Report:
Endpoint Protection Solutions (07/17)

Autoren: Kevin Börner, Markus Reiniger

Next-Gen Endpoint Protection vs. traditionelle Antivirus-Lösungen

MANAGEMENT SUMMARY

Endpoint-Security-Lösungen müssen sich aktuell ständig an neue Bedrohungen anpassen. Die Einbeziehung von Technologien wie künstlicher Intelligenz (KI) kann die Erkennung von potenziell schädlicher Software signifikant verbessern. Das Ziel dieser Untersuchung ist, einen Vergleich zwischen der neuen Generation von Endpoint-Security-Lösungen und herkömmlichen AV-Produkten, die schon länger am Markt bestehen, zu ziehen. Die Frage, die sich dabei ergibt, lautet: **Ist die Erkennungsrate traditioneller AV-Produkte weiterhin ausreichend oder bieten neue Lösungen einen nennenswerten Vorteil im Kampf gegen unbekannte und neue Malware?**

Bei dem vorliegenden Report handelt es sich um die zweite Ausgabe. Gegenüber der Vorigen wurden mehr AV-Lösungen verglichen, um ein vollständigeres Bild der im Markt erhältlichen Endpoint-Security-Lösungen zu bieten. Zusätzlich wurden neue Testszenarien entwickelt, die einen noch stärkeren Bezug zur Praxis bieten.

Das Ergebnis dieser Untersuchung ist, dass die neue Generation gegenüber herkömmlichen Endpoint-Security-Lösungen einen klaren Vorteil in Bezug auf Erkennungsrate und Performance bietet.

Dem Schutz der Endpoints kommt eine signifikant steigende Bedeutung in der Sicherheitsarchitektur zu. Oft sind Endgeräte der Haupteinstiegspunkt für Attacken auf Unternehmensnetzwerke. Endpoint-Security-Solutions werden daher ständig verbessert und nutzen neueste Entwicklungen der Technologie. Sogenannte „Next-Gen"-Lösungen setzen auf KI, Verhaltensanalysen und intelligente Prozessüberwachung, um einen Endpoint adäquat zu schützen. Dabei ist es irrelevant, ob es sich bei dem Endpoint um eine Workstation, einen Server, PC oder ein Tablet handelt. Signaturbasierte Anti-Viren-Programme bieten bei einer exponential wachsenden Anzahl an Bedrohungen keinen angemessenen Schutz mehr.

UNTERSUCHTE LÖSUNGEN

Next-Gen-Lösungen:

- **CylanceProtect in der Version 1450**
  Cylance nutzt einen ganz neuen Ansatz bei der Bekämpfung von Malware und Exploits. Zur Identifizierung von Malware wird fast ausschließlich auf KI gesetzt, die durch maschinelles Lernen erkennt, ob eine Datei gut- oder bösartig ist. Die KI erkennt Malware durch Untersuchung von Binaries und dlls, ohne sie ausführen zu müssen (pre-execution und predictive). Die neue Version verwendet eine neu entwickelte KI. Sie wurde weiter verbessert, um das mathematische Modell noch schlagkräftiger zu machen. Zusätzlich zur KI nutzt Cylance weitere Schutzmodule wie z.B. Script Control zum Schutz vor VBA-Scripts oder Excel-Makros, die häufig bei Ransomware eingesetzt werden.

- **Palo Alto Networks Traps in der Version 4.0.1**
  Traps ist vor allem auf Exploits spezialisiert, bietet aber auch einen adäquaten Schutz gegen Malware. Neu in der Version 4.0.1 ist eine erweiterte statische Analyse auf Basis von maschinellem Lernen. Ähnlich wie bei CylanceProtect werden Dateien vor ihrer Ausführung überprüft. Software wird an ihrer Ausführung gehindert, wenn die statische Analyse ein entsprechendes Urteil gibt. Das endgültige Schlussurteil bildet aber immernoch die Threat Intelligence Cloud WildFire. Executables werden auf WildFire hochgeladen und dort analysiert und ausgewertet u.a. mit Sandbox-Techniken. Ein entsprechendes Urteil, ob die Executables gut- oder bösartig sind, gibt WildFire dann nach Analyse zurück. Eine Besonderheit von Traps ist, dass es keine – wie von klassischem AV bekannte – Scanning Funktion besitzt. Die Schutzfunktionen greifen wenn versucht wird, eine entspreche Datei auszuführen.

- **SOPHOS Endpoint Protection 2017 mit Intercept X**
  Intercept X erweitert den SOPHOS Anti-Viren-Schutz u.a. um Threat- und Exploit-Erkennung. Unerlaubte Verschlüsselungsaktivitäten (wie z.B. bei Ransomware) werden durch ein gesondertes Modul von Intercept X (CryptoGuard) verhindert. Intercept X soll durch diese Erweiterungen Zero-Day-Malware erkennen, im Vorfeld verhindern und damit den klassischen AV-Ansatz mittels Signaturdatenbanken ergänzen.

Herkömmliche Lösungen:

- **Kaspersky Endpoint Security for Business Advanced 2017**
  Kaspersky Endpoint Security for Business bietet einen Schutz für den PC, Mac und für mobile Endgeräte. Die Schutzmodule sind ähnlich wie bei Symantec EP 14. Es ist ein AV-Scanner mit Signaturdatenbank integriert und zusätzlich besteht die Möglichkeit einer heuristischen Analyse von Dateien. Außerdem sind Module wie ein Password Manager, Schutz für mobile Geräte, eine Firewall und eine Programmkontrolle integriert.

- **McAfee ENS 10.5**
  McAfee bietet zusätzlich zu seinem AV-Scanner neuerdings Machine-Learning Techniken an. Diese werden aufgeteilt in eine statische und dynamische Verhaltensanalyse. Außerdem werden Firewall-Module mit der Endpoint Protection verknüpft. Das Threat-Prevention-Module soll Schutz vor Exploits bieten.

- **Symantec Endpoint Protection 14**
  Symantec Endpoint Protection 14 bietet viele neue und verbesserte Erkennungsfunktionen zusätzlich zu seiner Signaturdatenbank. Es werden z.B. Verhaltensanalysen, maschinelles Lernen sowie statische Analysen benutzt, um Malware zu erkennen.

- **TrendMicro OfficeScan Endpoint Protection**
  OfficeScan stellt wie alle herkömmlichen Lösungen einen AV-Scanner bereit. Seit der neuesten Version werden zusätzlich maschinelle Lernverfahren angeboten, die vor der Ausführung Dateien analysieren sollen. Zusätzlich werden Verhaltensanalysen von Skripts und Browser-Angriffen gemacht. Weitere Module beinhalten Data Loss Prevention (DLP) und benutzerdefinierte Connections zwischen Endpoints.

- **Windows Defender von Microsoft**
  Windows Defender bietet einen herkömmlichen AV-Scanner mit zusätzlich weiteren Features wie einer integrierten Firewall. Das Tool von Microsoft soll eine schlanke Alternative darstellen, damit Nutzer nicht viel Zeit in ihren AV investieren müssen.

Alle getesteten Endpoint-Security-Lösungen bieten eine zentrale Management-Konsole (teilweise in der Cloud und/oder On-Premises), um Policies einstellen zu können oder Deployment und Softwareverteilung zu betreiben. Eine Ausnahme hierbei ist lediglich der Windows Defender, der keine integrierte Softwareverteilung oder Management-Konsole bietet.

TESTKRITERIEN UND METHODIK

Testaufbau:

Der Testaufbau wurde gegenüber dem vorigen Test stark erweitert. Insgesamt wurden in einem ersten Durchgang (**Basis Test**) 2.790 Malware Samples genutzt. Ein Drittel der Samples (930) stellen einzigartige Samples dar. Sie wurden zur weiteren Teststellung auf zwei Arten mutiert. Die Mutation verändert die Signatur der Samples, also den „digitalen Fingerabdruck" in Form eines Hashwertes. Der Wert ist in der Regel dann „unbekannt".

Die erweiterte Mutation nutzt Packtechniken für ausführbare Dateien mithilfe von Software wie mPress und UPX. Damit können Natur und Funktion einer Programmdatei weiter verschleiert werden. Dies macht eine Erkennung schwerer.

Unterschiede durch die Mutation der Samples können z.B. in der Größe der Dateien gegeben sein. Dennoch können mutierte Malware Samples ihren Schadcode weiterhin ausführen. Gewöhnliche AV-Systeme sollten die mutierte Malware anhand ihrer Signaturdatenbank nicht mehr erkennen können.

Test Methodik:

Das Schlüsselkriterium für den Test der Endpoint-Security-Lösungen war die Erkennungsrate. Alle Endpoint-Security-Lösungen wurden unter den gleichen Bedingungen im Zeitraum von 30 Tagen im zweiten Quartal 2017 getestet:

- Die Signaturdatenbanken (falls vorhanden) der Endpoint Security Solutions wurden auf den neuesten Stand gebracht.
- Falls die Endpoint Security Solution eine Scanfunktion hatte (alle getesteten außer Palo Alto Networks Traps), wurden die Malware Samples vor der Ausführung gescannt und die Erkennungsrate ermittelt.
- Abschließend wurden die Malware Samples ausgeführt (Erkennungsrate nach der Ausführung).
- Damit die Malware Samples z.B. weitere bösartige Dateien herunterladen können und die Endpoint-Security-Lösungen ihre besten Ergebnisse zeigen können (z.B. durch Cloud-Anbindung), wurde auch ein Online-Zugriff ermöglicht (Erkennungsrate online).
- Das Testszenario wurde zusätzlich Offline betrieben (Erkennungsrate offline).
- Es wurden originale und mutierte Samples genutzt, die neue unbekannte Hash-Werte aufwiesen.
- Für den Test bestanden die Samples aus einem Mix von 50% Ransomware, 30% Zero-Day und 20% sonstiger Malware. Die sonstige Malware war höchstens 30 Tage alt.
- Die Malware Samples stammen aus verschiedenen bekannten Quellen. Folgende wurden benutzt: http://malwr.com, http://dasmalwerk.com, http://malc0de.com/database/, http://testmyav.com, http://virustotal.com

Zusätzlich wurde ein sogenannter **Holiday Test** durchgeführt. Dabei wurden die virtuellen Maschinen vom Internet getrennt. Nach fünf Tagen wurden neue, frische Malware Samples runtergeladen. Die Signaturdatenbanken wurden nicht aktualisiert. Dieser Test gibt Aufschlüsse über die Endpoint Protection Solutions mit alten nicht upgedateten Datenbanken gegen neue, unbekannte Malware. Er soll ein Szenario simulieren, in dem ein Mitarbeiter bspw. aus dem Urlaub zurück kommt und seinen Rechner nicht sofort aktualisiert.

Für diesen Test wurden 1.440 neue Malware Samples genutzt. Ein Drittel (480) stellten erneut einzigartige Samples dar. Die Test-Methodik war ansonsten die gleiche wie beim Basis Test. Ein Online-Zugriff wurde prinzipbedingt nicht eingerichtet.

ERGEBNISSE UND INTERPRETATION

Next-Gen-Lösungen (CylanceProtect, Palo Alto Networks Traps & SOPHOS mit Intercept X)

Alle Next-Gen-Lösungen erreichten generell sehr hohe Erkennungsraten. CylanceProtect und Palo Alto Networks Traps erkennen durchgängig über 95% der Samples. SOPHOS mit Intercept X ist stark im Ergebnis zurück gefallen und erreichte höchstens 63%.

Eine Besonderheit gibt es für CylanceProtect. Während Traps und Intercept X erst bei Ausführung einer Malware aktiv werden, agiert das KI-Modell von CylanceProtect als einzige Next-Gen-Lösung im Test bereits vorher. CylanceProtect konnte hierbei mit seinem KI-Modell und zusätzlichem Online-Zugriff zu seiner Cloud eine Erkennungsrate von knapp 98% erreichen, ohne die Datei ausgeführt zu haben. Das mathematische KI-Modell klassifiziert bei einem Scan mithilfe von Maschinellem Lernen jede Datei auf einem System nach den Kriterien gut- oder bösartig. Diese Voraussage entscheidet darüber, ob der CylanceProtect Agent die Datei in Quarantäne versetzt oder nicht.

Im Gegensatz zu herkömmlichen Lösungen erkennt die KI neuartige Malware Samples, ohne auf ein ständiges Updaten einer Signaturdatenbank angewiesen zu sein. Stattdessen wird die KI nur ca. alle sechs Monate erneuert, um optimierte Entscheidungsmodelle nachzuladen.

Durch zusätzliche Schutzmodule von CylanceProtect konnten weitere Malware Samples nach ihrer Ausführung gestoppt werden, was die Erkennungsquote weiter erhöht. Hierbei erkennt der Agent z.B. Veränderungen an Programmbibliotheken des Betriebssystems und überwacht zeitgleich die Ausführung bösartiger Makros oder VBA-Skripte. Diese Schutzmodule wurden jedoch kaum in Anspruch genommen, da das mathematische Modell bereits sehr gut war und nahe an 99% Erkennungsrate herankam. Die Reife, die das KI-Modell gezeigt hat ist außerordentlich. Man kann durchaus dieses Modell als das am weitesten Fortgeschrittene aller getesteten Lösungen bezeichnen.

Palo Alto Networks Traps setzt auf die Kombination mehrerer Techniken zur Abwehr von Malware und Exploits. Das System besteht aus einer Reihe von Exploit- und Malware-Protection-Modulen, um die einzelnen Schritte eines Angreifers (die sogenannte „Kill Chain") zu unterbrechen.

Bei einem Exploit wird ein Angriff unterbunden, wenn nur ein Schritt der Kill Chain gestoppt wird. Das passiert häufig bei Ransomware-Kampagnen. Hierbei werden von Traps einzelne Prozesse des Betriebssystems überwacht und geschützt. Bei Malware greift die statische Analyse vor dem Prozess ein und analysiert jede Datei vor der Ausführung. Auch hier war das statische Modell außerordentlich gut. Die zusätzliche Analyse durch die WildFire Threat Intelligence Cloud bietet einen Schutz gegen bekannte und unbekannte Malware und kann False Positives erkennen.

Herkömmliche AV-Lösungen

Bei den traditionellen AV-Ansätzen wäre die alleinige Nutzung ihrer Signaturdatenbank nicht ausreichend gewesen und hätte beispielsweise bei McAfee Ergebnisse von nur 24% Erkennungsrate ermittelt. Durch neuartige Entwicklungen wie statische Analysen, Verhaltensanalysen und Vertraulichkeitsabfragen werden teilweise signifikant höhere Raten von knapp 70% bis 80% (Symantec und Kaspersky) erreicht. Diese liegen jedoch noch immer weit hinter den Next-Gen-Ansätzen von CylanceProtect und Palo Alto Networks Traps zurück.

Enttäuschend waren die neuen Testkandidaten McAfee und TrendMicro. Trotz der Ausrichtung dieser Lösungen auf Next-Gen-Ansätze, können beide keine ausreichenden Erkennungsraten erreichen. Die Modelle dieser Systeme müssen als nicht ausgereift klassifiziert werden.

Windows Defender wird als kostenloser Schutz für Windows Betriebssysteme von Microsoft bereitgestellt und ist daher als Referenz hinzugenommen worden. Erstaunlicherweise kann der Windows Defender teilweise andere Hersteller überbieten.

Der Holiday Test bestätigt die Effektivität der Entscheidungsmodelle von Cylance und Traps. Andere Lösungen bieten keinen ausreichenden Schutz ohne ständiges Updaten ihrer Signaturdatenbanken oder Online-Zugriff.

Lösungen im Vergleich – Basis Test:

Lösung	Szenario			
	Erkennungsrate vor der Ausführung offline	Erkennungsrate vor der Ausführung online	Erkennungsrate nach der Ausführung offline	Erkennungsrate nach der Ausführung online
CylanceProtect 1450	**98,46%**	**99,32%**	**98,84%**	**99,52%**
Palo Alto Networks Traps 4.0.1	*keine Scanfunktion*	*keine Scanfunktion*	**96,30%**	**97,40%**
Kaspersky Endpoint Security for Business Advanced	**61,15%**	**63,48%**	**85,91%**	**86,95%**
Symantec Endpoint Protection 14	**65,70%**	**77,17%**	**74,18%**	**81,56%**
SOPHOS Endpoint Protection + Intercept X	**10,43%**	**18,21%**	**59,73%**	**63,06%**
TrendMicro OfficeScan	**16,02%**	**31,29%**	**40,65%**	**57,07%**
Windows Defender	**27,49%**	**40,04%**	**32,15%**	**44,95%**
McAfee ENS 10.5	**23,80%**	**32,94%**	**29,12%**	**38,44%**

Lösungen im Vergleich - Holiday Test:

Lösung	Szenario	
	Erkennungsrate vor der Ausführung offline	Erkennungsrate nach der Ausführung offline
CylanceProtect 1450	**97,99%**	**98,26%**
Palo Alto Networks Traps 4.0.1	*keine Scanfunktion*	**95,28%**
Kaspersky Endpoint Security for Business Advanced	**36,74%**	**70,00%**
SOPHOS Endpoint Protection + Intercept X	**23,13%**	**58,61%**
Symantec Endpoint Protection 14	**43,96%**	**56,81%**
TrendMicro OfficeScan	**13,75%**	**29,65%**
McAfee ENS 10.5	**18,75%**	**28,96%**
Windows Defender	**21,67%**	**23,47%**

Auslastung

Für das Kriterium der Auslastung wurden CPU- und Arbeitsspeicherauslastung verglichen. Naturgemäß ist die Auslastung bei einem laufenden Angriffsversuch höher. Es zeigten sich allerdings deutliche Unterschiede, wie stark die Belastung zunimmt. Teilweise waren mehr als 20 Prozesse für eine Endpoint Protection Solution aktiv.

Lösung	CPU-Last in %		RAM-Nutzung in MB
	Normal	Incident	
CylanceProtect 1450	**2-4%**	**5-10%**	**20-40 MB**
Palo Alto Networks Traps 4.0.1	**1-2%**	**10%**	**20-50 MB**
SOPHOS Endpoint Protection + Intercept X	**2-4%**	**bis zu 100%**	**Bis zu 400 MB**
Windows Defender	**2-4%**	**bis zu 100%**	**Bis zu 400 MB**
Symantec Endpoint Protection 14	**2-4%**	**bis zu 100%**	**Bis zu 600 MB**
Kaspersky Endpoint Security for Business Advanced	**2-4%**	**bis zu 100%**	**Bis zu 800 MB**
McAfee ENS 10.5	**2-4%**	**bis zu 100%**	**Bis zu 800 MB**
TrendMicro OfficeScan	**2-4%**	**bis zu 100%**	**Bis zu 800 MB**

CylanceProtect und Traps verursachen geringe Auslastungen auf einem Host-System. SOPHOS mit Intercept X verbraucht bei einem Incident hingegen bis zu 100% der CPU-Kapazität und mehrere hundert Megabytes Arbeitsspeicher, was das angegriffene System zumindest für die Zeit des Incidents praktisch unbrauchbar macht. Die hohe Auslastung von Sophos ist seinem klassischen AV-System zuzuschreiben. Das Erweiterungsmodul Intercept X verursacht nur eine geringfügige zusätzliche Auslastung.

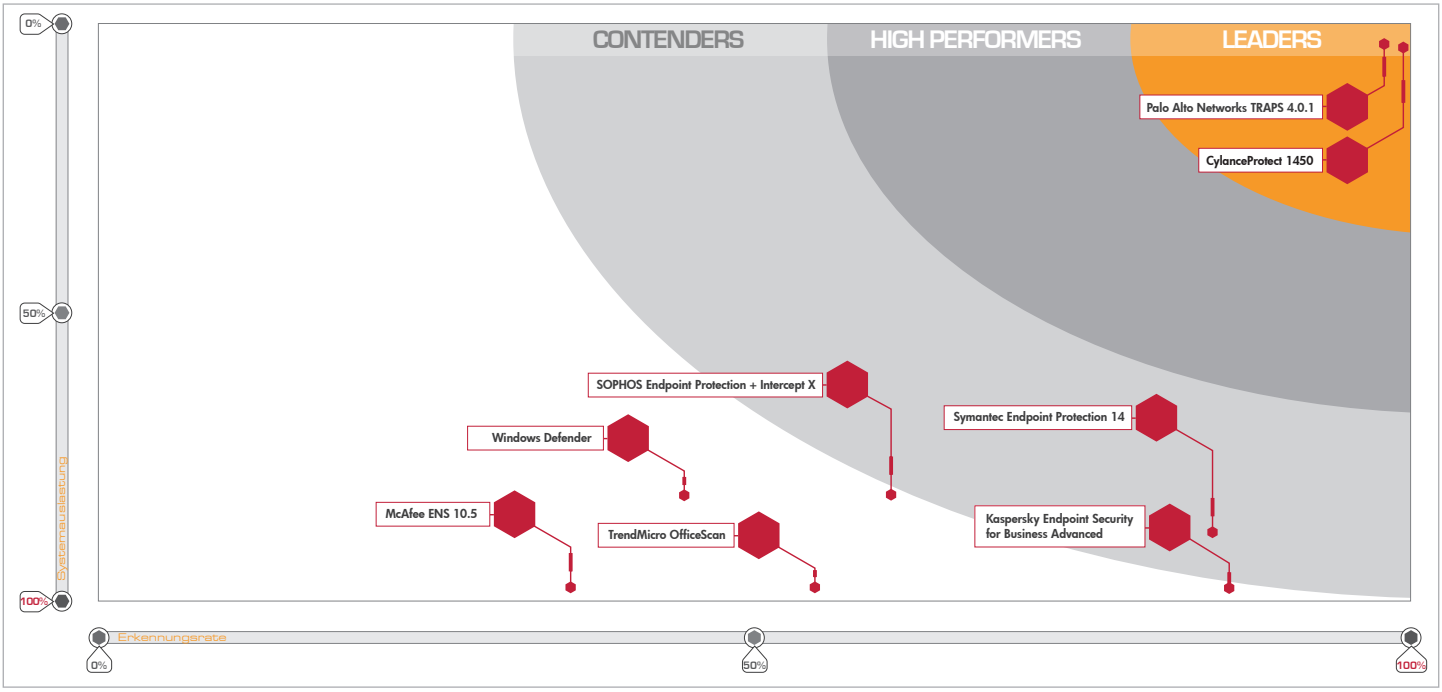
Bei Symantec, Kaspersky, TrendMicro, McAfee und Windows Defender sind ebenso hohe Auslastungen zu beobachten, die bei einem kompletten Scan des Systems die Rechenkapazität bis an die Grenze beanspruchen. Unterschiedlich fällt hier nur die Speicherbelastung ins Gewicht.

Ransomware

Die genutzten Ransomware Samples wurden nicht von allen Endpoint Protection Solutions gefunden. CylanceProtect war die einzige Lösung die alle Ransomware Samples blocken und löschen konnte bevor es zu Schäden kommen konnte. Bekannte Ransomwares, die genutzt wurden waren u.a. GoldenEye, Locky, Petya/Micha, WannyCry, PetWrap/NotPetya, etc.

ZUSAMMENFASSUNG

Zusammenfassend zeigt folgendes Diagramm die Ergebnisse in Bezug auf die Gesamtperformance:



iT-CUBE SYSTEMS AG
Paul-Gerhardt-Allee 24
81245 München, Germany
T: +49 89 2000 148 00
F: +49 89 2000 148 29
info@it-cube.de
www.it-cube.de