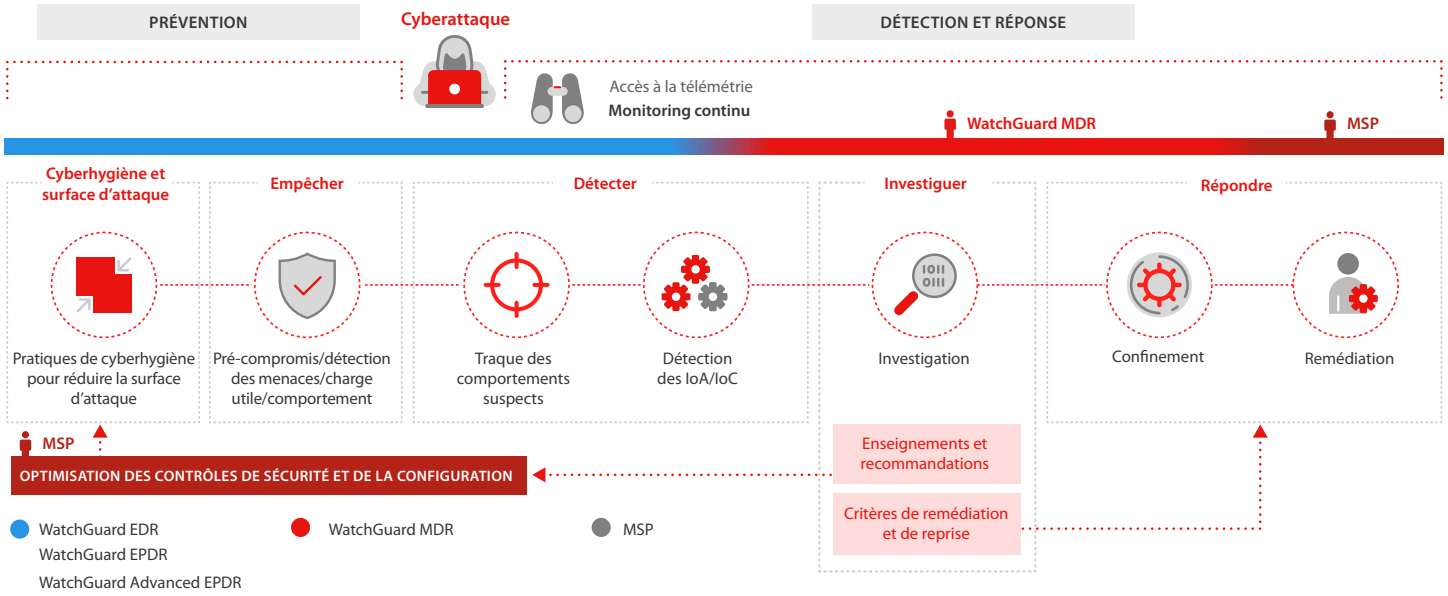
WatchGuard MDR pour les MSP

Détection et réponse à tout moment sans complications.

Alors que les cybermenaces continuent d'évoluer et de gagner en sophistication, les entreprises sont confrontées à de graves risques de sécurité, à une gestion inefficace des postures de cybersécurité et à une pénurie de personnel qualifié. Elles cherchent donc à externaliser leur protection auprès de fournisseurs de services managés (MSP) disposant de la technologie, du personnel et de l'expertise nécessaires pour contourner ces obstacles.

Cependant, la gestion des défis de sécurité complexes et de la menace croissante à laquelle la plupart des entreprises sont confrontées aujourd'hui nécessite des personnes qualifiées et quantité d'investissements, ce qui complique la tâche des MSP chargés d'offrir des services de détection et de réponse managés (MDR) de manière efficace et économique. C'est pourquoi WatchGuard a créé WatchGuard MDR, un service managé qui aide les prestataires de services de sécurité à résoudre ces problèmes. En intégrant dans leur offre notre service de détection et de réponse complet, les MSP peuvent répondre aux besoins des clients à tout moment sans qu'ils n'aient besoin de créer et d'entretenir leur propre Security Operations Center (SOC).

WatchGuard MDR fournit en continu des services de cybersécurité à nos partenaires et à leurs clients, offrant une surveillance des endpoints et de l'activité de Microsoft 365, des services de threat hunting, de prévention, de détection et de confinement des attaques, ainsi que des recommandations détaillées à des fins de remédiation. Cette offre est gérée par une équipe d'experts en cybersécurité et optimisée par l'IA. Elle ne nécessite aucun investissement dans une infrastructure de SOC traditionnelle, des technologies de pointe ou des experts en sécurité, permettant de faire face aux pressions mondiales liées à la pénurie de professionnels et de budget dans le domaine de la cybersécurité.



Fonctionnement

WatchGuard MDR fournit une surveillance continue des menaces enregistrées au niveau des endpoints et de Microsoft 365, permettant de corréler les activités suspectes afin de détecter, d'enquêter et de répondre aux cybermenaces de manière rapide et efficace. Voici comment fonctionne le service :

Intégration au service :

Le processus d'intégration commence immédiatement après l'activation du service MDR dans le compte de l'abonné. Les analystes SOC de WatchGuard unissent leurs efforts pour définir les types de réponse à apporter et assurer un service optimal. Nous confirmerons la configuration de WatchGuard EDR, EPDR et Advanced EPDR et travaillerons ensemble pour valider la fonctionnalité de vos contrôles de sécurité, en assurant que toutes les mesures de confinement et de réponse sont opérationnelles.

Surveillance continue des endpoints et de l'activité de Microsoft 365, et collecte des données :

WatchGuard MDR exploite les données des endpoints collectées par les capteurs hôtes WatchGuard, puis stockées pendant 365 jours dans notre SOC Cloud. À travers un traitement en temps réel et rétrospectif via le Machine Learning et des analyses avancées, nos threat hunters explorent de nouveaux modèles pour améliorer la cybersécurité.

Services proactifs de threat hunting et de détection en continu :

Nous utilisons le Machine Learning pour analyser les données et détecter les activités suspectes et les anomalies susceptibles d'indiquer la présence d'une menace. Nous cartographions tous les indicateurs d'attaque (IoA) selon le dispositif MITRE ATT&CK pour identifier rapidement les acteurs à l'origine de chaque menace. Notre équipe MDR traque de manière proactive les menaces au niveau des endpoints, réduisant ainsi le délai de détection et améliorant l'efficacité de la sécurité.

Investigation et validation en continu :

L'investigation et la validation constituent des éléments clés de notre service MDR. Assistés par des algorithmes de Machine Learning entraînés à partir d'incidents informatiques réels, nos experts relient les IoA aux incidents, les analysent et les valident afin de gérer rapidement les menaces potentielles et de minimiser leur impact.

Notification immédiate des incidents aux équipes partenaires :

Dès la confirmation d'un incident de sécurité, WatchGuard MDR informe rapidement nos partenaires MSP de la validation post-incident, leur évitant d'avoir à examiner les cas non confirmés. Les notifications détaillent les résultats de l'investigation et les machines affectées, permettant aux équipes partenaires de prendre des mesures rapides et éclairées tout en atténuant les menaces et en minimisant efficacement les éventuels dommages et pertes de données.

Critères de mitigation et de remédiation :

Lorsque des incidents de sécurité surviennent, l'équipe WatchGuard MDR collabore étroitement avec les MSP pour prodiguer des conseils clairs et exploitables afin de corriger les incidents et de mitiger les dommages. Ces conseils incluent des recommandations détaillées pour mettre en place des mesures de confinement, procéder à une remédiation et améliorer la posture en matière de sécurité. Nos directives aident les partenaires à réagir rapidement et efficacement aux menaces, à minimiser l'impact des incidents et à améliorer la posture globale des clients en matière de sécurité afin d'éviter que des incidents similaires ne se reproduisent.

Réponse et mitigation exécutées en continu par WatchGuard ou l'équipe partenaire :

Nos experts MDR créent des guides automatisés personnalisés pour atténuer et contenir les menaces validées, y compris celles qui impliquent une isolation potentielle des endpoints. Si les partenaires confient à leurs propres équipes les efforts de confinement, l'équipe WatchGuard MDR fournit une assistance guidée.

Réponse et remédiation exécutées par l'équipe partenaire :

Menée par des partenaires guidés par WatchGuard, la phase de confinement ou de remédiation post-incident concerne le traçage des pirates informatiques, la restauration des données et les correctifs de vulnérabilité. Elle peut également englober l'amélioration des configurations de sécurité existantes ou la mise en œuvre de nouveaux contrôles de sécurité pour éviter que des incidents similaires ne se produisent à l'avenir.

Rapports hebdomadaires et mensuels :

Les experts WatchGuard MDR fournissent des rapports de sécurité hebdomadaires et mensuels aux partenaires, détaillant les IoA détectés, les investigations réalisées, les incidents identifiés et une analyse de l'intégrité de la sécurité afin d'anticiper les menaces potentielles. Les partenaires peuvent personnaliser les rapports pour améliorer l'engagement des clients envers leur service MDR.

Avantages pour nos partenaires	
Fonctionnalités	**Avantages pour les MSP**
Monitoring continu et collecte de données via le SOC WatchGuard dans le Cloud	Capitalisez sur les possibilités offertes par les services MDR sans investir dans un SOC moderne.
Détection, threat hunting et investigation en continu par les experts de WatchGuard	Étoffez votre équipe avec du personnel qualifié en cybersécurité pour fournir des services MDR en continu.
Confinement automatique et continu des menaces	Confiez-nous le confinement continu des menaces découvertes.
Notification immédiate de l'équipe MSP	Concentrez-vous sur vos relations avec les clients pendant que nous veillons au grain
Critères de mitigation et de remédiation	Accédez à des connaissances et des bonnes pratiques en matière de sécurité qui offrent un avantage concurrentiel.
Intégration au service et contrôles d'intégrité périodiques	Empêchez les attaques résultant d'un manque de sécurité ou de gestion des endpoints.
Rapport hebdomadaire et rapport d'activité mensuel	Améliorez la sécurité des clients en gardant une longueur d'avance sur les menaces exploitant les vulnérabilités.

Modèle MDR et cas d'utilisation

1. Services MDR assurés via un Security Operations Center (SOC) interne :

Un SOC interne propose une installation et une équipe dédiées au sein d'un MSP chargées de gérer et de répondre aux problèmes de cybersécurité dans l'environnement de leurs clients.

- **Contrôle :** contrôle total de l'ensemble des processus, outils et données.
- **Coût :** élevé, implique d'investir dans une technologie et du personnel qualifié.
- **Évolutivité :** la mise à l'échelle nécessite des investissements supplémentaires en personnel et en technologie.
- **Gestion :** l'ensemble de la gestion et des opérations sont réalisées en interne.

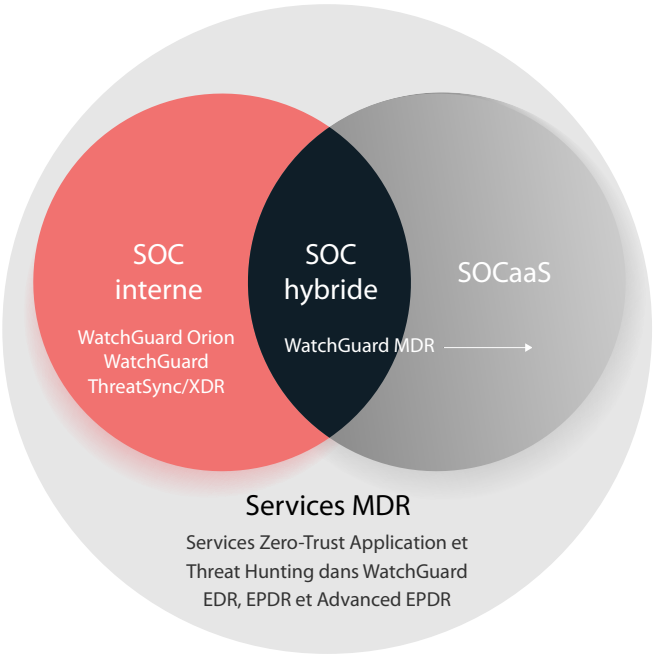
★ **Cas d'utilisation :** idéal pour les grandes organisations dotées de budgets conséquents en cybersécurité et des exigences de haute sécurité.

2. Services MDR assurés via un SOC en tant que service (SOCaaS) :

Le système SOCaaS est un service qui externalise le monitoring, la détection, les investigations et les réponses en matière de cybersécurité via un prestataire de services MDR tiers.

- **Contrôle :** contrôle limité car les processus sont gérés par le prestataire de services MDR.
- **Coût :** faible, sous la forme de frais d'exploitation plutôt que d'investissement en capital.
- **Évolutivité :** peuvent être évolutifs, en fonction des services choisis.
- **Gestion** : assurée par des professionnels tiers de la cybersécurité.

★ Cas d'utilisation : Convient aux petites et moyennes entreprises ou aux organisations disposant de budgets et de personnel de cybersécurité limités.



3. Services MDR assurés via un SOC hybride :

Un modèle de SOC hybride combine des fonctionnalités de SOC interne et externe afin d'équilibrer les capacités de cybersécurité internes et externes.

- **Contrôle :** contrôle modéré, géré en interne mais qui tire parti de ressources externes.
- **Coût :** peut être optimisé en fonction de l'équilibre des fonctions internes et externes.
- **Évolutivité :** élevé, les efforts internes peuvent être stimulés par des capacités externes.
- **Gestion :** implique à la fois une gestion interne et tierce.

★ Cas d'utilisation : idéal pour les organisations cherchant à augmenter leurs capacités SOC existantes sans réaliser d'importants investissements.

4. Services MDR automatisés

Dans un contexte de services MDR automatisés, la technologie joue un rôle central dans le renforcement de la cyberdéfense en rationalisant et en gérant automatiquement diverses fonctions à des fins d'efficacité et de réactivité.

- **Contrôle :** les activités de détection et de réponse sont automatisées. Permet aux équipes informatiques de se concentrer sur des questions stratégiques, complexes ou prioritaires.
- **Coût :** Aucune dépense supplémentaire n'est nécessaire car toutes les technologies, y compris l'IA dans le Cloud, le personnel qualifié, les outils et les informations sur les menaces, sont inclus dans le coût du produit.
- **Évolutivité :** facilite l'adaptation à l'échelle et à la complexité des environnements organisationnels.
- **Gestion :** offre une approche systématique de la détection et de la réponse aux menaces, en minimisant les efforts de gestion.

★ Cas d'utilisation : les services MDR automatisés conviennent aux entreprises disposant de personnel/d'un budget de cybersécurité limités, qui bénéficient d'un système de défense robuste et abordable.

Arguments en faveur de WatchGuard MDR

WatchGuard aide les MSP à créer leurs propres SOC internes tout en assurant l'efficacité de leurs équipes de cybersécurité grâce à des solutions telles que Advanced EPDR, WatchGuard Orion et WatchGuard ThreatSync pour XDR. Nous intégrons les services MDR automatisés ainsi que les services Zero-Trust Application et Threat Hunting dans WatchGuard EDR, EPDR et Advanced EPDR.

Grâce à WatchGuard MDR, nos partenaires MSP peuvent désormais fournir des services de détection et de réponse managés pour relever les défis métier liés aux problèmes de financement et au manque de compétences en cybersécurité.

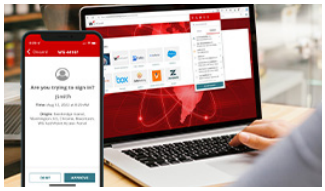
Au-delà de la détection et de la réponse, les prestataires de services MDR sont de véritables partenaires opérationnels stratégiques à long terme

Les services MDR s'inscrivent dans une stratégie de sécurité standard

Le portefeuille WatchGuard

Sécurité réseau

WatchGuard fournit une large gamme de solutions de sécurité réseau, comprenant des appliances version tabletop et d'autres montées en rack 1U, ainsi que des firewalls virtuels et dans le Cloud. Nos appliances Firebox® fournissent des services de sécurité essentiels, allant de l'IPS standard, du filtrage d'URL, de la passerelle AV, du contrôle d'application et de l'antispam, à des protections avancées telles que le sandboxing de fichiers, le filtrage DNS et plus encore. L'inspection approfondie des paquets (DPI) haute performance signifie que vous pouvez tirer parti de tous nos services de sécurité contre les attaques qui tentent de se cacher dans des canaux cryptés comme HTTPS. De plus, chaque appliance Firebox fournit des fonctionnalités SD-WAN prêtes à l'emploi pour améliorer la résilience et les performances du réseau.



Sécurité des identités

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. AuthPoint offre également une expérience utilisateur optimisée avec des méthodes d'authentification en ligne et hors ligne, ainsi qu'un portail d'applications Web pour un accès facile à l'authentification unique.

Wi-Fi Cloud sécurisé

Les solutions Wi-Fi sécurisées et gérées dans le Cloud de WatchGuard fournissent un espace en ligne sûr et protégé pour les environnements Wi-Fi tout en éliminant les maux de tête administratifs et en réduisant considérablement les coûts. Des bureaux à domicile aux vastes campus d'entreprise, WatchGuard propose la technologie Wi-Fi 6 avec chiffrement WPA3 sécurisé. Avec WatchGuard Cloud, la configuration du réseau Wi-Fi et l'administration des politiques, le déploiement sans contact, les portails captifs personnalisés, la configuration VPN, les outils d'engagement avancés, la visibilité sur les analyses commerciales et les mises à niveau sont à portée de clic.

Sécurité des endpoints

Les solutions de sécurité des endpoints de WatchGuard vous aident à protéger vos appareils contre les cybermenaces. Nos solutions endpoints phares fondées sur l'IA, que sont WatchGuard EPDR et Advanced EPDR, renforcent votre posture en matière de sécurité en intégrant de manière transparente la fonctionnalité de protection des endpoints (EPP) aux capacités de détection et de réponse (EDR), aux côtés de nos services Zero-Trust Application et Threat Hunting. Tous sont étroitement intégrés dans WatchGuard Cloud et ThreatSync, offrant une visibilité et une intelligence précieuses tout en renforçant la détection et la réponse multiproduit (XDR).

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 **WatchGuard.com/fr**.