Datenblatt

WatchGuard APT Blocker

SCHUTZ VOR MODERNEN SCHADPROGRAMMEN UND ZERO- DAY-BEDROHUNGEN

Unternehmen, die allein auf Antivirus-Software vertrauen, sind schon längst nicht mehr auf der sicheren Seite. Malware ist heutzutage deshalb so gefährlich, weil sie sich problemlos in Code verwandeln kann, der von signaturbasierten Virenschutzlösungen, die nach bekannten Schadmustern Ausschau halten, nicht identifiziert wird.

Sandbox-Lösung der nächsten Generation für vollständige Systememulation

WatchGuard APT Blocker nutzt das Prinzip der Verhaltensanalyse, um festzustellen, ob eine Datei bösartig ist. APT Blocker identifiziert verdächtige Dateien und gibt diese an eine fortschrittliche, cloudbasierte Sandbox-Lösung. Dabei handelt es sich um eine virtuelle Umgebung, in der Code analysiert, emuliert und ausgeführt wird, um sein Bedrohungspotenzial zu bestimmen.

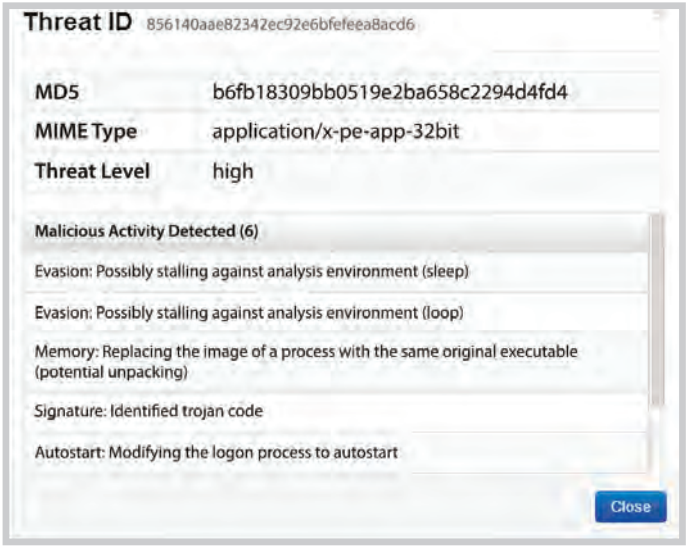
Moderne Bedrohungen, darunter Advanced Persistent Threats (APT), sind so konzipiert, dass sie Erkennungsmethoden identifizieren und dabei selbst verborgen bleiben. Die vollständige Systememulation von APT Blocker – bei der die physikalische Hardware, inklusive CPU und Speicher, simuliert wird – bietet umfassende Einblicke in das Verhalten von Schadprogrammen. Hinzu kommt, dass diese dabei nur schwer erkennen, dass sie bereits entdeckt wurden.

Durch APT Blocker analysierte Dateitypen

- alle ausführbaren Windows-Dateien
- Adobe PDF-Dateien
- Microsoft Office-Dateien, darunter Excel-, Word-, Visio- und PowerPoint-Dateien
- Android Application Installer (.apk)-Dateien

Gepackte Dateien – wie Windows .zip-Ordner – werden dekomprimiert.

Mehr als Erkennung: Beispiellose Transparenz



Ein APT-Bericht führt das Malware-Verhalten im Detail auf und erklärt, warum eine Datei als Malware markiert wurde.

APT Blocker bietet nicht nur beispiellosen Schutz vor modernen Schadprogrammen, sondern garantiert auch intuitive Nachvollziehbarkeit. Dank der Visualisierungslösung WatchGuard Dimension™, die zum Funktionsumfang jeder WatchGuard XTM- und Firebox®-Lösung gehört, erhalten Sie neben leistungsstarkem Zero-Day-Schutz ebenso sofortigen Überblick über alle Bedrohungen Ihres Netzwerks – inklusive gut verständlicher Informationen zu den jeweiligen Angriffen.

ZERO DAY IST DAS NEUE SCHLACHTFELD

Zero-Day-Angriffe sind Bedrohungen, für die es keine Software-Patches gibt. Auch Signaturen existieren nicht.

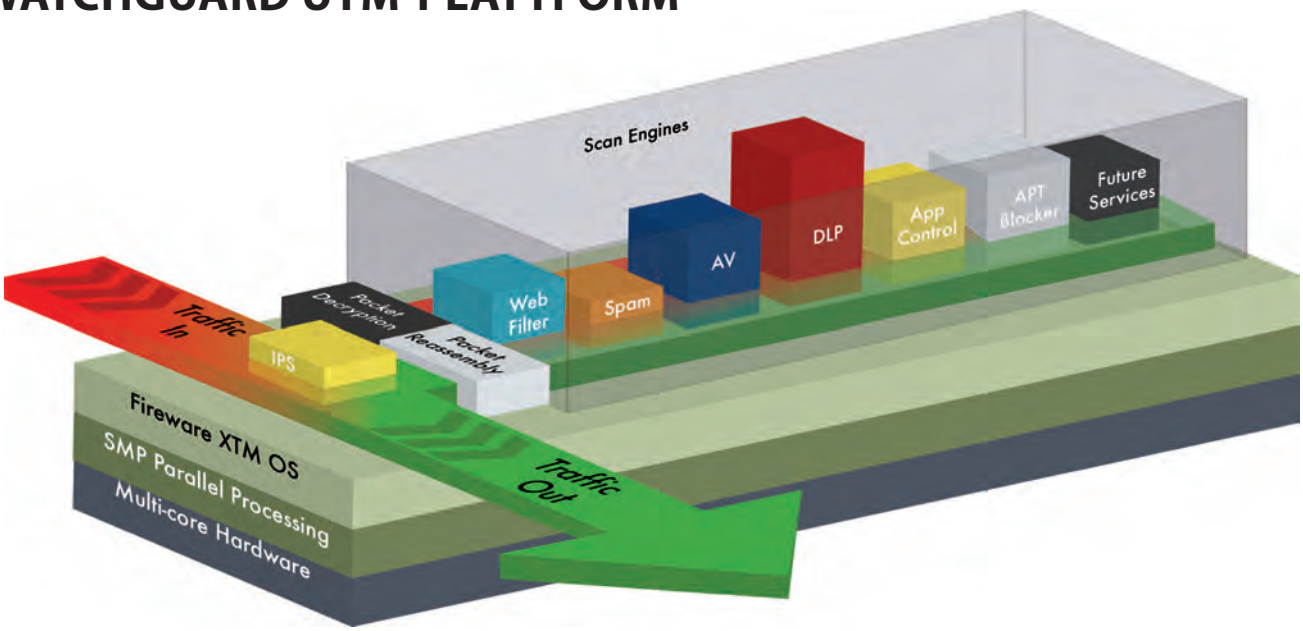
Trotzdem sind signaturbasierte Virenschutzlösungen als vorderste Verteidigungslinie nach wie vor unverzichtbar, um bekannte Bedrohungen bereits am Gateway abzufangen.

APT Blocker erweitert diesen Schutz und schiebt der Gefahr durch unbekannte Malware-Varianten ebenso den Riegel vor. Ihr Unternehmen ist so gegenüber den sich unaufhörlich weiterentwickelnden Bedrohungen von heute maximal abgesichert.

Fast 88 Prozent der heutigen Schadprogramme sind in der Lage, **sich zu verwandeln, um der Erkennung durch** signaturbasierte Virenschutzlösungen zu entgehen...

„Malwise", IEEE Computers

WATCHGUARD UTM-PLATTFORM



Flexible Architektur garantiert Abwehr von Netzwerkbedrohungen bei gleichzeitiger Leistungsoptimierung
Beim Einsatz einer UTM-Plattform (Unified Threat Management) von WatchGuard durchläuft der Netzwerkverkehr bei höchstem Leistungsniveau sämtliche Sicherheitsservices – vom Spam-Schutz bis hin zu Data Loss Prevention. Alle Scanvorgänge erfolgen dank Multi-Core-Verarbeitung gleichzeitig. Das Ergebnis: maximaler Schutz bei enorm hohem Datendurchsatz. Die Ressourcenzuweisung richtet sich stets nach dem Datenfluss und den für die jeweiligen Daten erforderlichen Sicherheitsservices. Wenn beispielsweise die Webfilterung mehr Leistung erfordert, werden automatisch mehr Prozessoren zugeschaltet – damit der Webverkehr ungehindert fließt und Ihr Unternehmen sicher bleibt.

EINFACHE ABOVERWALTUNG

Sämtliche Sicherheitsfunktionen Ihrer WatchGuard XTM- oder Firebox T10-Lösung, einschließlich Sicherheitsabonnements, können über eine einzige intuitive Konsole verwaltet werden.

ALLE NETZWERKAKTIVITÄTEN STETS IM BLICK

- Sicherheitsgefährdende Aktivitäten werden protokolliert und gespeichert. So können Sie anhand fundierter Berichte sofort vorbeugende oder korrigierende Maßnahmen ergreifen.
- Alle Management-Tools (darunter umfassende Reporting- und Überwachungsfunktionen) sind im Lieferumfang der WatchGuard Firewall enthalten. Der Kauf zusätzlicher Hard- oder Software ist nicht erforderlich.

BESTELLVERFAHREN

WatchGuard-Sicherheitsservices sind im ein- und mehrjährigen Abonnement erhältlich. Ihr lokaler autorisierter WatchGuard-Vertriebspartner gibt Ihnen gerne weitere Informationen zu zusätzlichen erstklassigen Abwehrfunktionen für Ihre WatchGuard Appliance sowie zu Servicepaketen und Sonderaktionen.

UTM DER SPITZENKLASSE

WatchGuard kombiniert modernste Technologien und bietet somit extrem zuverlässige Sicherheitslösungen. Aufgrund der Partnerschaft mit branchenführenden Anbietern sind die UTM-Netzwerksicherheitsprodukte von WatchGuard rundum erstklassig.

- **AVG**: Der laut Virus Bulletin durchgängig leistungsstarke Anbieter liefert die Engine für Gateway AntiVirus.
- **Cyren**: Die patentierte cloudbasierte RPD®-Technologie macht spamBlocker zur einzigen effektiven Anti-Spam-Lösung für UTM-Appliances mit geringem Ressourcenbedarf. Tagtäglich werden bis zu 4 Milliarden Nachrichten überprüft.
- **Websense**: Stellt die cloudbasierte URL-Datenbank für WebBlocker zur Verfügung. Ergänzt werden die Sicherheitsfunktionen durch ThreatSeeker Network von Websense Security Labs.
- **Trend Micro**: Führender Anbieter von IPS und Anwendungssignaturen für umfassenden Schutz vor aktuellen Bedrohungen.
- **Sophos**: Führender Anbieter von Endpunkt- und E-Mail-Sicherheitslösungen, einschließlich DLP, für Unternehmen weltweit.
- **Lastline**: Liefert mit der cloudbasierten, vollständige Systememulati-onsanalyse und erweiterten Identifikationsmöglichkeiten hinsichlich ausgefeilter Ausweichmanöver von Malware die Basis von APT Blocker.

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB +1.206.613.0895 www.watchguard.com