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 Anti-Viren System zuzuschreiben. Das Erweiterungsmodul Intercept X verursacht nur eine geringfügige zusätzliche Auslastung.

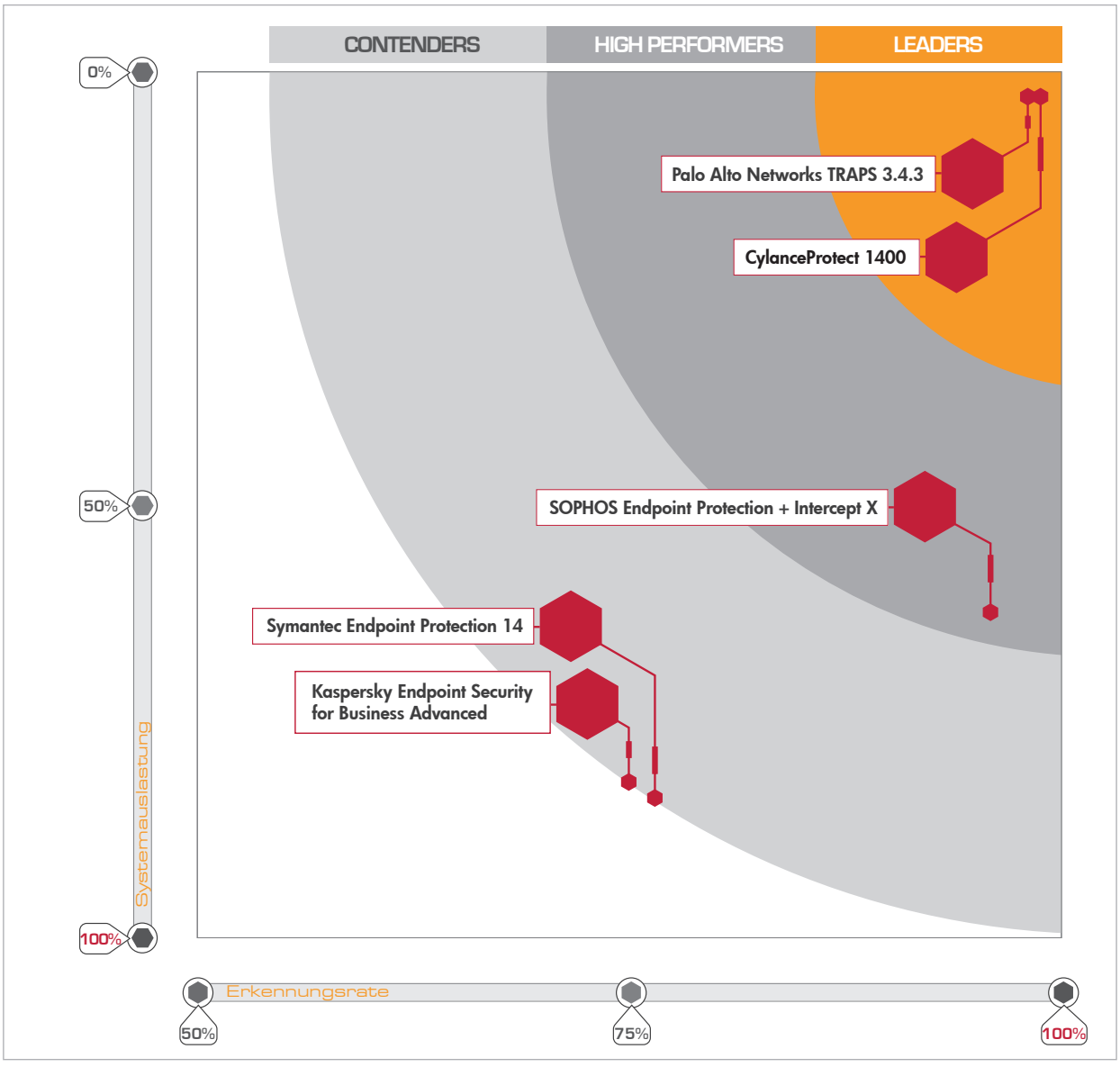
Bei Symantec und Kaspersky sind ebenso hohe Auslastungen zu beobachten, die bei einem kompletten Scan des Systems die Ressourcen bis an die Grenze auslasten.

Ransomware

Alle Endpoint-Protection-Lösungen konnten die in diesem Test genutzten Ransomwares blocken bzw. löschen, bevor es zu Schaden kommen konnte. Bekannte Ransomwares, die genutzt wurden, waren u.a. GoldenEye, Locky, Petya/Micha, etc.

ZUSAMMENFASSUNG

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



Quellen der verwendeten Malware

Die Malware-Samples stammen aus verschiedenen bekannten Quellen. Folgende wurden benutzt:
http://malwr.com, http://dasmalwerk.com, http://malc0de.com/database/, http://testmyav.com

iT-CUBE SYSTEMS AG

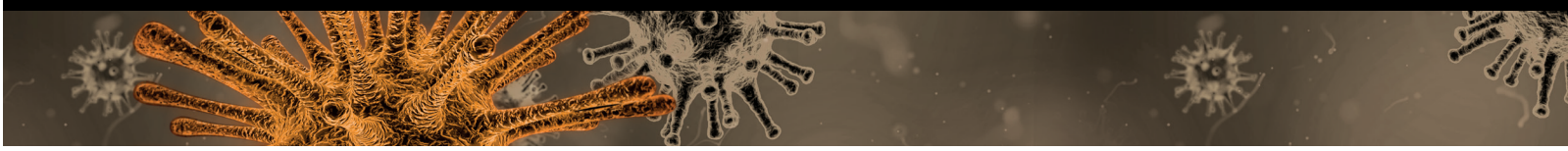
Paul-Gerhardt-Allee 24
81245 München, Germany

T: +49 89 2000 148 00
F: +49 89 2000 148 29

info@it-cube.de
www.it-cube.de

Report:
Endpoint Protection Solutions

Autor: Markus Reiniger



Next-Gen Endpoint Protection vs. traditionelle Antivirus-Lösungen

MANAGEMENT SUMMARY

Endpoint-Security-Lösungen müssen sich in der heutigen Zeit ständig an neue Bedrohungen anpassen. Das Gebot der Stunde ist die Einbeziehung künstlicher Intelligenz (KI), um potenziell schädliche Software zu erkennen. Das Ziel dieser Untersuchung war, einen Vergleich zwischen dieser neuen Generation von Endpoint-Security-Lösungen und herkömmlichen AV-Produkten zu ziehen, die schon länger am Markt bestehen. Die Frage, die sich dabei ergibt, lautet: **Ist die Erkennungsrate traditioneller AV-Produkte weiterhin ausreichend oder bieten die neuen Lösungen einen nenneswerten Vorteil im Kampf gegen unbekannte und neue Malware?**

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 künstliche Intelligenz, 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 1400**
  CylanceProtect geht einen ganz neuen Ansatz bei der Bekämpfung von Malware und Exploits. Zur Identifizierung von Malware wird fast ausschließlich auf künstliche Intelligenz 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). 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.
- **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.
- **Palo Alto Networks Traps in der Version 3.4.3**
  Traps ist vor allem auf Exploits spezialisiert, bietet aber auch einen geeigneten Schutz gegen Malware. Hierfür nutzt Traps die von Palo Alto Networks selbstentwickelte 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 wieder zurück.

Herkömmliche Lösungen:

- **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.
- **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 Anti-Viren 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.

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.

TESTKRITERIEN UND METHODIK

Testaufbau:

Insgesamt wurden 559 Malware Samples, die durch einen Packer (mpress.exe) gepackt wurden, im Test eingesetzt. Das Packen dient der Mutation der Malware-Samples, sodass die Samples neue Signaturen aufweisen und ihr Hash-Wert daher „unbekannt" ist. In der Regel ist die Dateigröße bei einer Mutation kleiner als die des Originals. Dennoch können mutierte Malware Samples ihren Schadcode weiterhin ausführen. Gewöhnliche Anti-Viren-Systeme sollten die Malware anhand ihrer Signaturdatenbank nicht mehr erkennen können. Anschließend wurden die Malware-Samples ausgeführt. 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 1.Qartal 2017 getestet:

- 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 ein Online-Zugriff ermöglicht.
- Es wurden nur mutierte Samples genutzt, die neue unbekannte Hash-Werte aufwiesen.
- Für den Test wurde neueste Zero-Day-Malware (ca.150 Stück) und Ransomware (ca. 70 Stück) benutzt. Die restlichen Malware-Samples waren höchstens 30 Tage alt.
- Die Signaturdatenbanken (falls vorhanden) der Endpoint Security Solutions wurden auf den neuesten Stand gebracht.
- Falls die Endpoint Security Solution eine Scanfunktion hatten (alle getesteten außer Traps), wurden die Malware-Samples vor der Ausführung gescannt.
- Abschließend wurden die Malware-Samples ausgeführt und die Erkennungsrate ermittelt.

ERGEBNISSE UND INTERPRETATION

Lösung	Szenario		
	Erkennungsrate vor der Ausführung und offline	Erkennungsrate vor der Ausführung und online	Erkennungsrate nach der Ausführung und online
CylanceProtect 1400	**75,13%**	**80,32%**	**96,06%**
Palo Alto Networks Traps 3.4.3			**95,89%**
SOPHOS Endpoint Protection + Intercept X		**58,68%**	**95,71%**
Kaspersky Endpoint Security for Business Advanced		**32,20%**	**72,27%**
Symantec Endpoint Protection 14		**44,90**	**75,13%**

Next-Gen-Lösungen (CylanceProtect, Traps & SOPHOS mit Inercept X)

Alle Next-Gen-Lösungen erreichten generell sehr hohe Erkennungsraten. CylanceProtect, Palo Alto Networks Traps und SOPHOS mit Intercept X erkennen über 95% der Samples (Erkennung nach Ausführung mit Onlinezugang).

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 80% erreichen, ohne die Datei ausgeführt zu haben. Das mathematische KI-Modell klassifiziert bei einem Scan 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.

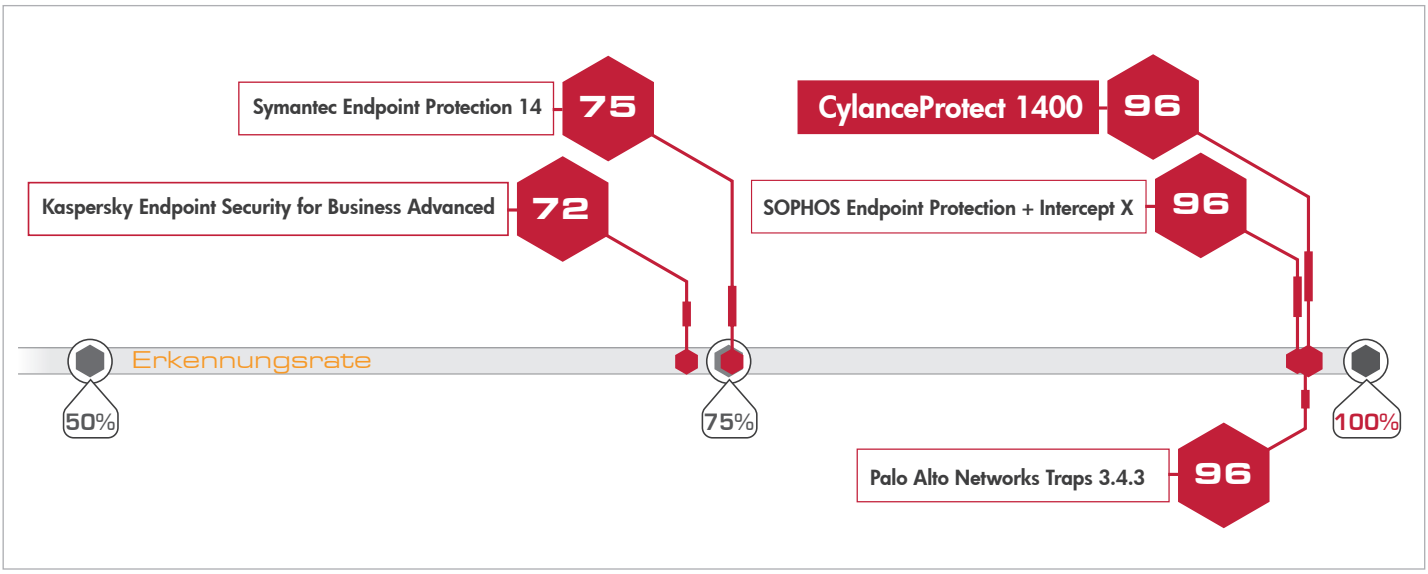
Palo Alto Networks Traps setzt auf die Kombination mehrerer Techniken zur Erkennung und Verhinderung von Malware und Exploits. Das System besteht aus einer Reihe von Exploit- und Malware-Protection-Modulen, um die einzelnen Schritte eines Angreifers (die sogenannte „Kill Chain") zu erkennen und zu blockieren. Bei einem Exploit wird ein Angriff unterbunden, wenn nur ein Schritt der Kill Chain gestoppt wird. Hierbei werden von Traps einzelne Prozesse des Betriebssystems überwacht und geschützt. Die zusätzliche Analyse durch die WildFire Cloud bietet einen Schutz gegen bekannte und unbekannte Malware.

Die Erkennungsrate von SOPHOS vor der Ausführung beruht auf der Verwendung des AV-Scanners.

Herkömmliche AV-Lösungen (Symantec, Kaspersky)

Bei den traditionellen AV-Ansätzen von Kaspersky und Symantec wäre die alleinige Nutzung ihrer Signaturdatenbank nicht ausreichend gewesen und hätte beispielsweise bei Symantec Ergebnisse von nur 40% Erkennungsrate ermittelt. Durch neuartige Entwicklungen wie statische Analysen, Verhaltensanalysen und Vertraulichkeitsabfragen erreichen sie eine signifikant höhere Rate von knapp 70%, liegen jedoch noch immer weit hinter den Next-Gen-Ansätzen zurück.

Die nächste Abbildung verdeutlicht die Ergebnisse anhand der Erkennungsrate.



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:

Lösung	CPU-Last in %		RAM-Nutzung in MB
	Normal	Incident	
CylanceProtect 1400	**2-4%**	**5-10%**	**20-40 MB**
Palo Alto Networks Traps 3.4.3	**1-2%**	**10%**	**20-50 MB**
SOPHOS Endpoint Protection + Intercept X	**2-4%**	**bis zu 100%**	**Bis zu 400 MB**
Kaspersky Endpoint Security for Business Advanced	**2-4%**	**bis zu 100%**	**Bis zu 800 MB**
Symantec Endpoint Protection 14	**2-4%**	**bis zu 100%**	**Bis zu 600 MB**