**MEDIENINFORMATION**

Zürich, 25. Juli 2019

**WatchGuard verkürzt die Erkennungsdauer von Zero-Day-Threats und Evasive Malware auf wenige Minuten**

**Dank neuer KI-basierter Funktionen können Managed Service Provider und Kunden schneller auf Bedrohungen reagieren und sind besser geschützt**

**Mit dem aktuellen Release 5.7 des Sicherheitsdienstes TDR (Threat Detection and Response) dreht WatchGuard hinsichtlich der Leistungsfähigkeit seiner Korrelations- und Analyseplattform „ThreatSync“ mächtig auf: Anstelle von Monaten werden Zero-Day-Threats und ausgefeilte Bedrohungen wie Evasive Malware nun innerhalb weniger Minuten erkannt und anschliessend automatisiert beseitigt. Denn die Gefahr für Unternehmen, Opfer einer solchen Attacke zu werden, ist durchaus real: Laut dem neuesten Internet Security Report von WatchGuard belief sich alleine im ersten Quartal 2019 der Anteil von Zero-Day-Malware, die von traditionellen Antiviren-(AV)-Lösungen übersehen wird, auf 36 Prozent. Demgegenüber beträgt nach Angaben des Ponemon Institute die ‚Mean Time To Identify‘ (MTTI) für eine Sicherheitsverletzung 197 Tage, während es im Schnitt 69 Tage ab dieser ersten Erkennung dauert, die Gefahr zu beseitigen (‚Mean Time To Contain‘ – MTTC). Dadurch steigt mit jedem Tag, an dem eine Attacke unbemerkt bleibt, auf Unternehmensseite das Risiko von finanziellen Einbussen und Imageschäden.**

Für eine adäquate Einschätzung und Bewertung der Bedrohungssituation werden die Informationen der Firebox-Appliances sowie der TDR-Hostsensoren an den Endpunkten mithilfe von TDR korreliert und über die ThreatSync-Plattform analysiert. Das erlaubt es nicht zuletzt Managed Service Providern (MSP), ihren Kunden hochwirksame Security-Services anzubieten: Auf Basis der Daten lassen sich mit TDR sowohl Zero-Day-Malware-Angriffe automatisiert abwehren als auch unbekannte Prozesse identifizieren, die mit bösartigen Zielen verbunden sind. Anwender können darauf vertrauen, dass auf Basis der Sicherheitsservices von WatchGuard Bedrohungen entsprechend erkannt und in wenigen Minuten beseitigt werden.

Brendan Patterson, Vice President of Product Management bei WatchGuard, ergänzt: „Cyberkriminelle setzen zunehmend auf zielgerichtete Angriffe mit fortschrittlichen Techniken, die von Standardlösungen zum Schutz vor Malware übersehen werden. Dementgegen verlassen sich mittelständische Unternehmen hingegen oft noch auf Anbieter, die weder über die dafür nötige Sicherheitserfahrung noch die entsprechenden technischen Ressourcen verfügen. Gefragt sind vertrauenswürdige IT-Lösungsanbieter, die schnell und effektiv auf diese Angriffe reagieren. Mit unseren neuen ThreatSync-Funktionen statten wir MSP mit den Tools aus, die sie zur Bereitstellung wirksamer Malware Detection and Response (MDR)-Dienste benötigen. Damit lassen sich derartige Attacken innerhalb von Minuten erkennen und automatisch entschärfen.“

Zu den wichtigsten ThreatSync-Funktionen, die jetzt im Rahmen von TDR verfügbar sind, gehören:

* **Host Containment und Automated Response** – Sobald ThreatSync einen gefährdeten Host-Computer erkennt, wird dieser automatisch vom Rest des internen Netzwerks isoliert. Host Containment ergreift anschliessend Massnahmen, die eine weitere Ausbreitung der Infektion verhindern: Die Malware wird automatisiert beseitigt, indem Prozesse beendet, bösartige Dateien unter Quarantäne gestellt und zugehörige Registrierungsschlüssel gelöscht werden.
* **Accelerated Breach Detection** – ThreatSync erkennt sofort, ob sich auf geschützten Endpunkten bösartige Dateien befinden und beseitigt diese anschliessend automatisiert. Im Gegensatz zu den meisten vergleichbaren Netzwerksicherheitslösungen erfolgt dies im engen Dialog mit der Endpoint Security: Sobald ein Benutzer unbekannte Dateien aus dem Internet herunterlädt, übergibt sie die Firebox zunächst zur erweiterten Analyse an APT Blocker, die Next-Gen Cloud-Sandbox von WatchGuard. Währenddessen werden sie von den Host-Sensoren der Endpoint Security aktiv überwacht. Stellt sich die Datei als bösartig heraus, identifiziert ThreatSync die Datei sofort an allen geschützten Endpunkten und beginnt mit der Problembehebung.
* **Network Process Correlation** – TDR erkennt und blockiert nicht nur Verbindungen zu bösartigen Zielen, sondern reagiert auch automatisch auf die bisher unbekannten Prozesse, die der Bedrohung zugrunde liegen. Mit ThreatSync werden die von der Firebox geblockten, bösartigen Verbindungen zudem korreliert. Dadurch lässt sich zurückverfolgen, von welchem Endpunkt die Bedrohung ausging und wie sich der Prozess ursprünglich gestaltete. Entsprechende Vorgänge werden automatisch abgebrochen. Dank dieser Funktion erhalten Managed Service Provider und Netzwerkadministratoren detaillierte Kontextinformationen zu Netzwerkziel, Name des Dienstes sowie zum Hostnamen und -prozess, um erfolgreiche Abwehr- und Vorbeugemassnahmen einzuleiten.
* **Artificial Intelligence Analysis** – Bei ThreatSync kommen neue KI-Funktionen zum Einsatz, mit denen Dateien automatisch analysiert und getestet werden, um diejenigen zu identifizieren, die verdächtige Merkmale aufweisen. Erst dann werden sie zur weiteren Analyse an APT Blocker weitergeleitet. Das verringert den Zeitaufwand für die Verwaltung von Warnmeldungen und verhindert, dass wirklich verdächtige Dateien unentdeckt bleiben. MSP und mittelständischen Unternehmen wird es dadurch ermöglicht, echte Bedrohungen schneller und sicherer zu identifizieren und zu blockieren.

ThreatSync steht als Teil des TDR-Sicherheitsmoduls allen Unternehmen mit einer Lizenz für die Total Security Suite zur Verfügung. Weitere Informationen finden Sie unter <https://www.watchguard.com/de/wgrd-products/security-services/threat-detection-and-response>

Bildmaterial

|  |
| --- |
|   |
| Brendan Patterson, Vice President of Product Management bei WatchGuard |

Das Bildmaterial zum Download finden Sie in unserem Medienportal press-n-relations.amid-pr.com (Suchbegriff „Brendan Patterson"). Selbstverständlich schicke ich Ihnen die Datei auch gerne per E-Mail zu. Kontakt: rh@press-n-relations.de

|  |  |
| --- | --- |
| Kontakt:WatchGuard Technologies GmbHPaul Moll – Field Marketing Manager Central EuropeWendenstr. 379, 20537 HamburgTel.: +49 152 31795040paul.moll@watchguard.comwww.watchguard.de | Presse- und Öffentlichkeitsarbeit:Press'n'Relations GmbH, c/o Medianovis AGRebecca HornSchaffhauser. 91, 8057 ZürichTel.: +49 731 962 87 15 rh@press-n-relations.dewww.press-n-relations.com |

**Über WatchGuard Technologies**

WatchGuard Technologies gehört zu den führenden Anbietern im Bereich Netzwerksicherheit. Das umfangreiche Produktportfolio reicht von hochentwickelten UTM (Unified Threat Management)- und Next-Generation-Firewall-Plattformen über Multifaktor-Authen­tifizierung bis hin zu Technologien für umfassenden WLAN-Schutz sowie weiteren spezifischen Produkten und Services rund ums Thema IT-Security. Mehr als 80.000 Kunden weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau, wobei dank der einfachen Handhabung neben kleinen und mittelständischen Unternehmen nicht zuletzt auch grosse, dezentral aufgestellte Organisationen vom Einsatz profitieren. Neben der Zentrale in Seattle im US-Bundesstaat Washington verfügt WatchGuard über Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum.

Aktuelle Informationen, Aktionen und Updates finden Sie auch auf [Twitter](https://twitter.com/sichersein), [Facebook](https://de-de.facebook.com/WatchGuardSichersein/) oder [LinkedIn](https://de.linkedin.com/company/watchguardsichersein). Der WatchGuard InfoSec-Blog Secplicity berichtet darüber hinaus über die neuesten Bedrohungen und zeigt auf, wie man mit ihnen umgeht: [www.secplicity.org](http://www.secplicity.org/). Oder Sie abonnieren den 443 - Security Simplified Podcast bei [Secplicity.org](http://www.secplicity.org/) bzw. wo immer Sie Ihre Lieblings-Podcasts finden.