent la charge de travail en déléguant la responsabilité de la gestion des alertes et en forçant la classification manuelle des menaces.

Le recrutement et le maintien en poste de personnel qualifié et compétent deviennent de plus en plus difficiles en raison de la demande croissante de professionnels hautement qualifiés dans le domaine.

Zoom sur les pièges des approches de sécurité des produits

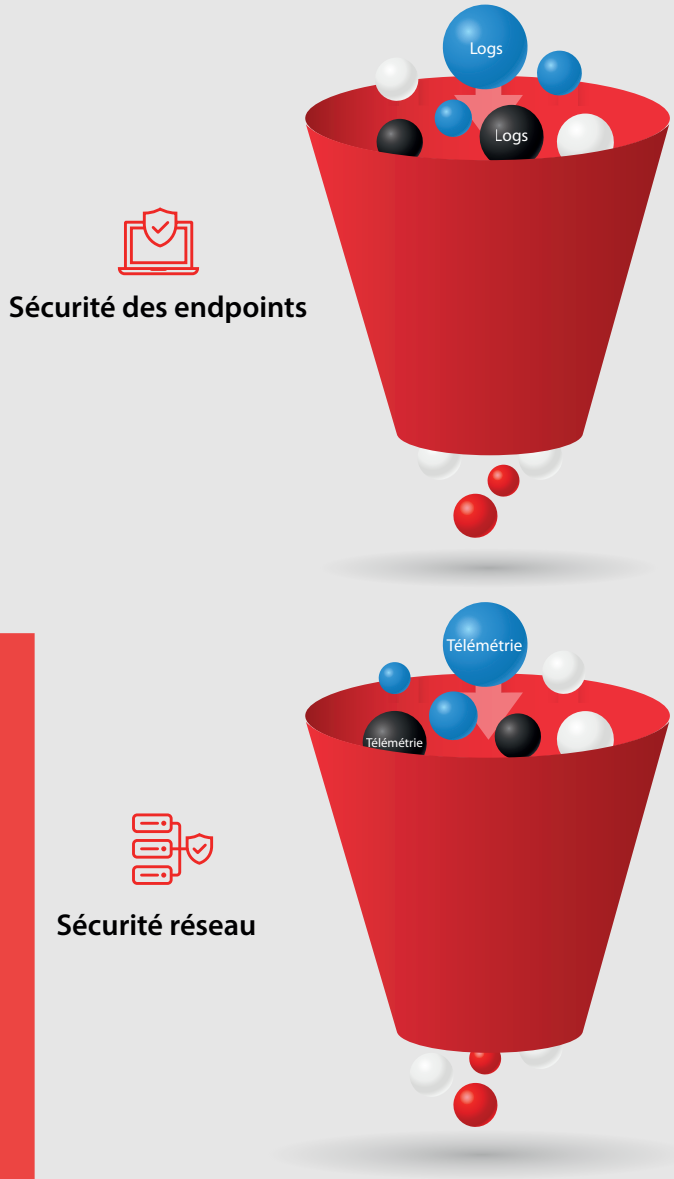
La détection et la réponse au niveau des endpoints (EDR) et les solutions de sécurité réseau sont deux éléments essentiels d'une stratégie de cybersécurité moderne. Ces outils vous aident à identifier, à détecter et à répondre aux menaces sophistiquées contre les domaines critiques.

Bien que les solutions de sécurité réseau et EDR appropriées soient très efficaces lorsqu'il s'agit de détecter et de répondre aux menaces sophistiquées, elles offrent également une visibilité sur des domaines spécifiques de l'infrastructure informatique. Les outils de sécurité réseau, tels que les firewalls et les systèmes de détection d'intrusion, fonctionnent sur un modèle centré sur le périmètre du réseau et ne fournissent tout simplement pas une visibilité suffisante sur les endpoints. Ils se concentrent sur la protection des points d'entrée et de sortie du réseau et la surveillance du trafic à la périphérie du réseau. Cependant, avec la montée d'un modèle de travail hybride, le périmètre du réseau est devenu de plus en plus poreux, ce qui rend plus difficile le maintien d'une sécurité efficace.

De même, les solutions EDR sont devenues des outils essentiels dans la bataille en matière de détection et de réponse aux menaces au niveau des endpoints. Toutefois, ces solutions à elles seules ne peuvent pas assurer de visibilité sur les menaces qui se produisent dans les environnements réseau de votre entreprise.

En conséquence, de nombreuses entreprises sont souvent obligés d'utiliser un ensemble de produits de sécurité disparates pour détecter les menaces sur plusieurs couches de sécurité. Cette approche fragmentée génère des angles morts, vos solutions de sécurité fonctionnant indépendamment les unes des autres. Elle limite la visibilité, les résultats contextuels et l'efficacité de la détection et de la réponse, rendant presque impossible la protection complète de bout en bout des clients.

Vous n'êtes probablement que trop familier avec ces enjeux. Cela fait bien longtemps que les responsables de la sécurité font face à ces enjeux. La vérité est que la plupart de ces obstacles sont simplement la conséquence d'approches obsolètes de la sécurité. Pour les surmonter, il convient de changer de cap et d'envisager une nouvelle approche en matière de sécurité.



02 XDR : votre passerelle vers la sécurité moderne

Pour relever ces défis, il vous faut une approche intégrée qui fournit une corrélation de données contextuelles et de télémétrie sur plusieurs couches de sécurité et domaines informatiques.

> Grâce à des solutions de sécurité plus étroitement intégrées, vous bénéficiez d'une vue d'ensemble de l'état de votre sécurité.

Une approche intégrée moderne de la cybersécurité qui inclut des fonctionnalités de détection et de réponse étendues (XDR) avec des technologies d'automatisation et d'Intelligence Artificielle, peut améliorer considérablement l'efficacité de la sécurité contre les menaces sophistiquées tout en simplifiant les opérations de sécurité.

Comment fonctionne la technologie XDR ?

Nous vivons dans une réalité où les cyberattaques sont plus la règle que l'exception, et rien ne pourrait causer plus de ravages que la matérialisation de ces menaces. Avec des experts aux prises avec des attaques persistantes et en évolution et de multiples systèmes et outils à prendre en charge, le moment est venu de proposer une solution complète de détection et de réponse aux menaces qui offre aux MSP des perspectives inédites. XDR est la solution.

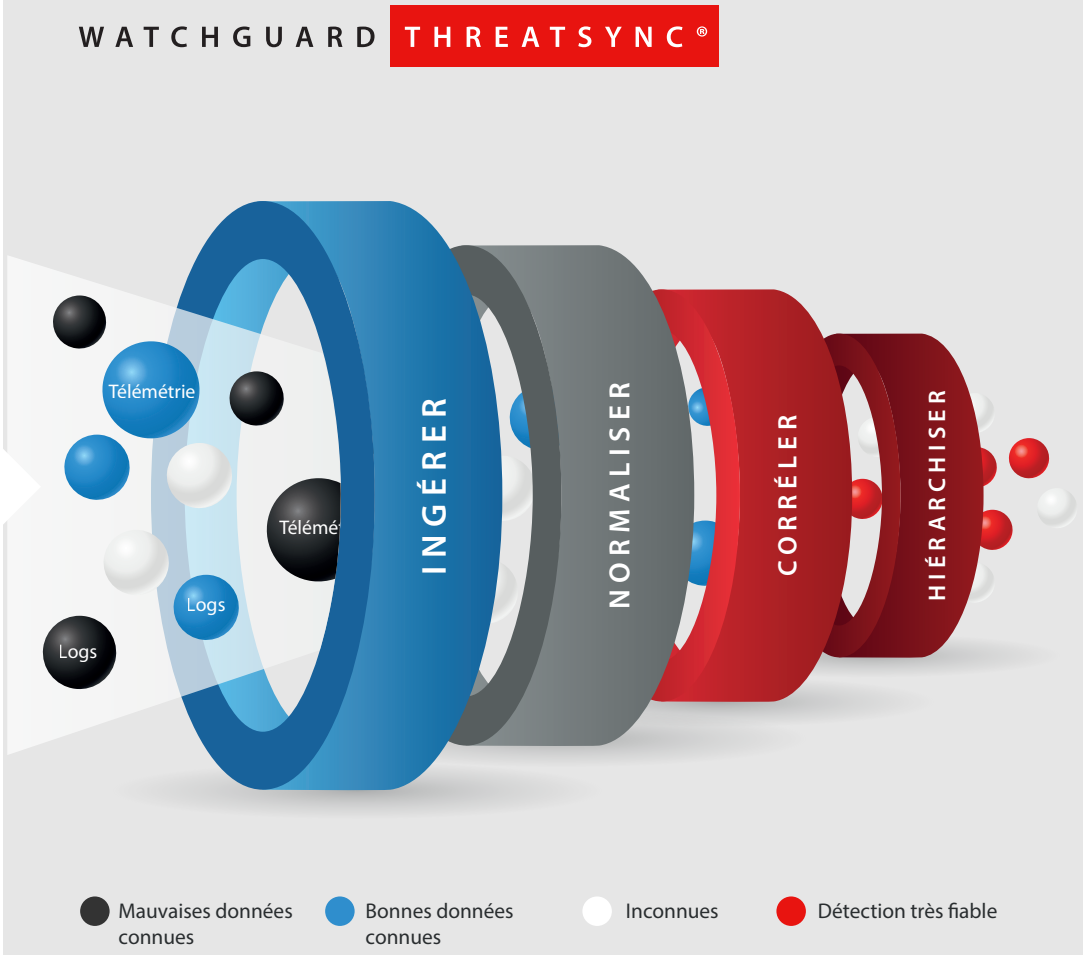
XDR offre des avantages considérables par rapport aux outils de sécurité déconnectés. Il offre le contexte et la visibilité nécessaires pour identifier les cyberattaques et y remédier avec une rapidité et une efficacité accrues. XDR offre une approche de sécurité complète qui exploite les technologies d'automatisation et d'Intelligence Artificielle pour détecter et répondre aux menaces sur les firewalls, les serveurs, les postes de travail et les appareils.

> Une solution XDR intégrée peut optimiser les opérations de sécurité, réduire les coûts opérationnels et vous aider à obtenir une posture globale plus robuste en matière de sécurité.

Sécurité des endpoints

XDR

Sécurité réseau



03 Accédez à l'univers du XDR et libérez tout le potentiel d'une sécurité unifiée

Nous proposons une solution XDR complète et intuitive avec ThreatSync, une couche centrale au sein de l'architecture Unified Security Platform® de WatchGuard. Nous pouvons ainsi unifier les détections multiproduits et remédier plus rapidement aux menaces depuis une interface unique.

eXtend, Detect, and Respond avec ThreatSync

1 eXtend

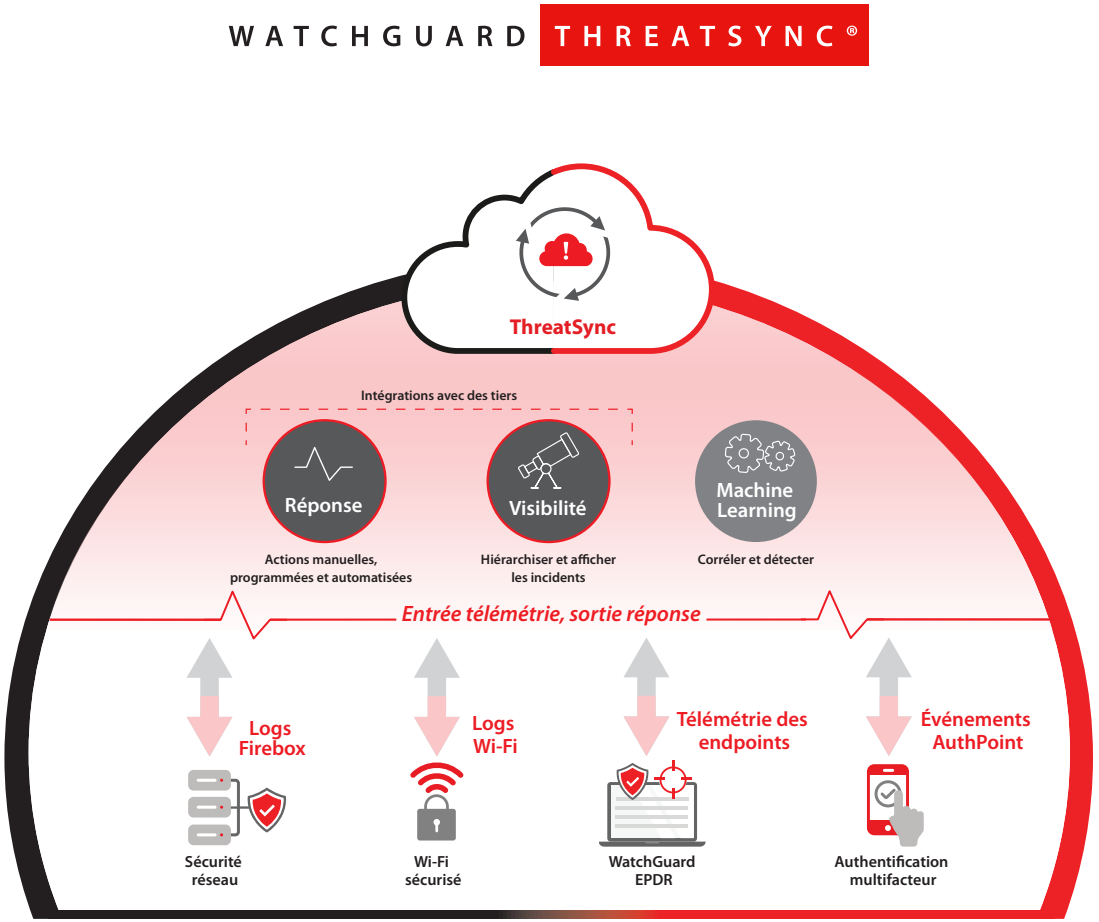
Nous mettons en œuvre le XDR avec des intégrations étroites et la télémétrie de données inter-domaines des technologies de dernière génération de WatchGuard. En élargissant la gamme des flux de données pour inclure la veille sur les réseaux, les endpoints et les utilisateurs, nous renforçons la visibilité et la protection.

2 Detect

Dites adieu aux approches de sécurité cloisonnées qui ralentissent la détection et laissent passer des attaques. Grâce aux fonctionnalités de l'Intelligence Artificielle et du Machine Learning de ThreatSync, nous identifions les menaces potentielles en temps réel dans différents domaines afin de réduire les délais de détection et d'exécuter un confinement rapide.

3 Respond

XDR permet d'accélérer les temps de réponse et d'améliorer la sécurité de votre entreprise. Grâce à ThreatSync, nous orchestrons des actions de réponse automatisées pour neutraliser les menaces qui visent votre entreprise, et ce de manière simple, rapide et plus précise.



* Le Wi-Fi sécurisé et AuthPoint seront bientôt disponibles et intégrés à ThreatSync.

La puissance de la technologie XDR en toute simplicité

Détection des menaces sur plusieurs plateformes

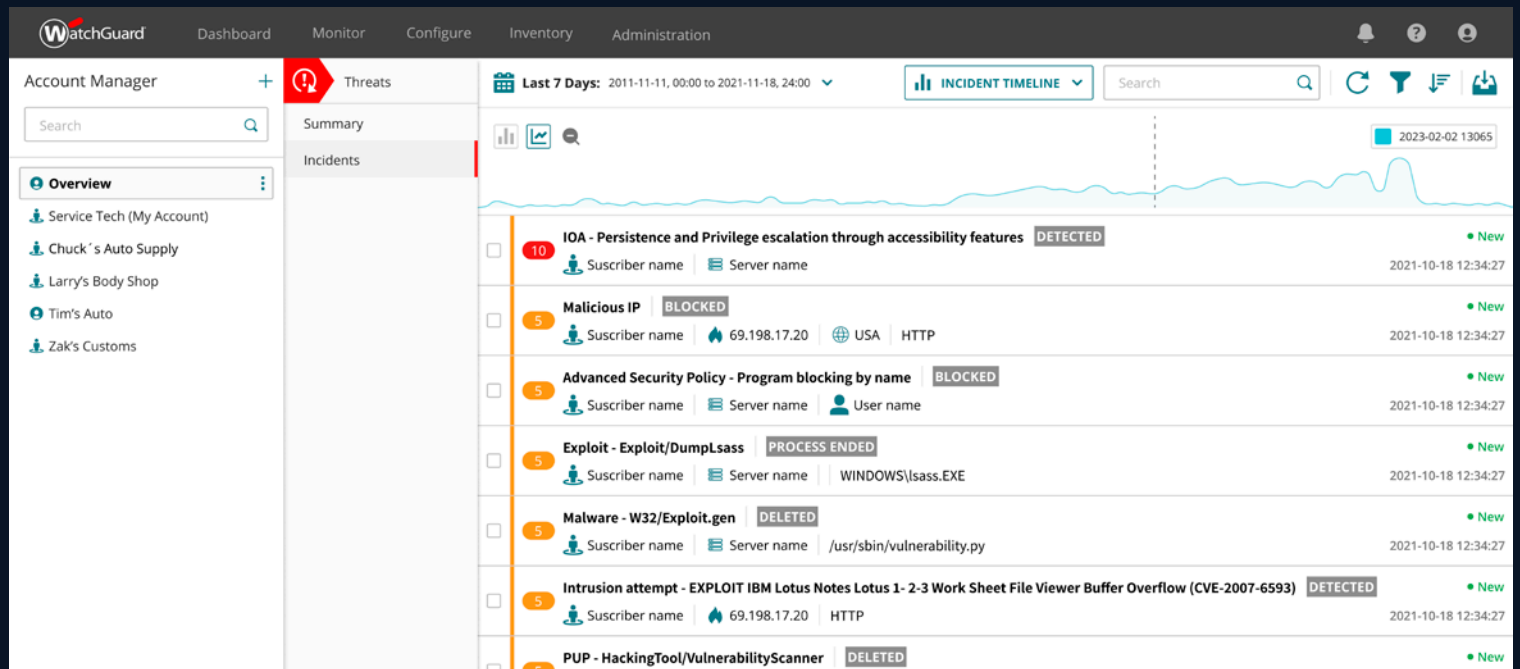
ThreatSync propose des fonctionnalités de détection étendues en corrélant les indicateurs de compromission (IoC) de tous les produits de sécurité WatchGuard. Cette corrélation entre les domaines et le contexte permettent à la solution de détecter et de noter les activités potentiellement malveillantes liées à des environnements, des utilisateurs et des appareils spécifiques afin de réduire le temps moyen de détection (MTTD), d'améliorer la précision et de permettre une remédiation plus rapide.

Orchestration de la sécurité et réponse aux menaces unifiées

XDR offre une vue d'ensemble de votre surface de menace, ce qui facilite l'identification et la hiérarchisation des problèmes et favorise une réponse fiable et rapide. ThreatSync permet de travailler plus efficacement grâce à la notation intelligente des alertes, aux stratégies de remédiation automatisées et aux options d'intervention manuelle selon les besoins. Ce niveau d'orchestration de la réponse aux menaces augmente à la fois la précision et le champ d'action.

Simplicité de déploiement et de gestion

ThreatSync facilite l'adoption d'une approche XDR grâce à ses capacités intuitives de gestion et d'automatisation dans le Cloud. En tant que couche XDR robuste de l'architecture Unified Security Platform® de WatchGuard, ThreatSync intègre la veille multiproduit afin de réduire les coûts et la charge de la gestion liés au déploiement de solutions à points multiples pour la détection et la réponse aux menaces.

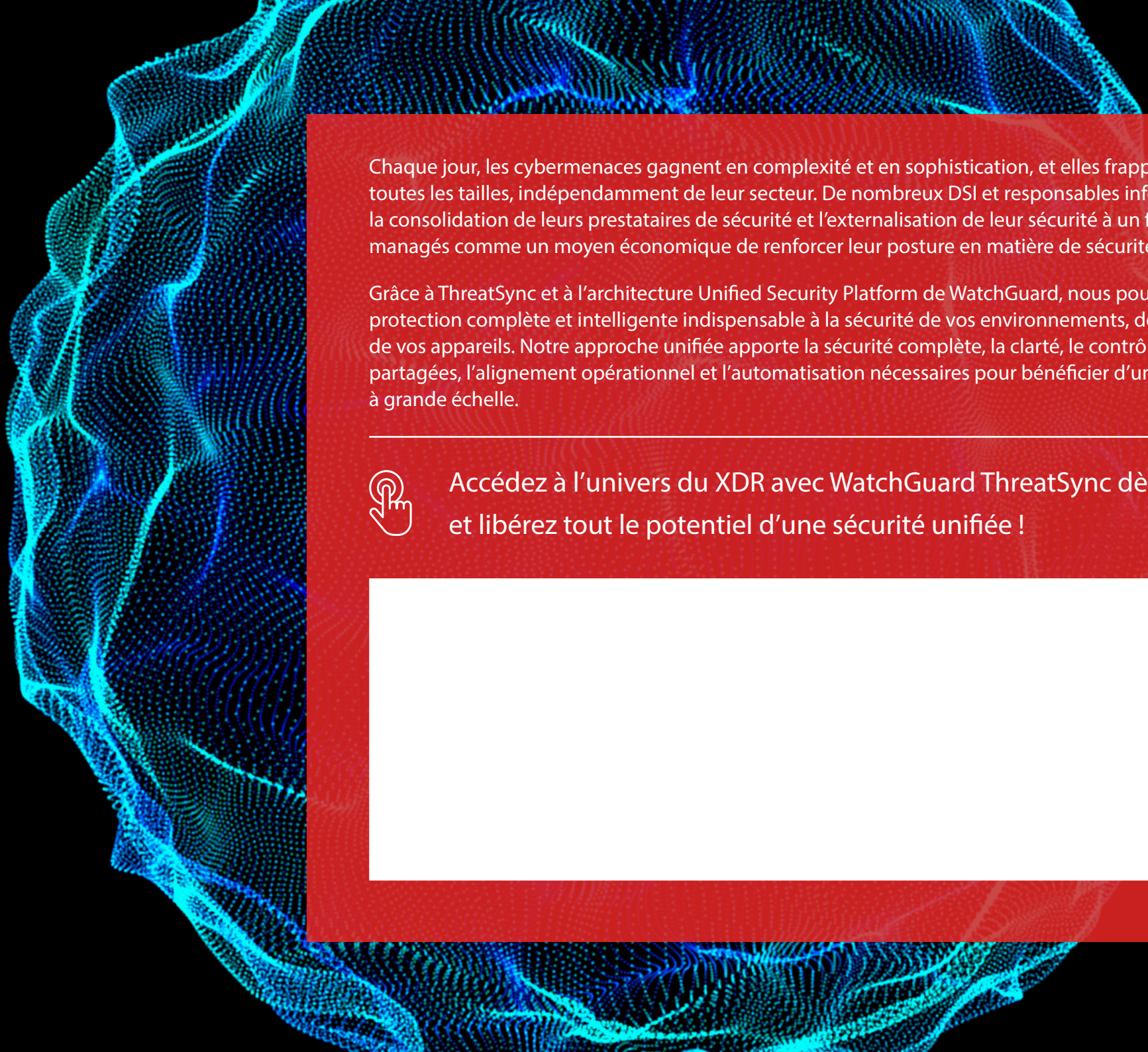


Meilleure visibilité sur l'activité du réseau et des endpoints, contribuant à identifier les menaces qui pourraient autrement passer inaperçues

Sécurité de bout en bout en unifiant les données et les alertes au sein d'une plateforme unique où les solutions peuvent fonctionner de concert pour hiérarchiser les menaces et y répondre

Réduire la charge de travail des équipes de sécurité en automatisant le processus de détection et de réponse aux menaces et en leur libérant du temps et des ressources pour gérer d'autres tâches importantes

Optimiser le processus de réponse en répondant de manière coordonnée et automatisée aux menaces détectées



Chaque jour, les cybermenaces gagnent en complexité et en sophistication, et elles frappent des entreprises de toutes les tailles, indépendamment de leur secteur. De nombreux DSI et responsables informatiques perçoivent la consolidation de leurs prestataires de sécurité et l'externalisation de leur sécurité à un fournisseur de services managés comme un moyen économique de renforcer leur posture en matière de sécurité.

Grâce à ThreatSync et à l'architecture Unified Security Platform de WatchGuard, nous pouvons vous apporter la protection complète et intelligente indispensable à la sécurité de vos environnements, de vos collaborateurs et de vos appareils. Notre approche unifiée apporte la sécurité complète, la clarté, le contrôle, les connaissances partagées, l'alignement opérationnel et l'automatisation nécessaires pour bénéficier d'une sécurité optimale à grande échelle.

Accédez à l'univers du XDR avec WatchGuard ThreatSync dès aujourd'hui, et libérez tout le potentiel d'une sécurité unifiée !

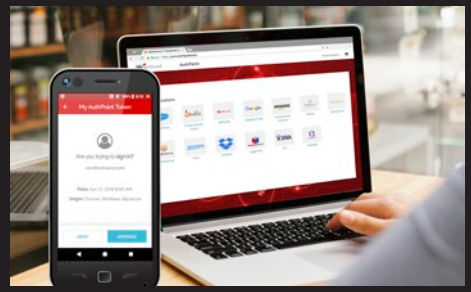
Portefeuille WatchGuard

Sécurité réseau

Les solutions de sécurité réseau WatchGuard sont spécifiquement conçues pour être faciles à déployer, à utiliser et à gérer, en plus d'offrir la meilleure sécurité qui soit. Notre approche novatrice de la sécurité réseau s'efforce de fournir une protection de pointe à toutes les entreprises, indépendamment de leur taille et de leur niveau d'expertise technique.

Wi-Fi sécurisé

Conçues pour offrir un environnement Wi-Fi de confiance et sécurisé, éliminant les tâches d'administration fastidieuses et réduisant considérablement les coûts, les solutions de Wi-Fi sécurisé WatchGuard changent littéralement la donne sur le marché actuel. Avec des outils d'engagement exhaustifs et une parfaite visibilité sur vos données d'entreprise, cette solution confère à votre entreprise un avantage concurrentiel.



Authentification multifacteur

WatchGuard AuthPoint® permet de combler la faille de sécurité qu'induit le recours à des mots de passe au moyen d'une authentification multifacteur, via une plateforme Cloud facile à utiliser. L'approche unique de WatchGuard se démarque grâce au facteur « ADN de téléphone portable » qui permet de vérifier que seules les personnes autorisées ont accès aux réseaux et aux applications Cloud sensibles.

Sécurité des endpoints

WatchGuard Endpoint Security est une gamme Cloud native de pointe qui assure la sécurité des endpoints et protège les entreprises contre toutes les cyberattaques, actuelles et futures. Sa solution phare reposant sur l'Intelligence Artificielle, WatchGuard EPDR, améliore instantanément la posture des entreprises en matière de sécurité. Elle associe des capacités de protection des endpoints (EPP) et de détection et de réponse au niveau des endpoints (EDR) avec les services Zero-Trust Application et Threat Hunting.

À propos de WatchGuard

WatchGuard® Technologies, Inc. est un leader mondial de la cybersécurité unifiée. Notre approche Unified Security Platform® est pensée pour les fournisseurs de services managés afin d'assurer une sécurité de pointe augmentant l'évolutivité et la vélocité de leur entreprise tout en améliorant leur efficacité opérationnelle. Recommandés par plus de 17 000 revendeurs et prestataires de services spécialisés dans la sécurité et adoptés par plus de 250 000 clients, les produits et services primés de WatchGuard mettent en lumière des solutions d'intelligence et de sécurité réseau, de protection avancée des endpoints, d'authentification multifacteur et de Wi-Fi sécurisé. Ensemble, ils offrent les cinq éléments essentiels d'une plateforme de sécurité : sécurité complète, intelligence collective, clarté et contrôle, alignement opérationnel et automatisation. La société a établi son siège social à Seattle, dans l'État de Washington, et possède des bureaux dans toute l'Amérique du Nord, en Europe, en Asie-Pacifique et en Amérique latine. Pour en savoir plus, rendez-vous sur le site www.watchguard.com/fr.

SERVICE COMMERCIAL FRANCE +33 97 755 4336 ADRESSE E-MAIL france@watchguard.com SITE INTERNET https://www.watchguard.com/fr