TEST: SECURITY-SUITEN

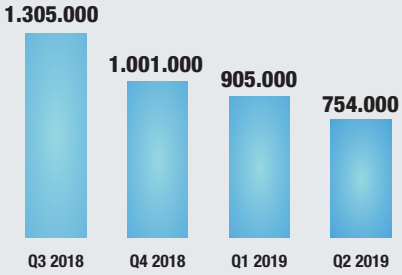
Sicherheit für jeden Rechner

Die Bedrohungslage wandelt sich rasant, und nur ein gutes Schutzprogramm kann mit den Böse-wichten mithalten.

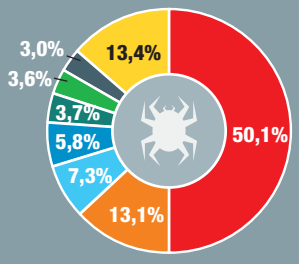
■ ANDREAS DUMONT

Böswillige Android-Apps

Mobile Malware wächst zwar immer langsamer, doch die Gesamtzahl steigt. Von Entwarnung kann also keine Rede sein. Quelle: Kaspersky



Neue Malware nach Verhalten



Etwas mehr als die Hälfte der neu entdeckten Malware-Samples sind Trojaner. Quelle: Kaspersky

- Trojaner
- Virus
- Adware
- Wurm
- Backdoor
- Ransomware
- Downloader
- sonstige

346.000

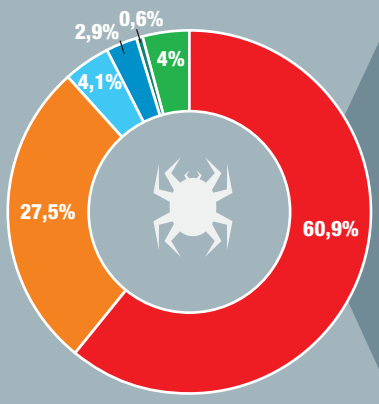
neue Malware-Dateien laufen täglich bei Kaspersky ein.

Quelle: Kaspersky

Angriffe mit Ransomware

Nov 18	37879
Dez 18	33446
Jan 19	35205
Feb 19	32614
Mär 19	36598
Apr 19	33738
Mai 19	32521
Jun 19	28296
Jul 19	33397
Aug 19	28178
Sep 19	26093
Okt 19	30093

Die Zahl der Ransomware-Attacken unterliegt saisonalen Schwankungen, ist aber insgesamt leicht rückläufig. Quelle: Symantec



Verwendete Benutzernamen bei erfolgreichen Angriffen

Viele Anwender machen es den Angreifern leicht, indem sie einfach zu erratende Benutzernamen und Passwörter verwenden. Quelle: Kaspersky

- admin
- root
- default
- support
- guest
- sonstige

Die Zahl der Bedrohungen nimmt seit vielen Jahren stetig zu. Noch in diesem Jahr könnte die Schallmauer von einer Milliarde Malware-Samples fallen. Wer dennoch auf einen Virenschutz verzichtet, beweist Mut zum Risiko. Die Schutzprogramme selbst nehmen ebenfalls stetig zu. Heutzutage gibt es keine schlichten Anti-Viren-Programme mehr, sondern nur noch komplette Security-Suiten mit zahlreichen Zusatzfunktionen, die bisweilen gar nichts mit Sicherheit zu tun haben. Puristen und Performance-Fanatikern ist die Überfrachtung der Schutzsoftware ein Dorn im Auge. Sie verlassen sich mitunter lieber auf den vergleichsweise spartanischen und unaufdringlichen Defender von Microsoft, der zudem nichts kostet. Doch genügt das?

Besser als nichts

Der Microsoft Defender wurde vor Jahren noch belächelt wegen seiner sehr bescheidenen Erkennungsraten. Security ist nun mal nicht die Kernkompetenz von Microsoft. Doch in jüngster Zeit hat das Schutzprogramm aufgeholt. Wenn es mit einer aktiven Malware konfrontiert wird, erkennt es diese in nahezu allen Fällen.

Doch die gute Erkennungsrate hat eine Kehrseite: Sie wurde mit einer sehr hohen Zahl an falschen Alarmen erkauft. Schwach ist die Offline-Detection-Rate, also der klassische Festplattenscan, mit der schlechtesten Erkennungsrate im Testfeld. Somit ist der Defender zwar besser als kein Virenscanner, doch für einen echten Schutz kommt man an den Schwergewichten der Branche kaum vorbei. Ein Aspekt sollte nicht unerwähnt bleiben: Die enorme Verbreitung des Defenders könnte eines Tages zum Problem werden. Denn Windows ist nicht gerade arm an Sicherheitslücken, wie die monatlichen Updates zeigen. Wenn eine Schwachstelle den Defender betrifft, ist auf einen Schlag ein Großteil der PC-Landschaft gefährdet.

Android im Visier

Die Angriffe auf Android-Smartphones häufen sich. Sicherheitsexperten von G Data haben ermittelt, dass durchschnittlich alle acht Sekunden eine neue Malware für Android erscheint. Da Smartphones als ständiger Begleiter nahezu unentbehrlich sind, bilden sie für Angreifer ein attraktives Ziel. Die Zahl der bekannten Schad-Apps hat inzwischen die 100-Millionen-Marke überschritten.

Zwar hat Google zwischenzeitlich Maßnahmen ergriffen, seinen Store besser abzusichern, aber der Trend ist ungebrochen. Ein Ärgernis sind Unternehmen, die aus Kostengründen Apps ausschließlich in alternativen Quellen anbieten, darunter auch populäre Spiele wie Fortnite. Dabei stellt der Verzicht auf die Installation von Apps aus unsicheren Quellen eine zentrale Grundregel dar. Die Hersteller der Security-Suiten tragen der Verbreitung mobiler Malware Rechnung und bieten ihre Pakete meist als *Multi-Device* oder *Cross-Device* an, sodass sich damit nicht nur der PC mit Windows 10, sondern auch Smartphones mit Android schützen lassen.

Performance ist Trumpf

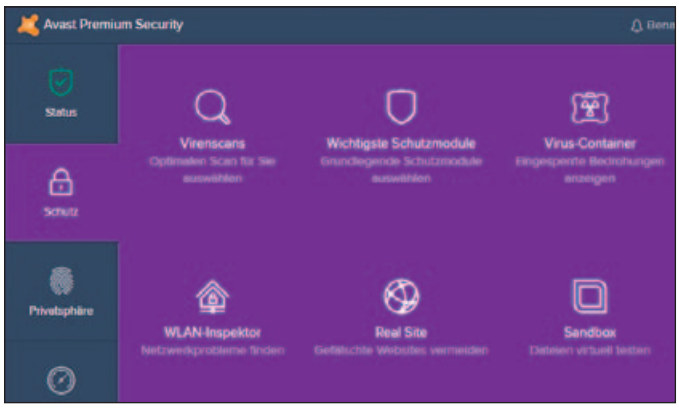
Eine Gruppe steht aufgeblähten Suiten besonders skeptisch gegenüber: die Gamer. Sie legen besonderen Wert darauf, dass die Geschwindigkeit des PCs nicht vermindert wird, und sie können auf den zusätzlichen Schnick-Schnack verzichten. Folgerichtig lässt sich vereinzelt bereits ein gegenläufiger Trend beobachten hin zu Spezial-Lösungen. Wer kein Online-Banking macht, braucht keinen Banking-Browser. Wer keine Kinder hat, braucht keine Kindersicherung. Und wer sich auskennt, nimmt die Systemoptimierung selbst in die Hand. McAfee etwa bringt mit der McAfee Gamer Security eine abgespeckte Version seiner Security-Suite speziell für Spieler heraus. Andere Hersteller haben einen besonderen Spiele-Modus eingebaut, der die Schutz-Software während eines Spiels zum Schweigen bringt. Weitere Spezial-Versionen könnten folgen, etwa für Eltern, Studenten oder Singles.

Aber auch Nicht-Gamer freuen sich über ein Schutzprogramm, das Start und laufenden Betrieb nicht ausbremst. Insofern haben wir uns dieses Jahr entschlossen, die Abzüge für schlechte Performance auf bis

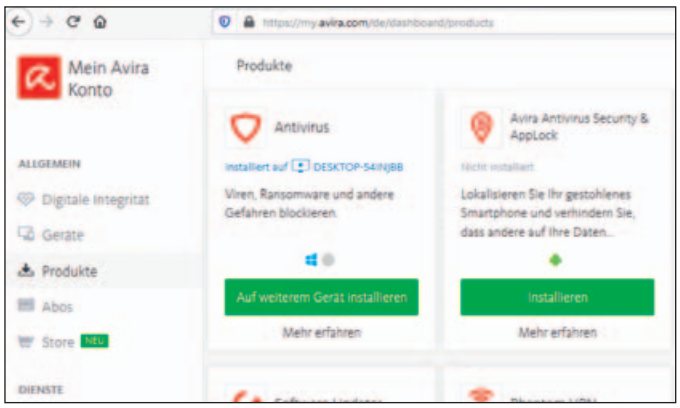
Andreas Dumont, Autor PC Magazin

Expertenmeinung

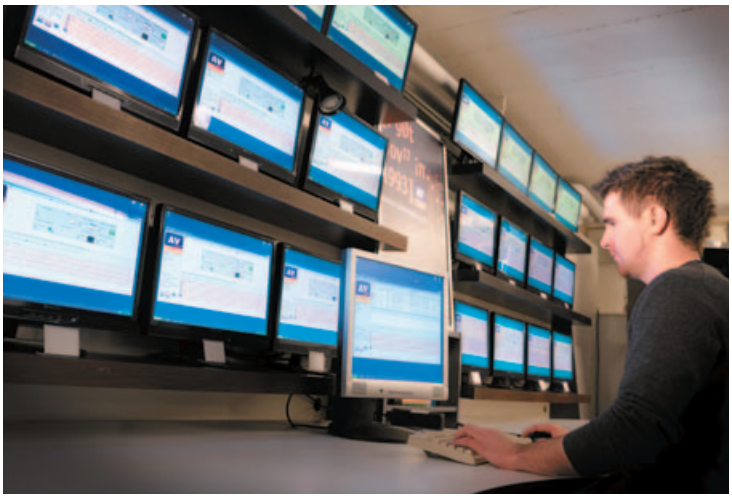
Die Erkennungsraten taugen kaum mehr als zentrales Entscheidungsmerkmal; hier sind die Unterschiede eher gering. Stattdessen rückt die Ausstattung in den Vordergrund. Hier gilt es genau zu überlegen, was Sie tatsächlich benötigen. Nicht zuletzt spielen auch die Optik und der persönliche Geschmack eine Rolle. Kachel-Layout oder Steuerung im Browser? Lila oder doch lieber grün? Schließlich sollte sich auch der Nerv-Faktor regeln lassen. Manch einer mag von seiner Security-Suite nur in Notfällen informiert werden; andere wollen alles wissen und sich über sämtliche Vorgänge unterrichten lassen.



Avast hat als Alleinstellungsmerkmal eine mutige Farbgebung und schneidet bei der Malware-Erkennung sehr gut ab.



Avira lässt sich im Wesentlichen über den Browser steuern und einrichten. Das Programm bietet den besten Virenschutz.



Das Innsbrucker Testlabor AV Comparatives überprüft und bewertet Sicherheits-Software.

zu 20 Prozent deutlich zu erhöhen. Wirklich überzeugen konnten uns hier nur Eset, McAfee, Avast und Kaspersky.

Ransomware leicht rückläufig

Ransomware zählt fraglos zu den gemeinsten Malware-Arten: Sobald ein entsprechender Trojaner auf den PC gelangt, beginnt er sein Zerstörungswerk, indem er Daten verschlüsselt. Anschließend fordert er Lösegeld für den Schlüssel zur Wiederherstellung der Daten. Ransomware ist neben Cryptojacking die wichtigste Einnahmequelle für Cyberkriminelle. Die Zahl der Ransomware-Angriffe ging zuletzt insgesamt leicht zurück. Allerdings nahmen Angriffe auf Unternehmen deutlich zu. Der Grund liegt auf der Hand: Unternehmen können mehr bezahlen. Für das kommende Jahr rechnen Experten mit einer gleichbleibenden Bedrohungslage – kein Grund zur Entwarnung.

Comeback für Cryptojacking

Cyrptojacking hatte 2018 Hochkonjunktur. Die Preise für Bitcoin, Monero und andere Kryptowährungen schwangen sich in ungeahnte Höhen. Somit war es sehr lukrativ, ahnungslosen PC-Anwendern eine Cyrptojacking-Malware unterzujubeln und damit unbemerkt Rechenleistung abzuzapfen für Krypto-Mining. Die Belohnung für einen erfolgreich in die Blockchain eingefügten Block liegt derzeit immerhin bei 12,5 Bitcoins. Cryptojacking bietet aus Sicht der Angreifer noch einen weiteren Charme: Anders als etwa eine Verschlüsselung durch Ransomware, bleibt etwas abgezweigte Rechenleistung oftmals lange Zeit unbemerkt. Dass sich Cryptojacking momentan eher auf dem absteigenden Ast befindet, liegt am Preisverfall der Kryptowährungen. Beispiel Bitcoin: Nach einem Höchststand von über 18.000 Euro im Januar 2018 ging es steil bergab auf unter 3000 Euro im Dezember. Mittlerweile steht der Kurs aber wieder bei knapp 8000 Euro, sodass für die kommenden Monate wieder mit einem Anstieg von Cryptojacking zu rechnen ist. Das gilt insbesondere für das erste Halbjahr 2020, bis sich irgendwann gegen Mitte des Jahres der Coin Reward auf 6,25 Bitcoins halbiert.

Neue Bedrohungen

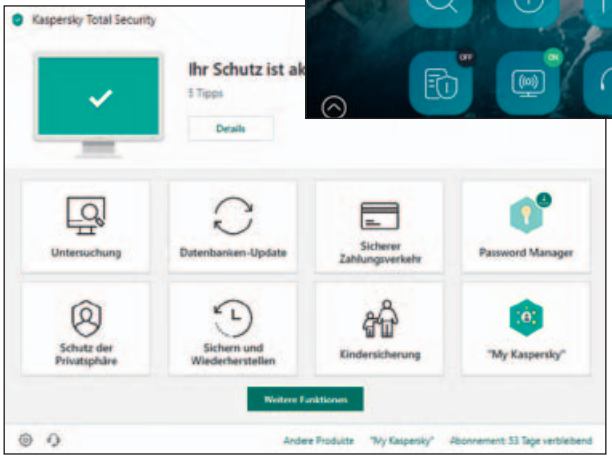
Freilich lässt sich schwer vorhersagen, was sich die Cyberkriminellen in naher Zukunft alles einfallen lassen. Es gibt jedoch Anzeichen, das Formjacking-Angriffe deutlich zunehmen, denn sie sind simpel und profitabel. Angreifer bringen dabei bösartigen Code auf den Webseiten von Online-Händlern unter. Der Code ermöglicht es ihnen dann, Kreditkarten-Informationen von Kunden abzugreifen. Laut Symantec sind davon schon rund 4800 Online-Shops im Monat betroffen. Eines ist gewiss – langweilig wird es nicht. Das Katz-und-Maus-Spiel zwischen Cybersecurity-Branche und Kriminellen wird wohl niemals enden.

Fazit

Das beste Schutzniveau im Test bieten in dieser Reihenfolge Avira, Kaspersky und Bitdefender. Der russische Hersteller Kaspersky ist Testsieger, da hier auch Ausstattung und Performance überzeugen. Kaspersky erzielte bei den Zusatzfunktionen die höchste Punktzahl. Knapp dahinter landete der rumänische Hersteller Bitdefender, der gleichzeitig das beste Preis-Leistungs-Verhältnis aufweist und in Sachen Schutz nur einen Zehntel Punkt hinter dem Testsieger liegt. Eset verdiente sich einen Platz auf dem Treppchen durch die Bestleistung bei der Performance.

Eine Überraschung ist der vierte Platz von McAfee, das zuletzt stets in der hinteren Hälfte zu finden war. Die guten Performance-Werte tragen hierzu bei. Der letzte Platz für den Defender von Microsoft verwundert nicht, aber insbesondere G Data und F-Secure haben schon bessere Zeiten erlebt und legen den Fokus inzwischen vor allem auf Unternehmens-Lösungen. ■

Panda zeigt eine ungewöhnliche Bedienoberfläche, liegt in Sachen Ausstattung aber eher im Mittelfeld.



Der Testsieger Kaspersky hat die meisten Zusatzfunktionen und schafft eine sehr gute Erkennungsrate.

PCM-Testverfahren Internet-Security-Suiten

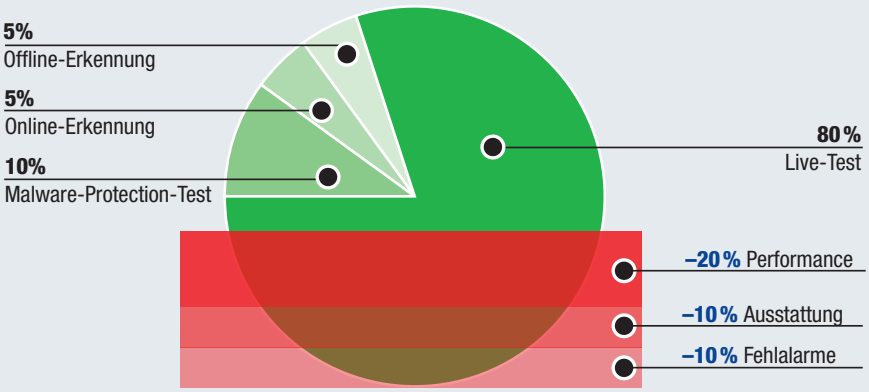
Ein verlässlicher und aussagekräftiger Anti-Malware-Test ist eine Aufgabe für Spezialisten. Die Anti-Viren-Funktionen der Programme testet daher unser Partner-Labor AV Comparatives (**www.av-comparatives.org**). Das Team um Andreas Clementi und Peter Stelzhammer analysiert seit vielen Jahren Anti-Malware-Lösungen und hat sich in der Branche einen Namen gemacht.

Ausgefeilte Testverfahren

Die Besonderheit von AV Comparatives ist der zusammen mit der Universität Innsbruck entwickelte Live-Test (*Real World Test*). Dabei werden programmgesteuert Tausende infizierte Websites aufgerufen. Die getesteten Programme müssen nun ihre Plattformen verteidigen, sei es durch URL-Blockaden, verhaltensabhängige Erkennung oder andere Mittel: im Unterschied zum reinen Festplatten-Scan ein sehr realitätsnahes Testverfahren.

Bei der vom Anwender angestoßenen Untersuchung der Festplatte unterscheiden wir zwischen Offline-Erkennung (ohne Internet-Verbindung), Online-Erkennung (mit Internet) und Malware-Protection-Test. Bei letzterem wird die Datei gestartet. Spätestens jetzt muss das Schutzprogramm reagieren.

PCM-Wertung und Benotung Security-Suiten



Offline-Erkennung: Test aller Daten auf Viren ohne bestehende Internetverbindung. Situation: z.B. Malware per USB-Stick unterwegs.

Online-Erkennung: wie Offline-Erkennung, aber bei bestehnder Internetverbindung.

Malware-Protection-Test: wie Online-Erkennung + Ausführung/Start der Malware. Situation: z.B. Start eines Word-Makros aus einer Mail.

Live-Test: Eine reale Arbeits- und Surf-Situation wird unter laufendem Windows-Betrieb simuliert und das Verhalten der Sicherheitssuite beobachtet. Wie gut erkennt diese unsichere Webseiten und Drive-by-Downloads?

Gesamtnote

In der großen Tabelle am Schluss finden Sie zwei Noten: Für die Gesamtnote vergeben wir positive Punkte nur für den reinen Virenschutz (*Live-Test* mit 80 %, *Malware-Protection-Test* 10%, *Online-Erkennung* 5% und *Offline-Erkennung* mit 5 %). So kann kein Produkt aufgrund anderer Merkmale, etwa der *Ausstattung*, in der Gesamtnote ein besseres Ergebnis erhalten als das für den Virenschutz. Abzüge gab es dann für „Mängel“ bei *Ausstattung*, *Performance* und *Fehlalarmen*.

Note Virenschutz

Diese Note bezieht nur die Sicherheitsfaktoren ein: *Offline-Erkennung, Online-Erkennung, Malware Protection, Live-Test* und negativ die *Fehlalarme*. Sie zeigt, wie gut das Programm schützt.

PCM-Messergebnisse aus dem Virenlabor

Die verschiedenen, oben genauer erklärten Faktoren spielen in unserem Vergleichstest eine Rolle. Dabei ist mit Grün in jeder Spalte der beste Wert und mit Rot der jeweils schlechteste Wert markiert.

	Live-Test (%)	Malware-Protection-Test (%)	Online-Erkennung (%)	Offline-Erkennung (%)	Kritische Fehlalarme (Stück)	Performance (Punkte) [1]	Ausstattung (Punkte) [2]
Avast	99	100	99	98	15	8,7	59
AVIRA	100	100	100	94	2	19,7	74
Bitdefender	100	100	98	98	5	11,8	90
ESET	99	100	98	98	8	1,6	53
F-Secure	100	100	98	94	44	17,8	50
G DATA	97	100	99	99	5	43,3	59
Kaspersky	100	100	97	97	0	9,9	93
McAfee	99	100	96	71	23	2,7	64
Microsoft	100	100	82	49	131	44,3	21
Norton Live	100	100	100	80	28	18,8	69
Panda	100	100	94	45	38	15,6	52
Sophos	99	100	99	69	15	57,3	34

[1] Niedrigere Werte sind besser. [2] Höhere Werte sind besser.

Security-Suiten

PC Magazin TESTSIEGER www.pc-magazin.de
PC Magazin SIEGER PREIS/LEISTUNG www.pc-magazin.de
PC Magazin SIEGER PERFORMANCE www.pc-magazin.de

Testergebnisse auf einen Blick
Zwölf Security-Suiten von 40 bis 100 Euro

Hersteller	1 KASPERSKY	2 BITDEFENDER	3 ESET	4 MCAFEE	5 AVAST
Produkt	**Total Security 2020**	**Total Security 2020**	**Smart Security Premium 2020**	**Total Protection**	**Premium Security**
Preis (drei Geräte oder mehr/ein Jahr)	69,95 Euro	39,99 Euro [1]	69,95 Euro	44,95 Euro [1]	79,99 Euro
Internet	www.kaspersky.de	www.bitdefender.de	www.eset.de	www.mcafee.com	www.avast.com
Engine	Kaspersky	Bitdefender	Eset	McAfee	Avast
Gesamtwertung	95	94	93	92	91
PC Magazin -Testurteil	sehr gut	sehr gut	sehr gut	sehr gut	sehr gut
Preis/Leistung	gut	sehr gut	gut	sehr gut	befriedigend
Punkte Virenschutz	99	99	98	96	98
Web-Schutz-Funktion					
Privacy-Schutz im Web	✔	✔	–	✔	✔
Browser-Cleaner	✔	✔	–	✔	✔
Browser-Konfigurator	✔	–	–	–	–
Sichere Suchfunktion	✔	✔	–	✔	–
Webcam-Sicherung	✔	✔	✔	–	✔
Link-Checker in Suchergebnissen	✔	✔	–	✔	✔
Sicherer Banking-Browser	✔	✔	✔	–	✔
Virtuelles Keyboard	✔	✔	–	–	–
Phishing-Schutz	✔	✔	✔	✔	✔
E-Mail-Scanner (POP, IMAP, MAPI)	✔	✔	✔	✔	✔
Spamfilter	✔	✔	✔	✔	✔
VPN	✔	✔	–	✔	–
Ransomware-Schutz					
Heuristik	✔	✔	✔	✔	✔
Geschützte Ordner	✔	✔	✔	–	✔
Echtzeit-Backup	✔	✔	–	–	–
Datensafe/Dateiverschlüsselung	✔	✔	✔	✔	–
Weitere Sicherheitsfunktionen					
Passwort-Sicherung des Programms	✔	✔	✔	–	–
Spielmodus ohne Unterbrechungen	✔	✔	✔	✔	✔
Rettungs-CD/-DVD/-USB	✔	✔	✔	✔	✔
Funktioniert ohne Cloud	✔	✔	✔	✔	✔
Router-Scan	–	✔	✔	–	✔
Remote-Verwaltung	✔	✔	–	–	–
Datenshredder	✔	✔	–	✔	✔
Passwortmanager	✔	✔	✔	✔	✔
Kindersicherung	✔	✔	✔	✔	–
Cloud-Backup	✔	–	–	✔	–
Backup	✔	–	–	–	–
Systemsicherung und -Tuning					
Schwachstellensuche	✔	✔	–	✔	✔
System-Tuning	✔	✔	–	✔	–
Löschen nicht benötigter Dateien	✔	✔	–	✔	–
Fazit					
	Kaspersky glänzt mit der besten Ausstattung, einer sehr guten Erkennungsrate und produziert als einziges Programm keine Fehlalarme.	Das Programm überzeugt bei Ausstattung, Schutz und auch beim Preis und hat nur hauchdünn den Spitzenplatz verpasst.	Eset schafft es trotz eher mittelmäßigen Zusatzfunktionen noch aufs Treppchen. In Sachen Performance ist es klar das beste Programm.	Die Suite des US-Herstellers McAfee lässt einige Funktionen vermissen, bietet aber einen guten Schutz.	Avast hat eine sehr gute Performance. Bei der Ausstattung liegt das Programm im Mittelfeld.

[1] nur im ersten Jahr, lässt sich dann aber kündigen.

PC Magazin
SIEGER
VIRENSCHUTZ
www.pc-magazin.de

	6 AVIRA	7 NORTONLIFELOCK	8 F-SECURE	9 PANDA	10 G DATA	11 SOPHOS	12 MICROSOFT
	Prime	Norton 360 Deluxe	Total	Dome Complete	Total Security 2020	Sophos Home Premium	Windows Defender
							
	99,95 Euro	39,99 Euro[1]	79,99 Euro	62,24 Euro[1]	65,95 Euro	40 Euro	kostenlos
	www.avira.com	de.norton.com/360	www.f-secure.de	www.pandasecurity.com	www.gdata.de	www.sophos.de	www.microsoft.com
	Avira	Symantec	Avira und F-Secure	Panda	G DATA und Bitdefender	Sophos	Microsoft
	90 ■■■■■	**87** ■■■■■	**85** ■■■■■	**84** ■■■■□	**79** ■■■■□	**71** ■■■■□	**64** ■■■□□
	sehr gut	**sehr gut**	**sehr gut**	**gut**	**gut**	**gut**	**befriedigend**
	befriedigend	**sehr gut**	**befriedigend**	**gut**	**gut**	**sehr gut**	**–**
	100	**97**	**96**	**94**	**97**	**97**	**87**
	✔	–	✔	–	✔	✔	–
	✔	–	–	✔	✔	✔	–
	–	–	–	–	–	–	–
	✔	✔	–	–	–	–	–
	–	✔	–	–	–	✔	–
	✔	✔	✔	–	–	–	–
	✔	✔	✔	–	✔	✔	–
	–	–	–	✔	–	–	–
	✔	✔	✔	✔	✔	✔	✔
	✔	✔	✔	–	✔	–	–
	✔	✔	✔	–	✔	–	–
	✔	✔	✔	✔	–	–	–
	✔	✔	✔	✔	✔	✔	✔
	–	–	–	✔	–	–	✔
	–	–	–	–	–	✔	–
	✔	–	–	✔	✔	–	–
	✔	✔	–	–	✔	–	✔
	✔	✔	✔	✔	–	–	✔
	✔	✔	✔	✔	✔	–	–
	✔	✔	–	✔	✔	✔	–
	✔	–	✔	–	–	–	–
	✔	✔	✔	–	–	✔	–
	✔	–	–	✔	✔	–	–
	✔	✔	✔	✔	✔	–	–
	–	✔	✔	✔	✔	–	✔
	–	✔	–	–	✔	–	–
	✔	✔	–	–	✔	–	–
	✔	–	–	–	✔	–	–
	✔	✔	–	✔	✔	–	–
	✔	✔	–	✔	✔	–	–
	Avira hat den besten Schutz und erzeugt fast keine Fehlalarme. Bei der Leistung ist noch Luft nach oben.	**Der Malware-Schutz von Norton ist gut. Ausstattung, Performance und die Zahl der Fehlalarme sind eher durchschnittlich.**	**Die finnische Security Suite ist recht spartanisch ausgestattet und leistet sich trotz guter Erkennungsraten zu viele Fehlalarme.**	**Panda schwächelt bei der Offline-Erkennung und erzielt in den übrigen Testfeldern solide Ergebnisse.**	**Der deutsche Hersteller G Data hat Probleme im Live Test und bei der Performance. Gut in den übrigen Kategorien.**	**Sophos konzentriert sich auf das Unternehmens-Geschäft und liefert für Privatanwender eine mäßige Security-Suite.**	**Der Defender schneidet in drei Testkategorien am schlechtesten ab und bietet allenfalls einen Basisschutz.**