DATENBLATT

HOST SENSOR

Wichtiger Bestandteil von Threat Detection and Response zur Endpunkt-Überwachung und Gefahrenabwehr.

Da Angreifer heutzutage immer perfider ans Werk gehen, gewinnt der Schutz des gesamten Netzwerks inklusive aller Endpunkte zunehmend an Bedeutung. Threat Detection and Response (TDR) setzt – als Baustein der Total Security Suite von WatchGuard – Security-Events im Netzwerk und am Endpunkt mit detaillierten Analysen zur Bedrohungslage in Verbindung. Dadurch können potenzielle Angriffe noch früher erkannt und bewertet werden. Sofortmaßnahmen zur Abwehr erfolgen ohne Verzögerung. Während der Einblick ins Netzwerk über die WatchGuard Firebox®-Appliance sichergestellt wird, sammelt der WatchGuard Host Sensor alle Ereignisdaten am Endpunkt.

Der WatchGuard Host Sensor identifiziert lückenlos alle Bedrohungen am Endpunkt und führt gleichzeitig die vorgegebenen Abwehrmaßnahmen aus. Durch die Kombination von Host Ransomware Prevention (HRP) – als Komponente des WatchGuard Host Sensors – und APT Blocker – für einen erweiterten Schutz vor Malware – entsteht die branchenweit effektivste Lösung zur Abwehr von Ransomware-Angriffen. Host Ransomware Prevention unterbindet die Ausführung von Ransomware noch bevor die Dateiverschlüsselung am Endpunkt erfolgt. So wird der Angriff wirkungsvoll abgewehrt, bevor Schaden entsteht.

TRANSPARENZ BIS ZUM ENDPUNKT

Der schlanke Host Sensor von WatchGuard überwacht und erkennt auf Basis von Heuristik und Verhaltensanalysen alle Bedrohungsaktivitäten im Netzwerk. Der Host Sensor sendet diese Ereignisse zwecks Korrelation mit Ereignissen aus der Firebox-Appliance fortlaufend an ThreatSync von TDR. Das Ergebnis: ein umfassender, nach Priorität geordneter Bedrohungsindex.

AUTOMATISCHE GEFAHRENABWEHR

Mithilfe des WatchGuard Host Sensors lassen sich Richtlinien zur automatisierten Abwehr von Bedrohungen erstellen. So kann entsprechend der von ThreatSync generierten Gefahrenbewertung gezielt festgelegt werden, welche konkrete Abwehrmaßnahme zum Tragen kommt – von der Isolierung der Datei über das Löschen des Registrierungsschlüssels bis hin zum Abbruch des Prozesses. Dadurch verkürzt sich nicht nur die Reaktionszeit im Umgang mit Bedrohungen. Zudem werden auch die zuständigen Mitarbeiter entlastet.

ADVANCED RANSOMWARE PREVENTION

Host Ransomware Prevention* ist ein Ransomware-spezifisches Modul im WatchGuard Host Sensor. Auf Grundlage von Verhaltensanalysen sowie aktuellen Verzeichnissen der jeweils im Umlauf befindlichen Gefahren überprüft HRP eine Vielzahl von Merkmalen und ist somit in der Lage zu erkennen, ob ein Ereignis mit einem Ransomware-Angriff in Verbindung steht oder nicht. Auf diese Weise kann HRP bei ernsthaften Gefahren automatisch einen Ransomware-Angriff verhindern – noch bevor am Endpunkt eine Dateiverschlüsselung stattfindet.

TRIAGE MODERNER BEDROHUNGEN MIT APT BLOCKER

Malware entwickelt sich laufend weiter und verdächtige Anzeichen können Frühwarnungen bisher noch nicht identifizierter Malware sein. Dank der engen Integration mit WatchGuard APT Blocker können die verdächtigen Dateien nun zur tiefgreifenden Analyse und Neubewertung in eine Cloud-Sandbox der nächsten Generation gesendet werden.

FUNKTIONEN UND VORTEILE

- Fortlaufende Überwachung und Erkennung von Bedrohungsaktivitäten am Endpunkt
- Schnellere Gefahrenerkennung und -abwehr dank Automatisierung
- Besserer Schutz vor modernen Malware-Angriffen, einschließlich Ransomware
- Vordefinierte Richtlinien sorgen automatisch für Prozessabbruch, Quarantänisierung von Dateien oder Löschung des Registrierungsschlüssels
- Der schlanke Software-Agent beansprucht kaum Verarbeitungsressourcen
- Problemlos parallel zu bereits installierten Antivirenlösungen einsetzbar

*Available on Windows 8, 8.1, and 10

DATENBLATT

HOST SENSOR-LIZENZEN

Im Abonnement der Total Security Suite ist für jede Appliance eine bestimmte Anzahl an Host Sensor-Instanzen enthalten. Diese werden von Threat Detection and Response zusammengeführt, verwaltet sowie zugeteilt und lassen sich für den gesamten Account nutzen. Im Hinblick auf unternehmensspezifische Anforderungen können weitere Host Sensoren jederzeit zusätzlich erworben werden.

FIREBOX MODEL	INCLUDED HOST SENSORS
T15 / T20	5
T40	20
T80	50
M270	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

TECHNISCHE DATEN HOST SENSOR

Kompatible Betriebssysteme –

- Windows 7, 8, 8.1, 10
- Windows Server 2012, 2016, 2019
- Linux RedHat/CentOS 6, 7
- macOS 10.10, 10.11, 10.12, 10.13, 10.14, 10.15

Kompatibel mit Firebox T-Serie, M-Serie und XTMv-Appliances.

WATCHGUARD SECURITY SERVICES

Ein Paket. Total Security.

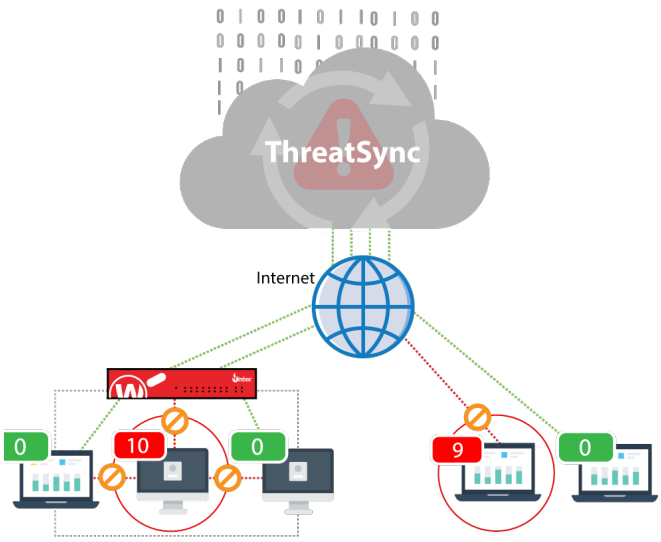
Anwender profitieren am meisten, wenn die unterschiedlichen Sicherheitsfunktionen ineinander greifen. Dadurch ergibt sich umfassender Schutz und maximale Effizienz bei enormer Performance. Die WatchGuard Total Security Suite bietet Kunden neben klassischen Network-Security-Services auch zusätzliche – der jeweils gegenwärtigen Bedrohungslage angepasste – Sicherheitsfunktionalität, einschließlich APT Blocker, Data Loss Prevention und Threat Detection and Response (TDR).

Gerade TDR unterstreicht diese Philosophie des perfekten Zusammenspiels: Security-Events im Netzwerk und am Endpunkt werden mit detaillierten Analysen zur Bedrohungslage in Verbindung gesetzt. Auf diese Weise ergibt sich ein solides Fundament für die Bewertung von Gefahren. Die Engine zur Korrelation und Bewertung – ThreatSync – erfasst die Daten aller Sicherheitsdienste – einschließlich WebBlocker, ATP Blocker, Gateway Antivirus und spamBlocker. Diese Informationen aus dem Netzwerk werden gemeinsam mit den vom Host Sensor am Endpunkt gesammelten Daten analysiert, bewertet und entsprechend des Schweregrads der jeweiligen Bedrohung eingeordnet.

Somit liefert die WatchGuard Total Security Suite Unternehmen modernste IT-Sicherheitsfunktionalität, umfassende Visualisierungswerkzeuge, effektive Möglichkeiten der Gefahrenabwehr sowie Threat Intelligence auf Enterprise-Niveau – in einem einzigen Angebotspaket.

	SUPPORT	BASIC SECURITY	TOTAL SECURITY
Stateful Firewall	✓	✓	✓
VPN	✓	✓	✓
SD-WAN	✓	✓	✓
Access Portal*	✓	✓	✓
Intrusion Prevention Service)IPS)		✓	✓
Anwendungskontrolle		✓	✓
WebBlocker (URL-/Inhaltsfilterung)		✓	✓
spamBlocker (Anti-Spam)		✓	✓
Gateway AntiVirus		✓	✓
Reputation Enabled Defense		✓	✓
Network Discovery		✓	✓
APT Blocker			✓
Threat Detection & Response			✓
DNSWatch			✓
IntelligentAV**			✓
WatchGuard Cloud Visibility Datenaufbewahrung		1 Tag	30 Tage
Support	Standard (24 x 7)	Standard (24 x 7)	Gold (24 x 7)

*Nicht erhältlich auf Firebox T15/T15-W, T20/T20-W oder T35-R. Total Security Suite erforderlich für M270, M370, M470, M570, M670, Firebox V und Firebox Cloud.
**Nicht erhältlich auf Firebox T15/T15-W, T20/T20-W oder T35-R.



WatchGuard verfügt über eines der größten Partnernetzwerke der Branche. Eine Liste unserer zertifizierten Partner finden Sie hier:

findpartner.watchguard.com Weitere Informationen zu Threat Detection and Response mit WatchGuard Host Sensor erhalten Sie unter watchguard.com/TDR.

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49.700.92229333 INTERNATIONALER VERTRIEB +1.206.613.0895 WEB www.watchguard.de WatchGuard Technologies, Inc.