DATENBLATT

THREAT DETECTION & RESPONSE

Hochentwickelte Malware mit korrelierter Sicherheit stoppen

Hacker rüsten auf und entwickeln Malware, wie es sie derart ausgeklügelt und perfide bisher noch nicht gab. Mit Methoden wie Packen, Verschlüsseln und Polymorphismus können Cyberkriminelle ihre Angriffe so geschickt tarnen, dass auch der aufmerksamste Beobachter kaum eine Chance hat, sie zu erkennen. Zero-Day-Angriffe und hochentwickelte Malware schlüpfen geschickt durch die Maschen von Antivirus-Lösungen, die schlichtweg zu langsam sind, um den nicht endenden Strom immer neuer Bedrohungen aufhalten zu können. Unternehmen aller Größen benötigen eine Lösung, die einen ganzheitlichen Ansatz für Sicherheit vom Netzwerk zum Endpunkt nutzt. WatchGuard Threat Detection and Response (TDR) ist eine leistungsstarke Sammlung hochentwickelter Tools, die durch Korrelation der von Firebox-Appliances und Host-Sensoren gemeldeten Anzeichen von Bedrohungen bekannte, unbekannte und schwer fassbare Malware-Angriffe abwehren.

„Durch die Korrelation der Erkennung und automatisierten Reaktion auf Gefahren entsteht in unserer Sicherheitsstruktur eine bislang noch fehlende Schicht, die es uns ermöglicht, Infektionen sofort zu erkennen und ihre Verbreitung in unserem Netzwerk zu unterbinden."

~ Andre Bromes, SVP und CIO/CISO bei Goodwill New York/New Jersey

KORRELATION UND PRIORISIERUNG

ThreatSync ist ein cloud-basiertes Korrelationsmodul, das die von Host-Sensoren und Firebox-Appliances gesammelten Daten auf bösartiges Verhalten hin analysiert. Bedrohungen werden basierend auf dem Schweregrad der Gefahr bewertet und danach geeignete Abwehrmaßnahmen ergriffen.

EINBLICK IN AKTIVITÄTEN AM ENDPUNKT

Der schlanke WatchGuard Host Sensor erweitert Sichtbarkeit und Management bis zum Endpunkt und sendet am Endpunkt erfasste heuristische und Verhaltensdaten zur Korrelation und zum Scoring kontinuierlich an ThreatSync. Die Host Sensoren werden zentral über die Cloud verwaltet, was IT-Administratoren und MSSPs (Managed Security Service Providers) die Bereitstellung, Aktualisierung und Verwaltung von weltweit verteilten Sensoren erleichtert.

AUTOMATISIERTE REAKTION

TDR bietet erweiterten Schutz vor den Gefahren ausgeklügelter Malware, denn TDR kann automatisch eingreifen und Dateien in Quarantäne verschieben, Prozesse abbrechen und Registrierungsschlüssel löschen. Ein Klick genügt, um auftauchende Bedrohungen umgehend manuell zu entschärfen. Oder Sie richten auf dem Schweregrad einer Gefahr basierende Behebungsrichtlinien ein, die automatisch eine bestimmte Reaktion auslösen.

E-MAIL-ALARME UND -BENACHRICHTIGUNGEN MIT THREATSYNC

WatchGuard ThreatSync ermöglicht Ihnen nun die Einrichtung konfigurierter E-Mail-Benachrichtigungen über Hinweise auf Bedrohungen, Zwischenfälle und Abwehrprozesse, die im Netzwerk und am Endpunkt entdeckt werden und ablaufen. So können Sie die Sicherheit stets im Auge behalten – egal, wo Sie sind und ohne Anmelden im Dashboard.

ABWEHR VON RANSOMWARE-ANGRIFFEN MIT HRP

Host Ransomware Prevention (HRP) ist ein Ransomware-spezifisches Modul der TDR, das mit Verhaltensanalysen und so genannten Honeypots als Lockmittel Ransomware erkennt und abwehrt. Wenn Malware erkannt wird, greift HRP automatisch ein und stoppt die Ransomware, bevor Dateien verloren gehen.

SICHTUNG MODERNER BEDROHUNGEN MIT APT BLOCKER

Tagtäglich taucht neue und weiterentwickelte Schadsoftware auf, und jedes verdächtige Anzeichen kann eine frühzeitige Warnung vor einer noch zu identifizierenden Malware sein. Dank der engen Verflechtung mit WatchGuard APT Blocker können verdächtige Dateien nun für eine umfassende Analyse und Neubewertung an eine fortschrittliche Cloud-Sandbox gesendet werden.

THREAT INTELLIGENCE AUF ENTERPRISE-NIVEAU

Threat Intelligence stand bisher nur Unternehmen mit ausreichend großem Budget und noch größeren Sicherheitsteams zur Verfügung. Mit Threat Detection and Response sammelt und analysiert WatchGuard Threat Intelligence -Feeds und bietet damit große sicherheitstechnische Vorteile, vereinfacht den Vorgang und senkt die Kosten.

DATENBLATT

Intelligentere Gefahrenerkennung durch Korrelation

Hochentwickelte Malware-Angriffe sind komplex und laufen in mehreren Phasen ab. Endpunkte werden in der Regel infiziert, wenn ein Benutzer Opfer einer Phishing-Kampagne oder dazu verleitet wird, einen bösartigen Link anzuklicken, der eine Infektion auslöst. Wenn der Angriff einmal läuft, versucht die Malware wahrscheinlich, Verbindungen zu Command-and-Control-Servern herzustellen, die weitere Anweisungen erteilen. Möglicherweise versucht sie außerdem, den Angriff über das Netzwerk auf andere Endstellen in Ihrem Unternehmen auszuweiten.

Die Malware selbst mag ein bislang einmaliges Erscheinungsbild haben, doch die Verhaltensweisen zur Verbreitung des Angriffs über das Netzwerk müssen bestimmten allgemeinen und vorhersagbaren Mustern folgen. Wenn die vorhandenen Sicherheitslösungen isoliert voneinander arbeiten, gibt es im Netzwerk keinerlei Möglichkeit zu erkennen, was am Endpunkt passiert. Umgekehrt gilt das Gleiche. Auf diese Weise sind Sie dieser gefährlichen Bedrohung schutzlos ausgesetzt. Aus genau diesem Grund ist die kombinierte Analyse des Netzwerks und der Endpunkte ein äußerst wirksames Mittel, wenn es darum geht, unbekannte Malware zu erkennen und zu stoppen. Möglich wird das alles mit Threat Detection and Response.

Ereignisdaten von Sicherheitsdiensten auf WatchGuard Fireboxe-Appliances, beispielsweise APT Blocker, Reputation Enabled Defense (RED), Gateway AntiVirus und WebBlocker, werden an ThreatSync gesendet und dort mit den vom Host Sensor gesammelten Endpunktdaten verglichen. Die Bedrohungsdaten werden anschließend von ThreatSync analysiert, um einen umfassenden Bedrohungsindex auf Grundlage des Schweregrads der Bedrohungen zu erstellen. Ereignisse, die sowohl im Netzwerk als auch am Endpunkt erfasst werden, werden automatisch mit der höchsten Gefahrenstufe 10 versehen.

Wenn entsprechende Regeln hinterlegt und aktiviert wurden, verhindert ThreatSync ohne weiteres Zutun, dass die Malware Kontakt zum externen Server aufnimmt. Hierfür wird die Datei entweder in Quarantäne verschoben, der Prozess abgebrochen oder der noch vorhandene Registrierungsschlüssel am Endpunkt gelöscht. Diese Aktionen können ebenso „manuell" ausgeführt werden – dank unserer Technologie ist dabei auch nur ein Klick nötig.

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

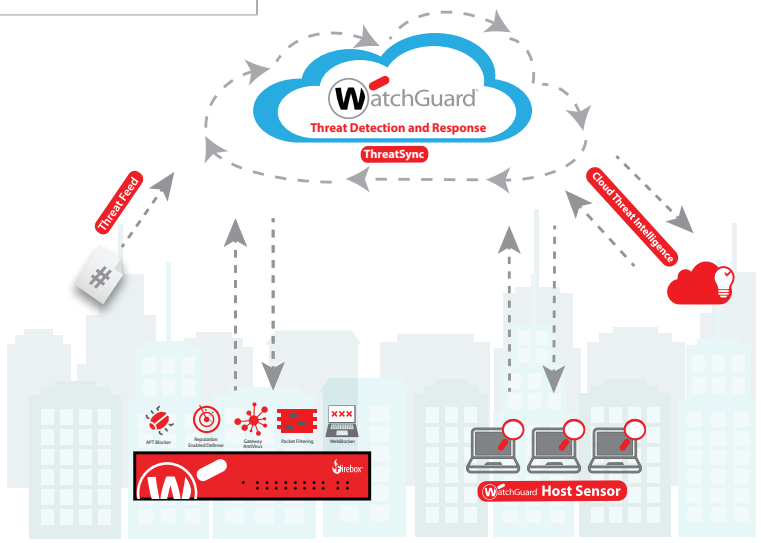
TECHNISCHE DATEN HOST SENSOR:

Kompatible Betriebssysteme –

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

Kompatibel mit Firebox-Appliances der T- und M-Serie sowie mit Firebox Cloud und FireboxV.

Funktionen und Dienste	TOTAL SECURITY SUITE	Basic Security Suite
Intrusion Prevention Service (IPS)	✓	✓
App Control	✓	✓
WebBlocker	✓	✓
spamBlocker	✓	✓
Gateway Antivirus	✓	✓
Reputation Enabled Defense (RED)	✓	✓
Network Discovery	✓	✓
APT Blocker	✓	
Data Loss Protection (DLP)	✓	
Threat Detection and Response	✓	
DNSWatch	✓	
Access Portal	✓	
Dimension Command	✓	
Support	Gold (24x7)	Standard (24x7)



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 erhalten Sie unter **watchguard.com/TDR.**

Deutschland, Österreich, Schweiz: +49 700 92229333 INTERNATIONALER VERTRIEB +1.206.613.0895 www.watchguard.de