DATENBLATT

THREATSYNC

Hochentwickelte Bedrohungen 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 ThreatSync korreliert von Firebox-Appliances und Host-Sensoren gemeldete Bedrohungen, um bekannte , unbekannte und schwer fassbare Malware-Angriffe abzuwehren.

> 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.

HOST-ISOLATION UND AUTOMATISCHE REAKTION

Kontrollieren Sie Infektionen automatisch, wenn eine Bedrohung erkannt wird. ThreatSync isoliert jedes Hostgerät schnell vom Netzwerk und verhindert weitere Infektionen Ihres Unternehmens. Sobald die Malware isoliert ist, wird sie durch ThreatSync automatisch eliminiert, bösartige Dateien werden in Quarantäne verschoben und dazugehörige Registrierungsschlüssel gelöscht.

ABWEHR VON RANSOMWARE-ANGRIFFEN MIT HRP

Host Ransomware Prevention (HRP) ist ein Ransomware-spezifisches Modul des ThreatSync, 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.

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.

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.

THREAT INTELLIGENCE AUF ENTERPRISE-NIVEAU

Threat Intelligence stand bisher nur Unternehmen mit ausreichend großem Budget und noch größeren Sicherheitsteams zur Verfügung. Mit ThreatSync 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 ThreatSync.

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-MODELL	ENTHALTENE HOST SENSOREN	ZUSATZ-OPTIONEN HOST SENSOR
T20	5	10 Host Sensoren
T40	20	25 Host Sensoren
T80	60	50 Host Sensoren
M290	75	100 Host Sensoren
M390	150	250 Host Sensoren
M590 / M690 / M4800 / M5800	250	500 Host Sensoren
Firebox Cloud / FireboxV S	50	1000 Host Sensoren
Firebox Cloud / FireboxV M	150	2500 Host Sensoren
Firebox Cloud / FireboxV L	250	5000 Host Sensoren
Firebox Cloud / FireboxV XL	250	

TECHNISCHE DATEN HOST SENSOR

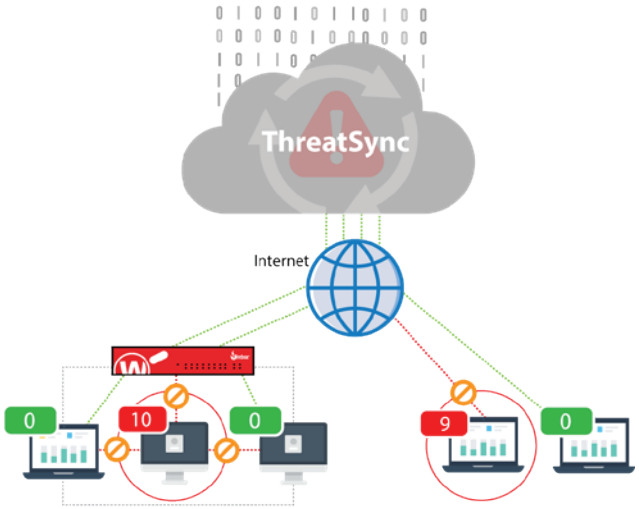
Kompatible Betriebssysteme –

- 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.

	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			✓
ThreatSync			✓
DNSWatch			✓
IntelligentAV*			✓
WatchGuard Cloud Visibility Datenaufbewahrung		1 Tag	30 Tage
Support	Standard (24 x 7)	Standard (24 x 7)	Gold (24 x 7)

*Total Security Suite erforderlich für Firebox V und Firebox Cloud.



WatchGuard verfügt über eines der größten Partnernetzwerke der Branche. Eine Liste unserer zertifizierten Partner finden Sie hier: **findpartner.watchguard.com** Weitere Informationen zu ThreatSync erhalten Sie unter **watchguard.com/ThreatSync**.

Deutschland, Österreich, Schweiz: +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.de WatchGuard Technologies, Inc.