Solutions WatchGuard Endpoint Security pour les MSP

WatchGuard Endpoint Security	Basic	Prime	360	Elite
Protection				
Protection anti-exploits		●	●	●
Protection contre les malwares connus et Zero Day	●	●	●	●
Protection contre les ransomwares connus et Zero Day	●	●	●	●
Protection contre les exploits connus et Zero Day		●	●	●
Protection anti-phishing	●	●	●	●
Protection de différents vecteurs d'attaque (web, email, réseau, appareils)	●	●	●	●
Protection traditionnelle avec signatures génériques et optimisées	●	●	●	●
Service Zero Trust Application			●	●
Requêtes vers l'intelligence collective basée dans le cloud de WatchGuard	●	●	●	●
Détection comportementale basée sur le contexte, alimentée par une IA auto-apprenante	●	●	●	●
Blocage des programmes d'installation malveillants (MSI) basé sur une IA auto-apprenante	●	●	●	●
Détection des fichiers .NET malveillants basée sur une IA auto-apprenante	●	●	●	●
Protection des scripts basée sur une IA auto-apprenante	●	●	●	●
Firewall personnel et managé	●	●	●	●
IDS/HIPS	●	●	●	●
Protection contre les attaques réseau		●	●	●
Contrôle des appareils	●	●	●	●
Filtrage des adresses URL par catégorie (surveillance de la navigation Web)	●	●	●	●
Surveillance				
Solution de surveillance des risques pour les endpoints	●	●	●	●
Surveillance continue de toutes les activités de processus	●	●	●	●
Conservation des données	30 jours*	30 jours	90 jours	90 jours
Module complémentaire de conservation des données pendant un an		●	●	●
Évaluation des vulnérabilités	●	●	●	●
Détection				
Détection des pilotes vulnérables		●	●	●
Alertes de sécurité entièrement configurables et instantanées	●	●	●	●
Détection des applications de confiance compromises			●	●
Service Zero Trust Application			●	●
ThreatSync eXtended Detection and Response (XDR) - fonctionnalités de détection	●	●	●	●
Visualisation des incidents (graphe d'incident et panneau de signaux avec chronologie)	●	●	●	●
Signaux d'incident mappés sur MITRE ATT&CK		●	●	●
Recherche d'IoCs STIX et de règles YARA				●
Confinement				
Isolation, analyse et redémarrage de l'ordinateur en temps réel		●	●	●

WatchGuard Endpoint Security	Basic	Prime	360	Elite
Réponse et remédiation				
Capacité à revenir en arrière et à remédier aux actions de ransomware menées par les attaquants (copies shadow)	●	●	●	●
Centralisation des fichiers mis en quarantaine	●	●	●	●
Analyse automatique et élimination des virus	●	●	●	●
Possibilité de bloquer des applications inconnues et indésirables			●	●
ThreatSync eXtended Detection and Response (XDR) - fonctionnalités de remédiation		●	●	●
Enquête				
Vue interactive des incidents, multi-signaux, pour une analyse approfondie de la cause racine (RCA)		●	●	●
Détection et corrélation automatiques d'une attaque, à l'aide d'alertes, mappées sur le framework MITRE ATT&CK®		●	●	●
Contexte approfondi et télémétrie de forensic informatique en temps réel				●
Requêtes avancées dans le cadre d'enquêtes				●
Assistant d'investigation GenAI				●
Enquête avancée sur une attaque (Jupyter Notebooks)				●
Shell distant pour un MTTR plus rapide et une réduction du temps de présence de la menace (dwell time)				●
Analyse approfondie des fichiers avec l'outil CAPA				●
Mode verbeux pour la simulation d'attaque				●
Advanced Reporting Tool (module complémentaire)		●	●	●
Découverte et surveillance des données personnelles non structurées sur les endpoints (module complémentaire)**		●	●	●
Réduction de la surface d'attaque				
Endpoint Access Enforcement			●	●
Mode verrouillage dans le module Advanced Protection			●	●
Technologie anti-exploits		●	●	●
Bloquer des programmes par hash ou par nom (par ex. PowerShell)			●	●
Contrôle des appareils	●	●	●	●
Protection Web	●	●	●	●
Mises à jour automatiques	●	●	●	●
Découverte automatique des endpoints non protégés	●	●	●	●
Gestion des correctifs pour les systèmes d'exploitation et applications tierces (module complémentaire)	●	●	●	●
Sécurité pour les connexions VPN (Firebox requis)	●	●	●	●
Stratégies de sécurité avancées				●

WatchGuard Endpoint Security	Basic	Prime	360	Elite
Gestion de la sécurité des endpoints				
Console centralisée basée sur le Cloud	●	●	●	●
Héritage des paramètres entre groupes et endpoints	●	●	●	●
Capacité à configurer et appliquer les paramètres au niveau des groupes	●	●	●	●
Capacité à configurer et appliquer les paramètres au niveau de chaque endpoint	●	●	●	●
Déploiement en temps réel des paramètres de la console vers les endpoints	●	●	●	●
Gestion de la sécurité basée sur des vues endpoints et des filtres dynamiques	●	●	●	●
Capacité à planifier et exécuter des tâches sur des vues endpoints	●	●	●	●
Possibilité d'attribuer des rôles préconfigurés aux utilisateurs de la console	●	●	●	●
Possibilité de personnaliser des alertes locales	●	●	●	●
Capacité à contrôler les redémarrages pour les mises à jour de correctifs et du moteur	●	●	●	●
Audit de l'activité des utilisateurs	●	●	●	●
Installation via des packages MSI, des URL de téléchargement et des emails envoyés aux utilisateurs finaux	●	●	●	●
Rapports à la demande et planifiés à différents niveaux et offrant plusieurs options de granularité	●	●	●	●
KPI de sécurité et tableaux de bord de gestion	●	●	●	●
Disponibilité de l'API	●	●	●	●
Intégration d'une solution RMM (surveillance et gestion à distance)				
ConnectWise Automate	●	●	●	●
Kaseya VSA	●	●	●	●
N-able N-central	●	●	●	●
N-able N-sight	●	●	●	●
NinjaOne (script de déploiement automatisé)	●	●	●	●
Modules				
Patch Management	●	●	●	●
Full Encryption	●	●	●	●
Advanced Reporting Tool		●	●	●
Data Control**		●	●	●
SIEMFeeder		●	●	●
MDR		●	●	●

WatchGuard Endpoint Security	Basic	Prime	360	Elite
Systèmes d'exploitation pris en charge				
Compatible avec Windows Intel	●	●	●	●
Compatible avec Windows ARM	●	●	●	●
Prise en charge de macOS ARM (M1 et M2)	●	●	●	●
Compatible avec macOS Intel	●	●	●	●
Compatible avec Linux	●	●	●	●
Compatible avec Android	●	●	●	●
Compatible avec iOS	●	●	●	●
Prise en charge des environnements virtuels - persistants et non persistants (VDI)***	●	●	●	●

Où se procurer WatchGuard EDR ?

Notre solution EDR a été retirée de cette matrice car elle est destinée à un cas d'usage spécifique : celui d'un client disposant déjà d'un AV/EPP et souhaitant ajouter une couche EDR par-dessus.

* Conservation de données d'incidents dans l'interface utilisateur de gestion uniquement.

* WatchGuard Data Control est uniquement disponible dans les pays suivants : Espagne, Allemagne, Royaume-Uni, Suède, France, Italie, Portugal, Pays-Bas, Finlande, Danemark, Suisse, Norvège, Autriche, Belgique, Hongrie et Irlande.

*** Systèmes compatibles avec les types de machines virtuelles suivants : VMWare Desktop, VMware Server, VMware ESX, VMware ESXi, Citrix XenDesktop, XenApp, XenServer, MS Virtual Desktop et MS Virtual Servers. Les solutions Endpoint Security 360 WatchGuard sont compatibles avec les applications Citrix Virtual, Citrix Desktops 1906 et l'application Citrix Workspace pour Windows.

Plateformes prises en charge et configuration système requise pour WatchGuard Endpoint Security

Systèmes d'exploitation pris en charge : Windows (Intel et ARM), macOS (Intel et ARM), Linux et Android.

Les fonctionnalités EDR sont disponibles sur Windows, macOS et Linux. Seul Windows permet de bénéficier de l'ensemble des fonctionnalités.

Liste des navigateurs compatibles : Google Chrome, Mozilla Firefox, Microsoft Edge et Safari.