Anti-Virus Comparative

Malware Protection Test

Dateierkennungstest mit Ausführung

einschließlich Fehlalarmtest

Letzte Überarbeitung: 12. April 2017

www.av-comparatives.org

Inhaltsverzeichnis

Getestete Produkte

- Adware Antivirus Pro 12.0
- Avast Free Antivirus 17.2
- AVG Free Antivirus 17.2
- AVIRA Antivirus Pro 15.0
- Bitdefender Internet Security 21.0
- BullGuard Internet Security 17.0
- CrowdStrike Falcon Prevent 3.0
- Emsisoft Anti-Malware 2017
- eScan Corporate 360 14.0
- ESET Internet Security 10.0
- F-Secure SAFE 14.176
- Fortinet FortiClient 5.4
- Kaspersky Internet Security 17.0
- McAfee Internet Security 19.0
- Microsoft Windows Defender 4.10
- Panda Free Antivirus 18.0
- Seqrite Endpoint Security 17.0
- Symantec Norton Security 22.9
- Tencent PC Manager 12.1
- Trend Micro Internet Security 11.0
- VIPRE Internet Security Pro 9.3

Einführung

Der Malware Protection Test ist eine Erweiterung des Dateierkennungstests, der in den vorangegangenen Jahren durchgeführt wurde. Aufgrund des größeren Umfangs des Tests empfehlen wir, die unten beschriebene Methodik durchzulesen. Bitte beachten Sie, dass wir nicht empfehlen, eines der Produkte nur auf der Basis eines einzelnen Tests oder gar eines Testtyps zu erwerben. Vielmehr raten wir Ihnen, auch unsere anderen neuen Testberichte zu lesen und Faktoren wie Preis, Benutzerfreundlichkeit, Kompatibilität und Support zu berücksichtigen. Mithilfe einer Testversion kann ein Programm im Alltagseinsatz getestet werden, bevor man es kauft.

Grundsätzlich wurden Internet-Security-Suites für Heimanwender für diesen Test genutzt. Jedoch hatten einige Anbieter darum gebeten, ihre (kostenfreien) Antivirus- oder Business[1]-Security-Produkte zu testen.

Getestete Produkte (aktuellste Version, die zum Zeitpunkt des Tests erhältlich waren)[2]:

- Adware Antivirus Pro 12.0.636.1167
- Avast Free Antivirus 17.2.3419.0
- AVG Free Antivirus 17.2.3419.0
- AVIRA Antivirus Pro 15.0.24.146
- Bitdefender Internet Security 21.0.23.1101
- BullGuard Internet Security 17.0.329.1
- CrowdStrike Falcon Prevent 3.0.5113.0
- Emsisoft Anti-Malware 2017.2.0.7219
- eScan Corporate 360 14.0.1400.1957
- ESET Internet Security 10.0.390.0
- F-Secure SAFE 14.176.101
- Fortinet FortiClient 5.4.2.0860
- Kaspersky Internet Security 17.0.0.611(c)
- McAfee Internet Security 19.0.3060
- Microsoft Windows Defender 4.10.14393.0
- Panda Free Antivirus 18.00.00
- Seqrite Endpoint Security 17.00.10.2.2.2
- Symantec Norton Security 22.9.0.71
- Tencent PC Manager 12.1.26375.901
- Trend Micro Internet Security 11.0.1186
- VIPRE Internet Security Pro 9.3.6.3

Für diesen Test wurden 37.999 Malware-Samples genutzt, die nach dem Hinzuziehen von Telemetriedaten mit dem Ziel zusammengestellt wurden, neue, weit verbreitete Samples einzubeziehen, die Anwender in der Praxis gefährden. Malware-Varianten wurden gruppiert, um ein repräsentativeres Test-Set aufzubauen (d. h., um eine Überrepräsentation derselben Malware im Set zu verhindern). Das Sammeln von Samples wurde am 24. Februar 2017 beendet.

Alle Produkte wurden auf einem absolut aktuellen 64-Bit Microsoft Windows 10 Professional RS1 System installiert. Die Produkte wurden Anfang März getestet mit Standardeinstellungen und unter Verwendung ihrer neuesten Updates.

---

[1] Die Programme von CrowdStrike, eScan, Fortinet und Seqrite, die hier getestet wurden, sind Business Security Produkte.

[2] Informationen über zusätzliche Drittanbieter-Engines/Signaturen, die in diesen Produkten verwendet werden: Adaware, BullGuard, Emsisoft, eScan, F-Secure, Lavasoft, Seqrite, Tencent (englische Version) und VIPRE nutzen die Bitdefender-Engine. AVG ist eine umfirmierte Version von Avast.

Methodik

Der Malware Protection Test beurteilt die Fähigkeit eines Sicherheitsprogramms, ein System vor Infektion durch schädliche Dateien vor, während und nach der Ausführung zu schützen. Die Methodik, die für jedes getestete Produkt genutzt wird, ist folgende: Vor der Ausführung werden alle Testsamples On-Access- und On-Demand-Scans durch das Sicherheitsprogramm ausgesetzt, wobei jeder Scan sowohl offline als auch online durchgeführt wird. Alle Samples, die von keinem dieser Scans erkannt wurden, werden dann auf dem Testsystem, mit verfügbarem Internet-/Cloud-Zugriff, ausgeführt, um zu ermöglichen, dass Verhaltenserkennungsfeatures ins Spiel kommen. Wenn ein Produkt nicht alle Veränderungen verhindert oder rückgängig macht, die von einem bestimmten Malware-Sample in einem festgelegten Zeitraum vorgenommen wurden, wird dieser Testfall als Versagen gewertet. Wenn der Anwender aufgefordert wird, zu entscheiden, ob ein Malware-Sample laufen darf, und im Falle der schlechtesten Anwenderentscheidung das System kompromittiert wird, wird der Testfall als „anwenderabhängig“ bewertet.

Offline- gegen Online-Erkennungsraten

Viele der Produkte im Test nutzen Cloud-Technologien, wie zum Beispiel Reputationsdienste oder cloud-basierte Signaturen, die nur zur Anwendung kommen können, wenn es eine aktive Internetverbindung gibt. Durch die Ausführung von On-Demand- und On-Access-Scans – sowohl offline als auch online – gibt der Test Aufschluss darüber, wie cloud-abhängig jedes Produkt ist und wie gut es das System schützt, wenn keine Internetverbindung verfügbar ist. Wir würden vorschlagen, dass Anbieter von überwiegend cloud-abhängigen Produkten ihre Anwender angemessen warnen für den Fall, dass die Verbindung zur Cloud unterbrochen wird, da dies den gebotenen Schutz erheblich beeinträchtigen könnte. Während wir in unserem Test überprüfen, ob die Cloud-Dienste des entsprechenden Sicherheitsanbieters erreichbar sind, sollten sich Anwender darüber im Klaren sein, dass nur online zu sein, nicht automatisch bedeutet, dass der Cloud-Service ihres Produktes erreichbar ist/ordnungsgemäß funktioniert. AMTSO[3] hat einen rudimentären Test, um das ordnungsgemäße Funktionieren von cloud-unterstützten Produkten zu verifizieren.

Zur Information der Leser und aufgrund der häufigen Anfragen von Magazinen und Analysten haben wir auch angegeben, wie viele der Samples von jedem Sicherheitsprogramm bei den offline und online Detection-Scans erkannt wurden.

	OFFLINE Detection Rate	ONLINE Detection Rate	ONLINE Protection Rate	False Alarms
Adaware	99.7%		99.89%	2
Avast	98.8%	99.8%	99.97%	20
AVG	98.8%	99.8%	99.97%	20
AVIRA	98.0%	99.9%	99.98%	2
Bitdefender	99.7%		99.95%	2
BullGuard	99.7%		99.97%	3
CrowdStrike	93.4%		99.67%	125
Emsisoft	99.7%		99.83%	4
eScan	99.7%		99.97%	2
ESET	99.7%		99.70%	0
Fortinet	99.1%		99.35%	4
F-Secure	99.7%	99.8%	99.93%	6
Kaspersky Lab	96.0%	99.9%	99.98%	4
McAfee	78.8%	99.4%	99.62%	9
Microsoft	98.2%	99.4%	99.64%	0
Panda	65.6%	99.6%	99.98%	1
Seqrite	99.7%		99.89%	3
Symantec	86.8%	99.8%	99.89%	96
Tencent	99.7%		99.94%	3
Trend Micro	63.7%	98.6%	100%	29
VIPRE	99.7%		99.96%	3

average	94.0%	99.3%	99.86%	16
min	63.7%	93.4%	99.35%	0
max	99.7%	99.9%	100%	125

[3] http://www.amtso.org/feature-settings-check-for-desktop-solutions

Erkennung gegen Schutz

Der Dateierkennungstest, den wir in den vorangegangenen Jahren durchgeführt haben, war ein reiner Erkennungstest. Das heißt, es wurde nur die Fähigkeit der Sicherheitsprogramme getestet, schädliche Programmdateien vor ihrer Ausführung zu erkennen. Diese Fähigkeit bleibt ein wichtiges Feature eines Antivirenproduktes und ist wesentlich für jeden, der sich beispielsweise vergewissern möchte, dass eine Datei harmlos ist, bevor er diese an Freunde, Familie oder Kollegen weiterleitet.

Der vorliegende Malware Protection Test überprüft nicht nur die Erkennungsraten der teilnehmenden Programme, sondern auch ihre Schutzfähigkeiten, d. h., die Fähigkeit zu verhindern, dass ein Schadprogramm tatsächlich Veränderungen am System vornimmt. In einigen Fällen erkennt ein Antivirenprogramm vielleicht ein Malware-Sample nicht, wenn es inaktiv ist, aber es wird erkannt, wenn es ausgeführt wird. Außerdem nutzt eine Reihe von AV-Produkten Verhaltenserkennung, um nach Versuchen eines Programmes zu suchen, Systemveränderungen auszuführen, die für Malware typisch sind, und diese zu blockieren. Unser neuer Malware Protection Test misst die Gesamtfähigkeit von Sicherheitsprodukten, Systeme vor Schadprogrammen zu schützen, vor, während oder nach ihrer Ausführung. Er ergänzt unseren Real-World Protection Test, der seine Malware-Samples von live URLs bezieht, und erlaubt Features wie zum Beispiel URL-Blocker, ins Spiel zu kommen. Der Malware Protection Test repliziert effektiv ein Szenario, in dem Malware über ein LAN oder Wechseldatenträger wie USB-Sticks (statt über das Internet) in ein System eingebracht wird. Beide Tests beinhalten die Ausführung jeglicher Malware, die nicht von anderen Features erkannt wird und somit zulässt, dass Features der „letzte Verteidigungslinie“ ins Spiel kommen.

Eine der Bedeutsamkeiten von Cloud-Erkennungsmechanismen ist folgende: Malware-Autoren suchen ständig nach neuen Methoden, um Erkennungs- und Sicherheitsmechanismen zu umgehen. Die Nutzung der Cloud-Erkennung ermöglicht Anbietern, verdächtige Dateien in Echtzeit zu erkennen und zu klassifizieren, um die Anwender vor derzeit unbekannter Malware zu schützen. Einige Teile der Schutztechnologie in der Cloud zu haben, hindert Malware-Entwickler daran, sich schnell an neue Erkennungsmöglichkeiten anzupassen.

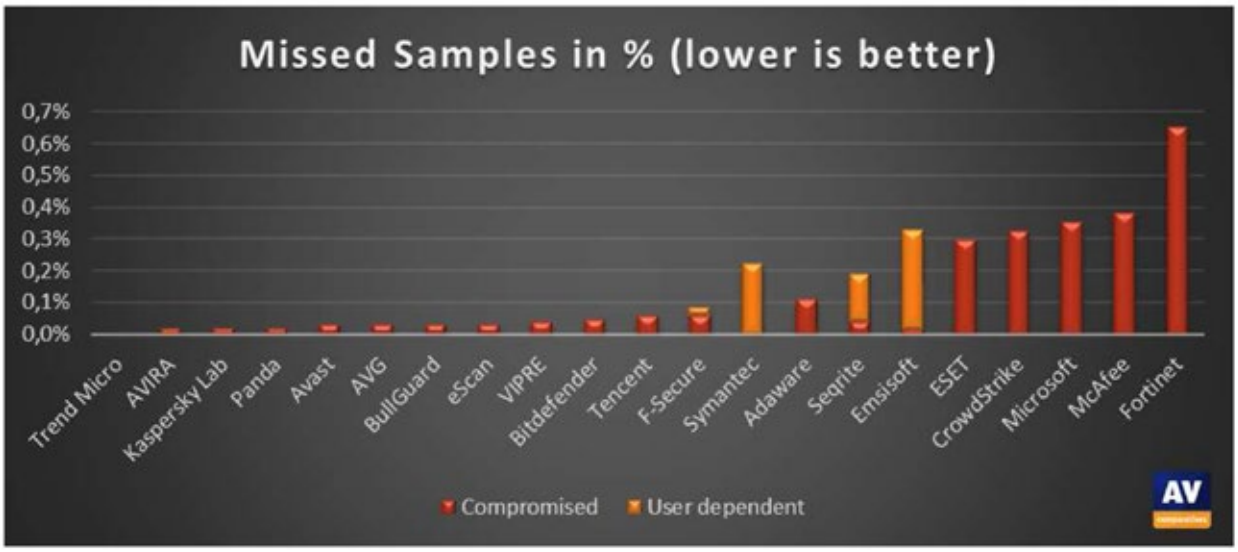
Ergebnisse

Gesamte Online-Erkennungsraten (in Gruppen zusammengefasst):

Berücksichtigen Sie bitte auch die Fehlalarmraten, wenn Sie sich die folgenden Erkennungsraten anschauen.

	Blocked	User dependent	Compromised	PROTECTION RATE[4] Blocked % + (User dependent % / 2)	Cluster[5]
Trend Micro	37999	-	-	100%	1
AVIRA	37994	-	5	99.99%	1
Kaspersky Lab	37993	-	6	99.98%	1
Panda	37992	-	7	99.98%	1
Avast, AVG, BullGuard, eScan	37987	-	12	99.97%	1
VIPRE	37984	-	15	99.96%	1
Bitdefender	37981	-	18	99.95%	1
Tencent	37978	-	21	99.94%	1
F-Secure	37968	9	22	99.93%	1
Symantec	37916	83	-	99.89%	2
Adaware	37957	-	42	99.89%	2
Seqrite	37927	58	14	99.89%	2
Emsisoft	37877	117	5	99.83%	2
ESET	37886	-	113	99.70%	3
CrowdStrike	37875	-	124	99.67%	3
Microsoft	37864	-	135	99.64%	3
McAfee	37854	-	145	99.62%	3
Fortinet	37751	-	248	99.35%	4

Das Test-Set enthielt 37.999 neuere/weit verbreitete Samples aus den vergangenen Wochen/Monaten.



[4] Anwenderabhängigen Fällen werden nur halbe Punkte gegeben. Beispiel: Wenn ein Programm 80 % selbst blockiert und weitere 20 % der Fälle sind anwenderabhängig, dann geben wir halbe Punkte für die 20 %, d. h. 10 %, also bekommt es insgesamt 90 %.

[5] Hierarchische Cluster-Methode: Definition von Clustern mithilfe der durchschnittlichen Vernetzung zwischen Gruppen (euklidischer Abstand), basierend auf der Schutzrate (Siehe Dendrogramm auf Seite 10).

False Positive (Fehlalarm) Test

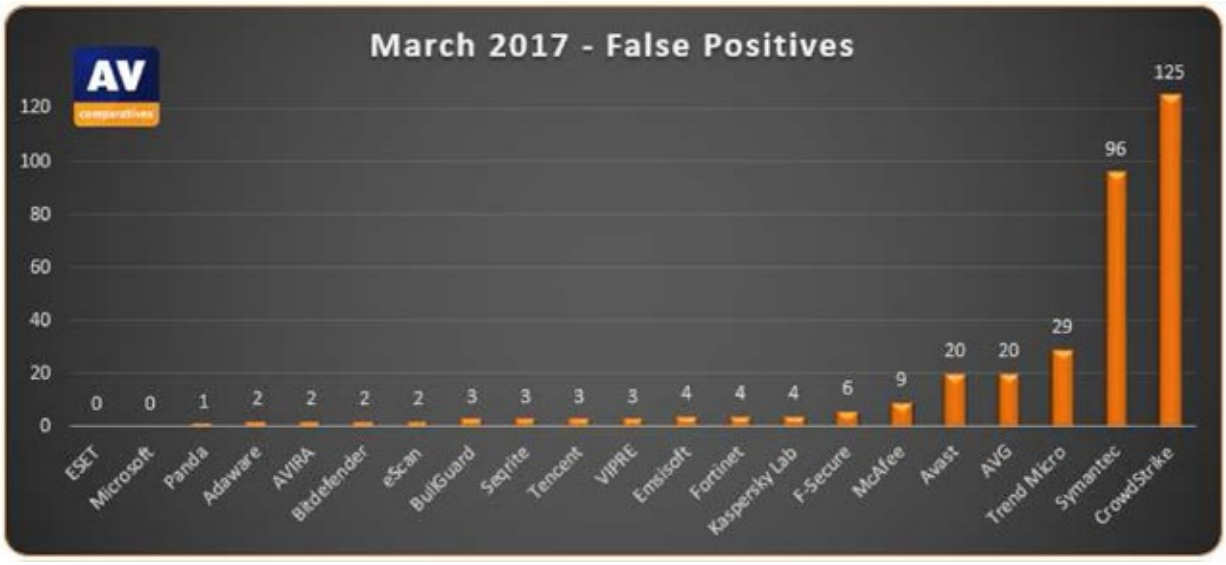
Um die Qualität der Dateierkennungsfähigkeiten (Fähigkeit, zwischen guten und schädlichen Dateien zu unterscheiden) von Antivirenprodukten besser beurteilen zu können, bieten wir einen False Positive Test. Fehlalarme können manchmal genauso viel Ärger verursachen wie eine tatsächliche Infektion. Bitte berücksichtigen Sie die Fehlalarmrate, wenn Sie sich die Erkennungsraten ansehen, da ein Produkt, das zu Fehlalarmen neigt, leichter höhere Erkennungsraten erzielen könnte. In diesem Test wird unser gesamtes Clean Set gescannt und ein repräsentativer Teilbereich des Clean Sets wird ausgeführt.

False Positive Resultate

Anzahl von Fehlalarmen, die in unserem Set an sauberen Dateien gefunden wurden (niedriger ist besser):

1.	ESET, Microsoft	0	keine/sehr wenige FPs
2.	Panda	1	
3.	Adaware, AVIRA, Bitdefender, eScan	2	
4.	BullGuard, Seqrite, Tencent, VIPRE	3	
5.	Emsisoft, Fortinet, Kaspersky Lab	4	wenige FPs
6.	F-Secure	6	
7.	McAfee	9	
8.	Avast, AVG	20	
9.	Trend Micro	29	viele FPs
10.	Symantec	96	sehr viele FPs
11.	CrowdStrike	125	bemerkenswert viele FPs

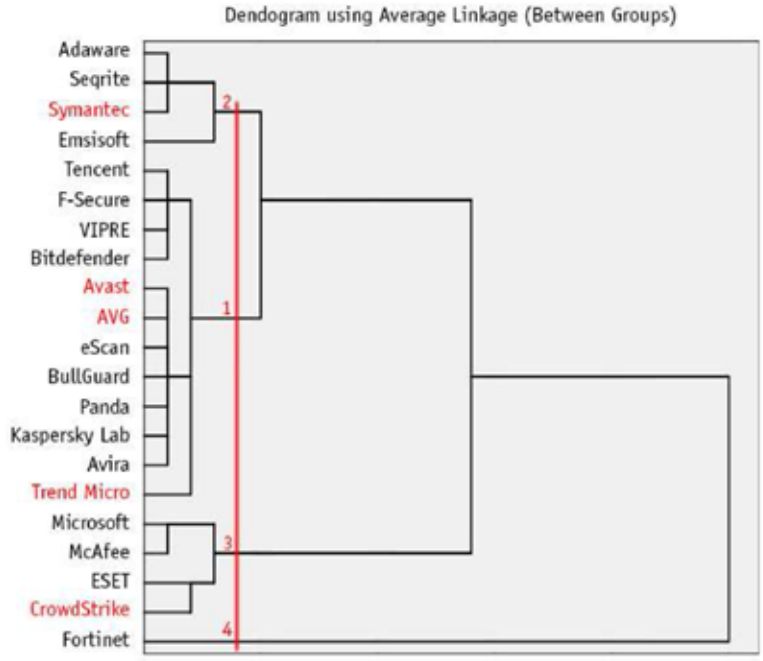
Einzelheiten über die entdeckten Fehlalarme (einschließlich ihrer angenommenen Prävalenz) können Sie einem gesonderten Bericht entnehmen. Sie finden ihn unter: http://www.av-comparatives.org/wp-content/uploads/2017/04/avc_fps_201703_en.pdf



Ein Produkt, das erfolgreich ist bei der Erkennung eines hohen Prozentsatzes an schädlichen Dateien, jedoch viele Fehlalarme hat, ist nicht notwendigerweise besser als ein Produkt, das weniger schädliche Dateien entdeckt, aber weniger Fehlalarme verursacht.

Ranking-System

Hierarchische Cluster-Analyse



Dieses Dendrogramm zeigt die Ergebnisse der Cluster-Analyse[6] bezüglich der Online-Schutzraten. Es gibt an, auf welchem Grad der Ähnlichkeit die Cluster verbunden sind. Die rote Linie definiert den Grad der Ähnlichkeit. Jeder Schnittpunkt gibt eine Gruppe an.

Die Malware-Schutzraten sind von den Testern gruppiert, nachdem die Cluster betrachtet wurden, die mithilfe der hierarchischen Cluster-Methode gebildet wurden. Jedoch halten sich die Tester nicht starr daran in Fällen, bei denen es keinen Sinn hätte. Zum Beispiel werden in einem Szenario, in dem alle Produkte niedrige Schutzraten erzielen, nicht automatisch die mit den höchsten Raten auch das höchstmögliche Gütesiegel erhalten.

	Protection Rate Clusters/Groups (given by the testers after consulting statistical methods)			
	4	3	2	1
Very few (0-1 FP's) Few (2-10 FP's)	TESTED	STANDARD	ADVANCED	ADVANCED+
Many (11-50 FP's)	TESTED	TESTED	STANDARD	ADVANCED
Very many (51-100 FP's)	TESTED	TESTED	TESTED	STANDARD
Remarkably many (over 100 FP's)	TESTED	TESTED	TESTED	TESTED

Alle Produkte, die an diesem Test teilgenommen haben, erzielten hohe Werte (über 99 %) im Verhältnis zu einfachen Dateierkennungstests. Dafür gibt es zwei Gründe. Erstens: Es wurde ein repräsentatives Set von weit verbreiteten Malware-Samples genutzt. Zweitens: Zusätzlich zur On-Demand-Erkennung enthält der Test On-Access-Erkennung und On-Execution-Schutz. Aufgrund des sehr hohen Gesamtstandards, der somit erreicht wurde, sind die Minimalscores, die für die verschiedenen Gütesiegel benötigt werden, auch sehr hoch im Vergleich zu anderen Tests.

[6] Weitere Informationen über die Cluster-Analyse finden Sie in diesem leicht verständlichen Tutorial: http://strata.uga.edu/software/pdf/clusterTutorial.pdf

Award-Level, die in diesem Test erreicht wurden

AV-Comparatives bietet Rangauszeichnungen, die sowohl auf den False Positives Levels als auch auf den Schutzraten basieren. Da dieser Bericht auch die reinen Erkennungsraten und nicht nur die Awards enthält, können sich Anwenderexperten, die sich weniger Sorgen um Fehlalarme machen, ausschließlich auf die Schutzrate verlassen. Einzelheiten darüber, wie die Awards vergeben werden, sind auf Seite 10 dieses Berichtes zu finden.

AWARDS (based on protection rates and false alarms)	PRODUCTS
AV comparatives ADVANCED+ ★★★ MALWARE PROTECTION TEST MAR 2017	✓ AVIRA ✓ Kaspersky Lab ✓ Panda ✓ eScan ✓ BullGuard ✓ VIPRE ✓ Bitdefender ✓ Tencent ✓ F-Secure
AV comparatives ADVANCED ★★ MALWARE PROTECTION TEST MAR 2017	✓ Trend Micro* ✓ Avast* ✓ AVG* ✓ Adaware ✓ Seqrite ✓ Emsisoft
AV comparatives STANDARD ★ MALWARE PROTECTION TEST MAR 2017	✓ ESET ✓ Microsoft ✓ McAfee
AV comparatives TESTED MALWARE PROTECTION TEST MAR 2017	✓ Symantec* ✓ CrowdStrike* ✓ Fortinet

* Diese Produkte haben aufgrund von Fehlalarmen[7] niedrigere Awards erhalten.

[7] Bitte lesen Sie Einzelheiten und Kommentare in: http://www.av-comparatives.org/wp-content/uploads/2017/04/avc_fps_201703_en.pdf

Copyright und Haftungsausschluss

Weitere Informationen über AV-Comparatives und die Testmethoden finden Sie auf unserer Webseite.

AV-Comparatives (April 2017)