Détection et réponse aux menaces 24 h/24 et 7 j/7 sur l'ensemble de vos solutions de sécurité

WatchGuard MDR est un service entièrement managé, disponible 24 h/24 et 7 j/7, qui ne se contente pas de vous alerter des menaces, mais qui agit également pour y remédier. En éliminant les faux positifs, notre équipe vous aide à vous concentrer sur ce qui compte et à réagir rapidement aux menaces qui pèsent sur vos ordinateurs portables, vos serveurs, les identités de vos utilisateurs, votre réseau et votre Cloud.

Votre activité ne s'arrête jamais, votre sécurité non plus. WatchGuard MDR vous offre une visibilité complète et une protection experte 24 heures sur 24. Qu'il s'agisse d'une connexion risquée, d'un e-mail suspect ou d'une menace cachée dans votre réseau, nous la détectons rapidement et la bloquons avant qu'elle ne cause des dommages, sans alourdir la charge de travail de votre équipe.

Les avantages de WatchGuard MDR

- Détection des menaces réelles 24 h/24 et 7 j/7 dans l'ensemble de votre environnement : endpoint, identité, réseau et Cloud.
- Élimination du « bruit » pour n'émettre que des alertes très fiables.
- Réponse automatique ou transmission du problème à des experts en fonction de la gravité.
- Réduction des risques grâce à l'identification des causes profondes et la correction des lacunes.
- Visibilité et rapports en temps réel sur les activités malveillantes, les mesures prises pour y répondre et les performances du SOC.

Fonctionnalités clés

Vue d'ensemble de toute votre sécurité
Obtenez une vue unifiée et centralisée des activités malveillantes sur les endpoints, les identités, le réseau et l'activité Cloud, ce qui vous permet de gagner du temps et de réduire les complexités.

Surveillance et réponse 24 h/24 et 7 j/
Notre SOC mondial est actif en permanence. Des collaborateurs experts et une automatisation puissante travaillent ensemble pour détecter et bloquer les menaces. Vous bénéficierez de traqueurs de menaces qui agissent en direct au moment où vous en aurez le plus besoin, grâce à des opérations de sécurité réparties sur quatre sites pour une couverture 24 h/24 et 7 j/7.

Détection plus intelligente avec l'IA/le ML
L'IA et le Machine Learning analysent des milliers de signaux en temps réel, détectent des schémas que les humains pourraient manquer et apprennent à contrer les nouvelles menaces. Le système apprend de chaque incident et devient chaque jour plus intelligent afin de détecter et de réagir plus rapidement.

Recherche proactive des menaces
Nos analystes recherchent les menaces cachées que les outils automatisés peuvent manquer, afin que vous soyez protégé même lorsque les pirates tentent d'utiliser des techniques sophistiquées.

Automatisation à action rapide
Nous automatisons les évaluations et actions manuelles, filtrons le bruit, ne transmettons que ce qui est important et agissons rapidement pour contenir les menaces avant qu'elles ne se propagent.

Réponse précise aux menaces
Nous agissons rapidement pour contenir les menaces, isoler les endpoints, bloquer les fichiers malveillants et enquêter sur les activités dans votre environnement.

Options de réponse flexibles
Vous décidez de la manière dont la réponse est gérée : vous vous en chargez vous-même, vous nous la confiez ou nous partageons cette responsabilité. C'est à vous de décider.

Visibilité en temps réel
Le portail MDR offre une vue en direct de votre environnement, notamment les alertes, les mesures prises et les indicateurs qui montrent comment vous êtes protégé, le tout de manière centralisée.

Bruit réduit, signal élevé
Vous ne recevrez que des alertes hautement fiables, avec moins d'un faux positif par mois, ce qui permettra à votre équipe de rester concentrée.

Conseils d'experts intégrés
Les Technical Account Managers (TAM) fournissent des conseils continus en matière de sécurité, aident à comprendre l'activité du SOC, identifient les tendances et améliorent la protection au fil du temps. Grâce à l'assistance d'experts toujours à votre disposition, vous pouvez offrir en toute confiance de meilleurs résultats à vos clients.

Pourquoi WatchGuard ? Avantage concurrentiel

Leader de la sécurité éprouvé
Avec plus de 25 ans d'expérience dans le domaine de la cybersécurité, WatchGuard s'est forgé une réputation en fournissant une protection de pointe de manière simple, évolutive et accessible. Aujourd'hui, nous aidons à sécuriser plus de 10 millions de endpoints dans 250 000 entreprises à travers le monde.

Sécurité véritablement intégrée
Contrairement aux fournisseurs MDR qui se contentent de surveiller les endpoints ou d'offrir une assistance Cloud, nous proposons une solution de détection au niveau des endpoints, de l'identité, du firewall et du réseau.

Résolument axés sur nos partenaire
Nous sommes conçus pour les MSP et les petites entreprises, sans qu'elles aient à détourner des outils pensés pour les grandes structures. Vous gardez le contrôle des relations avec les clients et de la prestation de services.

Moins de désensibilisation aux alertes, plus d'action
Nous enregistrons en moyenne moins d'un faux positif par mois contre plus de 15 par jour pour certains fournisseurs. Cela signifie moins de distractions et une réponse plus rapide.

Délai de protection plus rapide
Une prise en main rapide, des intégrations prédéfinies et un solide soutien de nos partenaires vous permettent d'être opérationnel rapidement, sans effort.

Conçu pour vos environnements
Grâce à la prise en charge native de Microsoft 365, Azure, AWS et Google Workspace, nous vous aidons à sécuriser les environnements hybrides et axés sur le Cloud dès leur mise en œuvre.

Technologie éprouvée, équipe de confiance
Notre SOC combine une expertise approfondie en matière de sécurité avec une IA puissante pour détecter et bloquer rapidement les menaces. La plateforme MDR de WatchGuard a été testée dans le cadre d'évaluations sectorielles comme MITRE et s'appuie sur des décennies d'expérience dans la fourniture d'une protection fiable et hautement performante aux entreprises du monde entier.

Sécuriser la surface d'attaque complète

Protection des endpoints
Les endpoints sont une cible principale pour les ransomware, le phishing et les attaques sans fichier. WatchGuard MDR (Managed Detection & Response) s'intègre à des produits de sécurité endpoint WatchGuard ou tiers pour détecter des comportements tels que le vol d'identifiants et l'élévation des privilèges, puis isole les appareils compromis, arrête les processus malveillants et permet une intervention en direct des analystes avant que les malwares ne puissent se propager latéralement et s'intensifier.

Protection des identités
WatchGuard MDR s'intègre à Okta ou à AuthPoint de WatchGuard pour détecter et répondre aux activités suspectes, telles que les anomalies de connexion, les tempêtes de connexion échouées ou la création de comptes malveillants. En désactivant les comptes compromis en temps réel, il empêche les attaquants de se faire passer pour des utilisateurs ou d'accéder à des plateformes cloud sans être détectés.

Protection du réseau
Les attaques qui contournent les endpoints, telles que les mouvements latéraux, les analystes de ports ou le trafic C2, sont identifiées par Firebox et ThreatSync NDR. Total MDR répond instantanément en bloquant les adresses IP malveillantes, en fermant les ports ou en arrêtant l'exfiltration des données, protégeant ainsi les systèmes internes des menaces furtives.

Protection cloud
WatchGuard MDR surveille Microsoft 365 et d'autres plateformes cloud pour détecter les signes de compromission, y compris les connexions suspectes, les modifications d'autorisations et l'accès aux boîtes aux lettres. Pour Microsoft 365, il répond via des intégrations API afin de révoquer l'accès, de réinitialiser les identifiants et de contenir les menaces avant que la fraude par email ou la perte de données ne se produise.

Temps moyen de réponse <6 minutes

« Nous avons besoin de solutions faciles à déployer et à entretenir. Nous ne pouvons pas nous permettre d'acheter des outils lourds et compliqués. Cela nous fait gagner du temps, ce qui nous permet de nous concentrer sur le soutien et conseil envers nos clients. Nous n'avons plus à jongler entre plusieurs consoles, ce qui serait ingérable avec une petite équipe. »
~ Julien Perret, Eiffie

Chasse aux menaces basée sur l'IA + automatisation

Prise en charge intégrée des outils de sécurité WatchGuard et des tiers.

Prise en charge de Microsoft 365, Azure, AWS CloudTrail, Google Workspace

Portail unique pour la visibilité, la réponse et la génération de rapports

Options de sécurité auto-gérées ou co-gérées

<1 faux positif par mois

Améliorez la protection avec WatchGuard MDR

ACTIONS DES PIRATES	WATCHGUARD MDR VOUS PROTÈGE	CE QUI EST PROTÉGÉ
Identifiants volés	**Identité** : bloque le piratage de compte	Identités
Exploits et malwares	**Endpoint** : arrête les malwares et isole les endpoints	Données au repos
Attaques par mouvement latéral	**Réseau** : détecte et bloque les mouvements latéraux	Données en mouvement
Accès au Cloud et exfiltration	**Intégration Cloud** : révoque l'accès, réinitialise les identifiants	Applications

Quel service MDR vous convient le mieux ?

Chaque environnement est différent. Certains clients utilisent déjà Microsoft Defender. D'autres souhaitent bénéficier de la protection de la pile complète de WatchGuard. WatchGuard MDR vous permet d'adapter le niveau de protection à chaque client.

	WatchGuard Core MDR	WatchGuard Core MDR pour MS	WatchGuard Total MDR	WatchGuard Open MDR
Idéal pour les partenaires/clients :	Utilisant WatchGuard Endpoint	Utilisant Microsoft Defender	Utilisant WatchGuard Endpoint, NDR, Identity, Firewall	Utilisant des outils tiers
Surveillance SOC 24 h/24 et 7 j/7	✓	✓	✓	✓
Détection des menaces basée sur l'IA/le ML	✓	✓	✓	✓
Réponse aux incidents (réponse humaine et automatisée, analyse des causes profondes)	✓	✓	✓	✓
Réponse avancée aux incidents (enquête, récupération et prévention après la faille de sécurité)	✓	✓	✓	✓
Traqueurs de menaces	✓	✓	✓	✓
Portail de défense	✓	✓	✓	✓
Accès des partenaires au gestionnaire de compte technique	✓	✓	✓	✓
Intégration des endpoints	WatchGuard Endpoint	Microsoft Defender	WatchGuard Endpoint	WatchGuard Endpoint, CrowdStrike, Microsoft Defender
Intégration des réseaux			WatchGuard Firebox ThreatSync NDR	WatchGuard Firebox, ThreatSync NDR et la plupart des firewalls tiers
Intégration de l'identité			WatchGuard AuthPoint	AuthPoint de WatchGuard et Okta
Microsoft 365	✓	✓	✓	✓
Couverture AWS CloudTrail			✓	✓
Google Workspace			✓	✓

À propos de WatchGuard Technologies, Inc.

WatchGuard® Technologies est un leader mondial de la cybersécurité unifiée, avec des solutions spécialement conçues pour les fournisseurs de services managés. Contrairement à d'autres, WatchGuard offre une véritable sécurité pour le monde réel grâce à sa plateforme de sécurité unifiée (Unified Security Platform®) qui regroupe les réseaux, endpoints et identités en s'appuyant sur l'IA, ainsi que les avancées réalisées au niveau de l'approche Zero Trust pour garantir une protection fiable et évolutive. Recommandé par plus de 17 000 revendeurs et fournisseurs de services managés spécialisés dans la sécurité et adoptés par plus de 250 000 entreprises, WatchGuard permet à ses partenaires de se développer rapidement, d'éliminer les casse-têtes opérationnels et d'obtenir des résultats probants, sans le moindre fournisseur ou la moindre console ou complexité supplémentaire. La société a établi son siège social à Seattle, dans l'État de Washington, et possède des bureaux dans le monde entier. Pour en savoir plus, rendez-vous sur watchguard.com/fr.