

PRESSEMITTEILUNG

Adaptive Defense 360 erhält Gütesiegel von AV-Comparatives

Panda Security bietet optimalen Schutz gegen moderne Hackerattacken

Duisburg, den 26. Januar 2017 - Das international renommierte Testinstitut AV-Comparatives hat der Anti-Malware-Lösung ‚Adaptive Defense 360‘, Panda Securitys Premiumschutz für Unternehmen, sein Gütesiegel gegeben. Im Dezember 2016 prüfte das Institut die Panda-Lösung mit 220 Testdatensätzen, die Ransomware, Backdoors, Password-Stealer, Würmer, Viren, Trojaner oder PuPs (Potenziell unerwünschte Programme) enthielten. Alle Bedrohungen wurden von Adaptive Defense 360 erkannt und blockiert. Während des gesamten Testzeitraumes hat AV-Comparatives keine Fehlalarme auf dem Testsystem beobachtet.

Adaptive Defense 360 ist die erste und derzeit einzige IT-Security-Lösung, die eine Endpoint Protection Platform (EPP) mit einem cloud-basierten intelligenten Endpoint Detection and Response (EDR) Service kombiniert. Das innovative Sicherheitsmodell des spanischen IT-Sicherheitspezialisten beruht dabei auf drei Säulen: Der ständigen Überwachung aller Anwendungen auf Firmenservern und Workstations (1); der automatischen Klassifizierung aller auf den Endpoints laufenden Prozesse mithilfe von Big Data und maschinellen Lernverfahren (2); der manuellen Analyse und Klassifizierung von Anwendungen, die nicht automatisch klassifiziert werden konnten, durch Techniker der PandaLabs (3).

Die Experten von AV-Comparatives beschreiben die Arbeitsweise von Adaptive Defense 360 folgendermaßen: „Während EPP mithilfe von bestehenden Methoden, beispielsweise Signaturen und Verhaltenserkennung, Malware erkennt und blockiert, überwacht und klassifiziert der Endpoint-Schutz der nächsten Generation 100 Prozent der Prozesse, die auf den Netzwerkcomputern laufen. Dabei werden forensische Daten generiert, die genutzt werden können, um den Ursprung, die betroffenen Geräte und die von der Malware ausgeführten Aktionen zu bestimmen; zum Beispiel wie die Bedrohung begonnen hat, welche Prozesse verursacht wurden und wann, geöffnete Verbindungen usw. All diese Informationen sind über die Konsole in Echtzeit verfügbar.“

Es gibt keine Malware, die nicht von Adaptive Defense 360 erfasst wird

Auf diese Weise erkennt und blockiert Adaptive Defense 360 Malware, die andere Schutzsysteme nicht einmal sehen. „Da diese Lösung alle laufenden Prozesse klassifiziert, gibt es keine Malware, die nicht von ihr erfasst wird.“, so die AV-Comparatives-Experten weiter.

In dem gegebenen Testszenario vom Dezember mit 220 unterschiedlichen Bedrohungen blockierte Adaptive Defense 360 alle Bedrohungen bis auf eine. Diese Malware – ein Password-Stealer – konnte zunächst auf das Testsystem gelangen, wurde dann jedoch

aufgrund ihres schädlichen Verhaltens umgehend als Malware identifiziert und blockiert, ohne dabei Schaden zu verursachen oder eine Veränderung am System vorzunehmen.

Dank der lückenlosen Überwachung aller Prozesse, die auf den Netzwerk-Geräten laufen, ist Adaptive Defense 360 in der Lage, alle Arten von bekannter und unbekannter Malware sowie Zero-Day-Angriffen (Ransomware, Botnetze, Exploits, dateilose Malware, APTs usw.) zu erkennen und die Endpoints davor zu schützen. „Auch wenn das Produkt einen schädlichen Prozess fälschlicherweise als vertrauenswürdig klassifiziert, wird er als Malware klassifiziert, sobald aufgrund der Echtzeitüberwachung schädliche Aktivitäten erkannt werden oder verdächtiges Verhalten festgestellt wird. Wenn die Malware bereits im System war, bevor Adaptive Defense 360 installiert wurde, erkennt das Produkt die Malware, wenn sie aktiv ist, und liefert Informationen darüber, was sie seit der Installation von Adaptive Defense 360 getan hat.“, erläutern die AV-Comparatives-Experten in ihrem Testbericht.

Testscenario simulierte die realen Bedrohungen, denen Firmen ausgesetzt sind

„Für uns war es sehr wichtig, dass die Tests in einer Umgebung durchgeführt wurden, die perfekt die echte Welt simulieren konnte sowie die Bedrohungen, denen Unternehmen ständig ausgesetzt sind“, sagt Luis Corrons, Leiter des Anti-Malware-Labors PandaLabs am Hauptstandort von Panda Security in Spanien.

Jan Lindner, Geschäftsführer von Panda Security Deutschland, ergänzt: „Das Gütesiegel des unabhängigen Testlabors AV-Comparatives bestätigt, dass der Schutz, den Adaptive Defense 360 bietet, mehr ist als eine leere Worthülse oder reines Marketing. Diese Lösung bietet ein neues Sicherheitsmodell, das jedes Unternehmen benötigt, das im Kampf gegen moderne Cyberbedrohungen bestehen will.“ Die Herausforderung durch kreative und professionell agierende Hacker ist heutzutage so groß wie nie zuvor. „Der Angreifer passt sein Verhalten ständig an, um klassische Antivirensoftware zu umgehen. Er infiltriert Systeme, agiert im Stillen und führt alle möglichen Bewegungen aus, die wir mit Adaptive Defense 360 überwachen, analysieren und blockieren können, bevor er seine Ziele erreicht.“, fährt Jan Lindner fort.

Den vollständigen Bericht von AV-Comparatives sowie weitere Details zum Testscenario und den Funktionsweisen von Adaptive Defense 360 erhalten Sie unter

http://pandanews.de/wp-content/uploads/AV-Comparatives_AD360.pdf

Über Panda Security

Seit seiner Gründung 1990 in Bilbao kämpft Panda Security gegen jedwede Bedrohung der IT-Infrastrukturen von Unternehmen bis zu Heimanwendern. Als Pionier der IT-Security-Branche gelang es dem Entwicklerteam immer wieder, mithilfe bedeutender technologischer Meilensteine den Sicherheitslevel seiner Kunden entscheidend zu erhöhen. So gilt Panda heute als ‚Entwickler des Cloud-Prinzips bei der Malware-Bekämpfung‘. (Quelle: Magic Quadrant for Endpoint Protection Platforms, Gartner, 2012)

Basierend auf seinen Entwicklungen stellt das Unternehmen heute eine einzigartige Plattform zur Verfügung, die unter der Bezeichnung Adaptive Defense verschiedenste Technologien wie EDR (Endpoint Detection and Response), EPP (Endpoint Protection Platform), SIEM (Security Information and Event Management) und DLP (Data Loss Prevention) verbindet. Dadurch wird ein zuverlässiger Schutz wie zum Beispiel vor Ransomware (Cryptolocker) auf den Endpoints realisiert.

Das Unternehmen Panda Security mit Hauptsitz in Spanien ist aktuell in 60 Ländern präsent, schützt weltweit mehr als 25 Millionen Anwender und stellt seine Lösungen in 23 Sprachen zur Verfügung.

Pressekontakt

Kristin Petersen
Presse & PR
PAV Germany GmbH
Dr.-Alfred-Herrhausen-Allee 26
47228 Duisburg

Tel: +49 2065 961 352
Fax: +49 2065 961 195
Kristin.Petersen@de.pandasecurity.com
www.pandanews.de
www.pandasecurity.com/germany/