FICHE TECHNIQUE

THREAT DETECTION AND RESPONSE

Bloquez les malwares avancés grâce à la sécurité corrélée

Les pirates informatiques conçoivent des malwares plus sophistiqués que jamais. A travers des techniques d'archivage auto-extractible, de chiffrement et de polymorphisme, les cyber-criminels parviennent à dissimuler leurs attaques pour éviter la détection. Les attaques de type Zero Day et les malwares avancés échappent facilement aux solutions antivirus, qui sont tout simplement trop lentes à répondre au flux constant de menaces émergentes. Les entreprises de toutes tailles ont besoin d'une solution qui s'appuie sur une approche holistique de la sécurité, du réseau jusqu'aux postes de travail. WatchGuard Threat Detection and Response (TDR) est un puissant ensemble d'outils de défense contre les malwares avancés qui corrèle les indicateurs de menace provenant des appliances Firebox et des agents Host Sensor pour bloquer les malwares connus, inconnus et évasifs.

« Les fonctions de détection corrélée et de réponse automatique nous apportent la couche de sécurité qui nous manquait pour détecter immédiatement les infections et les empêcher de se propager dans notre réseau. »

~ Andre Bromes, Vice-président principal et Directeur informatique/Responsable de la sécurité des systèmes d'information de Goodwill New York, New Jersey

CORRÉLATION ET PRIORISATION

ThreatSync est un moteur de corrélation Cloud qui analyse les données d'événement provenant des agents Host Sensor et des appliances Firebox pour identifier les comportements malveillants.
Les menaces sont notées en fonction de leur degré de gravité afin d'orienter la résolution.

VISIBILITÉ SUR LES MENACES AU NIVEAU DES POSTES DE TRAVAIL

Le capteur léger WatchGuard Host Sensor étend la visibilité sur les menaces et leur gestion jusqu'aux postes de travail. Il envoie en continu des données heuristiques et comportementales depuis le poste de travail jusqu'au moteur ThreatSync à des fins de corrélation et de scoring.
Les capteurs hôtes étant gérés de manière centralisée depuis le Cloud, les administrateurs informatiques et les fournisseurs de services de sécurité managés (MSSP) peuvent facilement les déployer, les mettre à jour et les gérer depuis n'importe où à travers le monde.

RÉPONSE AUTOMATISÉE

TDR assure une protection complète contre les malwares avancés et peut intervenir automatiquement pour mettre des fichiers en quarantaine, tuer les processus et supprimer les clés de registre. Atténuez les menaces dès leur détection en un simple clic ou en définissant des stratégies de réponse automatique basées sur les scores qui leur sont attribués.

PRÉVENTION CONTRE LES RANSOMWARES AVEC HRP

Host Ransomware Prevention (HRP) est un module dédié aux ransomwares intégré à TDR qui se base sur des analyses comportementales et des appâts pour les détecter. Si un ransomware est détecté, HRP intervient automatiquement pour le bloquer avant qu'il n'ait eu le temps de chiffrer vos fichiers.

PRIORISATION DES MENACES AVANCÉE AVEC APT BLOCKER

Les malwares sont en constante évolution et les indicateurs suspects pourraient être des signes avant-coureurs de menaces encore non identifiées. Désormais, grâce à l'intégration étroite avec WatchGuard APT Blocker, les fichiers suspects peuvent être envoyés dans une sandbox Cloud nouvelle génération à des fins d'analyse approfondie et de réévaluation.

INTELLIGENCE SUR LES MENACES DE HAUT NIVEAU

L'intelligence sur les menaces était jusqu'à présent réservée aux grandes entreprises aux budgets importants et aux équipes de sécurité conséquentes. Grâce à Threat Detection and Response, WatchGuard regroupe et analyse les flux d'intelligence sur les menaces, vous offrant ainsi les avantages de ce haut niveau de sécurité sans devoir passer par la complexité ni les coûts associés.

FICHE TECHNIQUE

Une détection plus intelligente grâce à la corrélation

Les attaques de malwares avancés sont complexes et divisées en plusieurs étapes. Les postes de travail sont généralement infectés lorsqu'un utilisateur est victime d'une campagne d'hameçonnage ou clique sur un lien malveillant conçu pour déclencher le processus d'infection. Une fois l'attaque initiée, le malware peut tenter de s'introduire dans les serveurs et d'en prendre le contrôle afin de recevoir d'autres instructions. Il peut également tenter de se propager à d'autres appareils de l'entreprise via votre réseau.

Tandis que le malware lui-même peut sembler unique en son genre, les comportements du réseau nécessaires pour faciliter l'attaque suivent des schémas communs et prévisibles. Si vos solutions de sécurité fonctionnent en silos, le réseau n'a aucun moyen de savoir ce qui se passe au niveau des postes de travail, et inversement ; vous êtes donc vulnérable face à ce type de menace. Aussi, l'analyse conjointe des comportements du réseau et des postes de travail offre un excellent moyen pour identifier et bloquer des malwares pourtant inconnus. C'est ce que fait Threat Detection and Response.

Les données d'événement provenant des services de sécurité des appliances WatchGuard Firebox, y compris APT Blocker, Reputation Enabled Defense (RED, Autorité de réputation), Gateway AntiVirus (Antivirus de passerelle) et WebBlocker, sont envoyées à ThreatSync afin de les mettre en correspondance avec les données des postes de travail collectées par les agents Host Sensor. ThreatSync analyse alors ces données sur les menaces afin de fournir un score de menace complet et évaluer leur niveau de gravité global. Les événements qui sont détectés à la fois au niveau du réseau et d'un poste de travail reçoivent automatiquement le score de 10, niveau de menace le plus élevé.

Lorsque des stratégies sont activées, ThreatSync indique automatiquement à l'appliance Firebox de bloquer le malware afin qu'il ne puisse pas communiquer avec le serveur malveillant. L'appliance va alors mettre le fichier en quarantaine, tuer le processus ou supprimer la clé de registre persistante sur le poste de travail. Ces mêmes actions peuvent également être effectuées manuellement via la résolution en un clic.

Firebox Model	Included Host Sensors
T15	5
T35	20
T55	35
T70 / M200	60
M370	150
M470	200
M440 / M570 / 670/M4600 / M5600	250
Firebox Cloud / FireboxV S	50
Firebox Cloud / FireboxV M	150
Firebox Cloud / FireboxV L	250
Firebox Cloud / FireboxV XL	250

Host Sensor Add-On Options
10 Host Sensors
25 Host Sensors
50 Host Sensors
100 Host Sensors
250 Host Sensors
500 Host Sensors
1000 Host Sensors
2500 Host Sensors
5000 Host Sensors

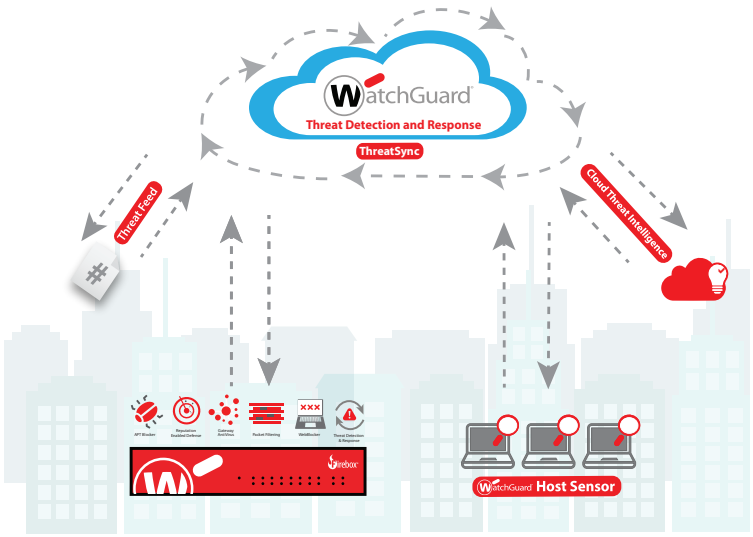
SPÉCIFICATIONS DE HOST SENSOR :

Systèmes d'exploitation compatibles –

- Windows 7, 8, 8.1, 10
- Windows Server 2008, 2012, 2016
- Linux RedHat/CentOS 6, 7

Compatible avec les appliances Firebox série T, série M, Firebox Cloud et FireboxV.

Fonctionnalités et services	TOTAL SECURITY SUITE	Basic Security Suite
Service de prévention d'intrusions (IPS)	✓	✓
Contrôle d'application	✓	✓
WebBlocker (filtrage d'URL)	✓	✓
spamBlocker (antispam)	✓	✓
Gateway AntiVirus (Antivirus de passerelle)	✓	✓
Reputation Enabled Defense (RED, Autorité de réputation)	✓	✓
Network Discovery (Découverte réseau)	✓	✓
APT Blocker	✓	
Protection contre les pertes de données (Data Loss Protection, DLP)	✓	
Threat Detection and Response	✓	
Access Portal	✓	
Dimension Command	✓	
Support	**Gold (24 h/24, 7 j/7)**	Standard (24 h/24, 7 j/7)



WatchGuard propose le plus important réseau de revendeurs et de fournisseurs de services à valeur ajoutée du secteur. Consultez notre réseau de partenaires certifiés à l'adresse findpartner.watchguard.com. Pour en savoir plus sur Threat Detection and Response : **watchguard.com/TDR.**

FRANCE 01 40 90 30 35 SERVICE COMMERCIAL INTERNATIONAL +1.206.613.0895 www.watchguard.fr