

An Update on Malware and Anti-Malware for Windows Computers

compiled by Gary Patrick
from Published Articles & Test Reports

Lexington Computer & Technology Group
February 7, 2018 (rev. 2/14/18)

What's New since my June 2017 Update?

- A) the Meltdown and Spectre vulnerabilities:
 - discovered as flaws in nearly all modern c.p.u. chips
 - would allow targeted malware to read private data

- B) New rounds of testing on Anti-virus and Security Software

- C) Introduction of anti-Ransomware software

What's New?

A) the Meltdown and Spectre vulnerabilities:

- Intel processor designs and some ARM processor designs are vulnerable to Meltdown.
 - (AMD chips are not affected)
 - Meltdown can be mitigated by operating system patches.
- Nearly all processors are susceptible to Spectre.
 - Spectre has two variations -
 - Mitigation requires operating system patches for the 1st variant;
processor chip firmware changes for the 2nd variant.⁽³⁾
- Intel, AMD, and ARM will be issuing firmware updates – but the channel for getting updated will probably be through your p.c. manufacturer.
- Raspberry Pi is gloating it is not susceptible to either.
(its ARM processor doesn't use speculative execution)

What is Meltdown?

Meltdown breaks down the barriers between software and the operating system; Meltdown lets malicious software access the memory of other software, and the operating system; ⁽¹⁾

What is Spectre?

Spectre breaks down barriers between software programs.
Spectre "tricks" an otherwise-safe program into leaking sensitive data. ⁽¹⁾

Windows, Mac, Linux, iOS, and Android are all affected by the bugs.

Both exploits attack the computer's in-use memory, and get it to share information that it normally wouldn't.

Malicious software could then access that data, which could include passwords, documents, banking details, and even other users in a cloud-computing environment. ⁽¹⁾

Meltdown and Spectre flaws allow specially-written malware to get access to supposedly protected data, by finding and using crumbs left by speculative execution, to determine where protected data is located, and get it by indirect access.

What is Speculative Execution?

It's an attempt to make CPU operation faster by being more efficient. All modern processor architectures use precise timing of instruction execution, and keep track of it. This tracking enables a processor to pre-process some data, instead of idling, guessing the program is going to call for those steps next, and then undo that pre-processing if the program actually branches [in] a different direction. This wastes no more time than if idle states were used, and may speed up program execution if the pre-processing guess was correct. (analogy next)

What is Speculative Execution?

- My wife thought of the analogy made evident by text messaging on a mobile phone.
- The phone is forward-guessing what word you will want next :
- It improves your typing efficiency if the phone's guess turns out to be correct.



Speculative Execution is managed by the kernel in your p.c. -
what's the kernel?

The kernel inside your operating system is basically an invisible process that facilitates the way apps and functions work on your computer, talking directly to the hardware. It has complete access to your operating system, with the highest possible level of permissions. Standard software has much more limited access. Here's how The Register puts it: "Think of the kernel as God sitting on a cloud, looking down on Earth. It's there, and no normal being can see it, yet they can pray to it." (2)

What should you do to protect your p.c.?

- 1) Be sure the latest Windows Update has been installed, or install it, to mitigate Meltdown.

Detail: Microsoft rolled out this update on January 3rd, but it can't be installed unless the anti-virus software on your machine is compatible – compatibility requires your AV vendor to make a update that writes a new key into the Windows Registry.

(see a test to detect this Windows Update two slides ahead)

What should you do to protect your p.c.? (continued)

- 2) Get any updates offered for your web browser(s) and Extensions (such as Adobe Flash);
- 3) Disable Javascript in your browser(s).
Javascript makes it easier for a hacker to implement malicious software that could exploit Meltdown or Spectre.
- 4) In the coming weeks, check for firmware updates for the CPU in your p.c. (BIOS update likely), and firmware for your graphics processor as well (i.e. revised graphics card drivers).

Steve Gibson has written a freeware program to check your computer for existence of the Microsoft Windows Update and/or BIOS firmware updates to mitigate Meltdown and Spectre.

Download it from <https://www.grc.com/inspectre.htm>.

The file name is InSpectre.exe. (size: 126 kilobytes)

Save it on your hard drive and run it.

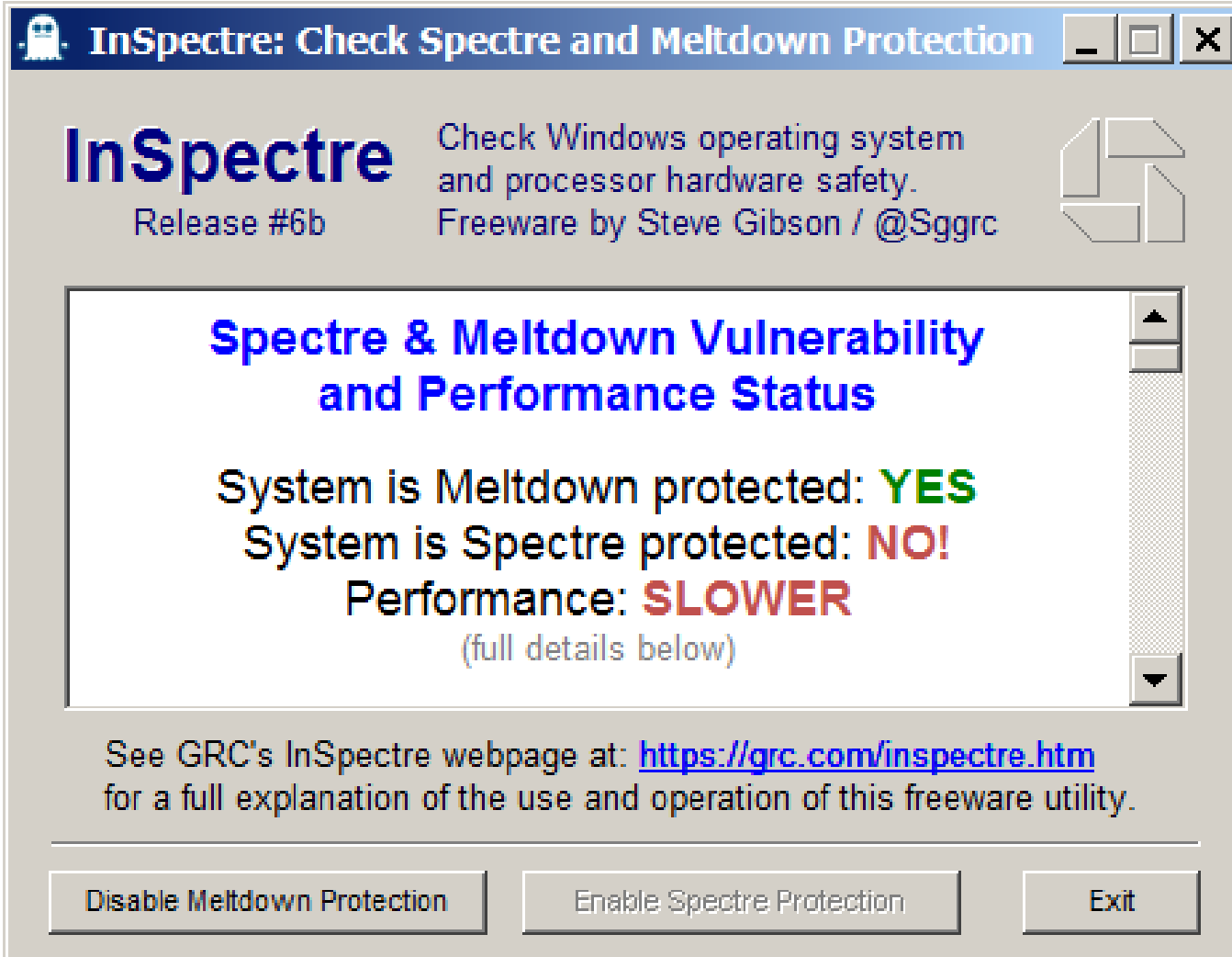
(There is no installer file required; a result is shown in next slide)

The explanation of protections against Meltdown and Spectre, displayed upon scrolling beneath the test result, is quite well written;

The grc.com website has more references and a release history for InSpectre.

(Steve Gibson is trustworthy – his utility program SpinRite has been respected for decades for its ability to refresh data stored on a hard disk drive, and in many cases, recover “unreadable” data).

Gibson's InSpectre Test Report:
Case of Windows Update having been installed,
but no BIOS update (for Spectre) is available yet.



The screenshot shows a window titled "InSpectre: Check Spectre and Meltdown Protection". The window contains the following information:

- InSpectre** Release #6b
- Check Windows operating system and processor hardware safety. Freeware by Steve Gibson / @Sggrc
- Spectre & Meltdown Vulnerability and Performance Status**
- System is Meltdown protected: **YES**
- System is Spectre protected: **NO!**
- Performance: **SLOWER**
- (full details below)
- See GRC's InSpectre webpage at: <https://grc.com/inspectre.htm> for a full explanation of the use and operation of this freeware utility.
- Buttons: Disable Meltdown Protection, Enable Spectre Protection, Exit

Explanation of the Buttons at the bottom of the window:

When InSpectre is run with elevated administrative privilege, each button below toggles its respective protection on or off. Any changes will take effect after the system is restarted. Each button will be disabled if its protection is not available to be changed.

[For more information see GRC's InSpectre web page](#)

Copyright © 2018 by Gibson Research Corporation

See GRC's InSpectre webpage at: <https://grc.com/inspectre.htm> for a full explanation of the use and operation of this freeware utility.

Disable Meltdown Protection

Enable Spectre Protection

Exit

B) An update on Anti-Virus Software:

1) New rounds of tests by independent laboratories and p.c. enthusiast magazines are regularly made available;

There are updates this winter from AV-test, AV-comparatives, Simon Edwards Labs, and Virus Bulletin. (see example graphs below)

There is not much change among the rankings of the best:

- Avira, Avast, and AVG Free versions twirl around 1,2,3 ranking by the test houses of the free ones;
- Norton, Kaspersky, Gdata, ESET, play musical chairs among the test results and opinions of test houses.
- Every anti-virus program has some complaints from users. (refer back to my June 2017 Presentation slides to see user comments, mostly from Consumer Reports)

(Consumer Reports has not published its 2018 tests yet but their website has continued to gather user comments since last spring – an update on those is two slides down):

PCMag Best Security Suites, 1/12/2018:

Editors' Choice, score=4.5*: Bitdefender, Kaspersky, Norton;
score=4*: McAfee, Webroot, Trend Micro;

PCWorld, 1/25/2018, Best Antivirus Software:

Norton Security Premium, 4.5*; Avast Premier, 4*;
Eset I.S., 4*; AVG I.S., 3.5*; Windows Defender, 3*

AV-comparatives Real World Protection, Jul-Nov '17 Awards:

Advanced+: [*Avast, AVG, Avira, Bitdefender, Emsisoft, Eset, Kaspersky, McAfee, Panda, Trend Micro, Vipre*]

AV-Test Top Products, December 2017 Windows Ten tests:

Score=18: Kaspersky I.S., McAfee I.S., Vipre Security
Score=17: Ahnlab, Bitdefender, Trend Micro.

Simon Edwards Labs, test results Oct-Dec 2017:

AAA: Norton Security; Kaspersky I.S.

AA: Eset Smart Security, Avira Free, Avast Free;

A: Trend Micro I.S., AVG Antivirus Free, ZoneAlarm Free

User comments since June 2017:

Avira Free: two user comments in Consumer Reports online, both giving it a score of 1. (range: 1 = poor, to 5 = excellent)
One review complains about scans never completing; the other complains about pop-ups coming on top of web pages.

AVG Free: no additional comments in Consumer Reports

Avast Free: one additional comment, score=1, in CR
complains of unauthorized charge to credit card.

MS Windows Defender: one new comment, score 4, in CR
“Except for a ransomware event a couple years ago (easily dealt with), have never had a problem with malware or virus attacks.”

ESET Internet Security: still no comments in CR online.

Norton Security Deluxe: now 6 comments total; score distribution:

two "4", one "2", three "1" for average = 2.2, in Cons. Reports.

Oct.'17 says it has zero AV protection for iPad or iPhone despite advertised claim. score =1.

Aug.'17 says that since Symantec purchased LifeLock they now pester you with pop up ads for that; owned more than 6 months; score = 2]

July '17 complains he had it on two laptops acquired used, he reformatted the hard drives and reinstalled everything, and suffered slow operation and crashes. Replaced Norton with AVIRA, and the problems went away. score = 1.

Bitdefender Internet Security 2017: now there are 3 CR user reviews, score distribution: two "5," one "1".

"I have had this for 4 years -greatest protection of all. Every time I have had a problem, it has been taken care of from one day to no later then a week." score = 5

"It catches everything you could throw at it.The support team is second to none." score = 5.

Kaspersky Internet Security 2017: now 5 reviews total, scores one "5", two "4", one "2", one "1".

"I've had this for years and it has been great. But is it a "back door" by which Russian Government could spy on U.S. users who happen to be military or government personnel? spooky!" score = 4

"I have generally felt well-protected." score = 4

"Causes Facebook and other sites with displays, and browsers (edge, firefox, and chrome) to crash. Removing Kaspersky extensions and turning off banner blocker solved problem." score = 1.

"Too many issues with this program.. It froze my computer and had very difficult time in getting it restarted. Unable to open any tabs on my browsers. Had to remove it to be able to use my computer again. Windows 7 desktop." score = 2

G-Data: now there's one review, score 2; "Great except that email scanning slows or completely stops Outlook from loading. Endless "processing" that goes away when disabling "email check."

Also review the User Comments captured in my June 2017 anti-virus report, in the Files area on our Yahoo Group website.

The Best Security Suites of 2018

Most entry-level suites include antivirus, firewall, antispam, parental control, and additional privacy measures such as protection against phishing sites. Advanced suites typically add a backup component and some form of system tune-up utility, while others throw in a password manager and other extras. But what do you really need to keep your PC safe? We tested, rated, and reviewed nearly four dozen security suites, and these 10 get top marks and our highest recommendation.



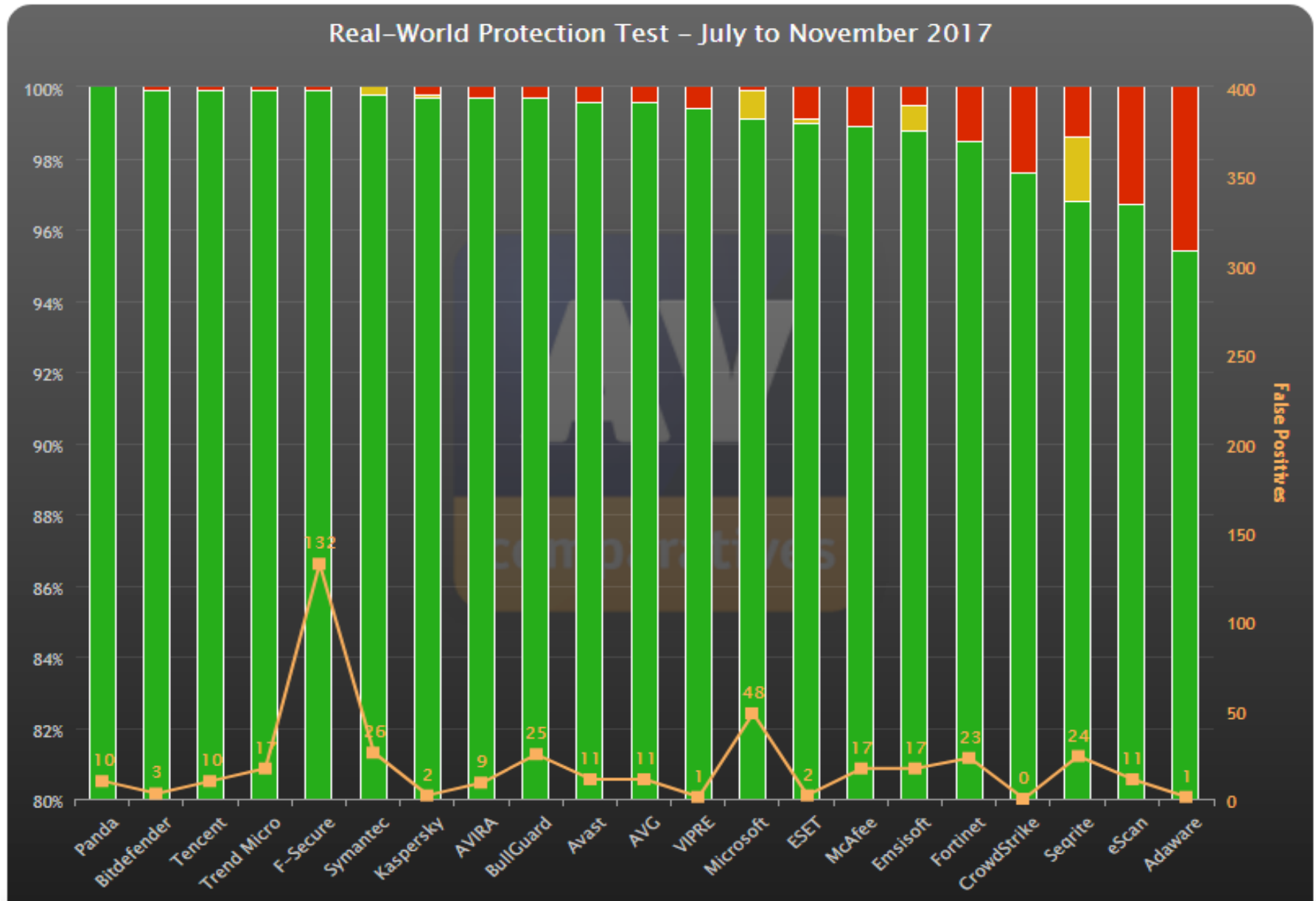
By Neil J. Rubenking January 12, 2018 1:51PM EST

244
SHARES



Product	McAfee Total Protection	McAfee LiveSafe	Bitdefender Internet Security	Symantec Norton Security Deluxe	Kaspersky Internet Security	Webroot SecureAnywhere Internet Security Comp...	Kaspersky Total Security	Bitdefender Total Security	Symantec Norton Security Premium	Trend Micro Maximum Security
Lowest Price	\$24.99 McAfee - 1	\$44.99 McAfee	\$51.99 Bitdefender	\$39.99 Norton - 1 year	\$39.99 Kaspersky Lab	\$29.99 Webroot	\$49.99 Kaspersky Lab	\$58.49 Bitdefender	\$49.49 Norton - 1 year	\$49.95 Trend Micro
	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT
Editors' Rating	●●●●○	●●●●○	●●●●● EDITORS' CHOICE	●●●●● EDITORS' CHOICE	●●●●● EDITORS' CHOICE	●●●●○	●●●●○	●●●●● EDITORS' CHOICE	●●●●● EDITORS' CHOICE	●●●●○
Firewall	✓	✓	✓	✓	✓	✓	✓	✓	✓	—
Antispam	✓	✓	✓	✓	✓	—	✓	✓	✓	✓
Parental Control	—	✓	✓	—	✓	—	✓	✓	✓	✓
Backup	—	—	—	—	—	✓	✓	—	✓	—
Tune-Up	—	—	—	✓	—	✓	✓	✓	✓	✓
Read Review	McAfee Total Protection Review	McAfee LiveSafe Review	Bitdefender Internet Security Review	Symantec Norton Security Deluxe Review	Kaspersky Internet Security Review	Webroot SecureAnywhere Internet Security Complete Review	Kaspersky Total Security Review	Bitdefender Total Security Review	Symantec Norton Security Premium Review	Trend Micro Maximum Security Review

AV-comparatives: <http://chart.av-comparatives.org/chart1.php>



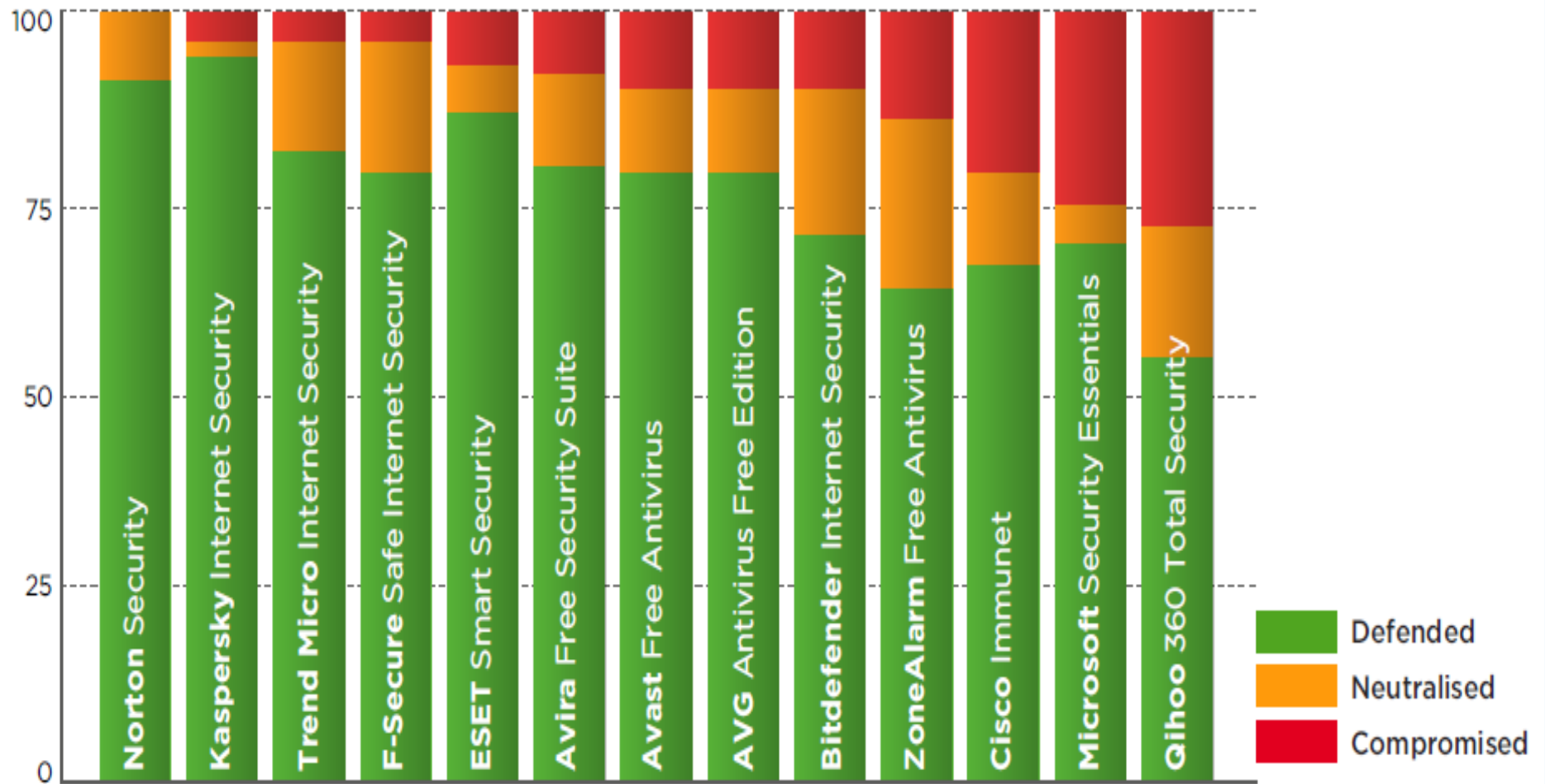
AV-test Report, running Windows 10

<https://www.av-test.org/en/antivirus/home-windows/>

December 2017					
Name			Protection	Performance	Usability
 AhnLab	AhnLab V3 Internet Security 9.0		●●●●●	●●●●●	●●●●●▶
 avast	Avast Free AntiVirus 17.7 & 17.8		●●●●●	●●●●●	●●●●●▶
 AVG	AVG Internet Security 17.7 & 17.8		●●●●●	●●●●●	●●●●●▶
 Bitdefender	Bitdefender Internet Security 22.0		●●●●●	●●●●●	●●●●●▶
 COMODO	Comodo Internet Security Premium 10.0		●●●●●	●●●●●	●●●●●▶
 F-Secure	F-Secure Safe 17		●●●●●	●●●●●	●●●●●▶
 KASPERSKY	Kaspersky Lab Internet Security 18.0		●●●●●	●●●●●	●●●●●▶
 McAfee	McAfee Internet Security 20.5		●●●●●	●●●●●	●●●●●▶
 Microsoft	Microsoft Windows Defender 4.12		●●●●●	●●●●●	●●●●●▶
 panda	Panda Security Free Antivirus 1.0		●●●●●	●●●●●	●●●●●▶
 Norton	Norton Norton Security 22.11		●●●●●	●●●●●	●●●●●▶
 TREND MICRO	Trend Micro Internet Security 12.0		●●●●●	●●●●●	●●●●●▶
 VIPRE	VIPRE Security VIPRE AdvancedSecurity 10.1		●●●●●	●●●●●	●●●●●▶
 Avira	Avira Antivirus Pro 15.0		●●●●●	●●●●●	●●●●●▶
 BullGuard	BullGuard Internet Security 18.0		●●●●●	●●●●●	●●●●●▶

Simon Edwards Labs Protection Test, results bar graph: (contained in their Anti-malware Protection Report, Oct-Dec 2017)⁽⁷⁾

Protection Details



This data shows in detail how each product handled the threats used.

- C) Some vendors have introduced Anti-Ransomware software,
- as a separate program:
examples: Checkpoint ZoneAlarm Anti-Ransomware
(rated 4.5* by PCMag, and is an Editors' Choice.)
 - or incorporated within their anti-virus offering:
examples – BitDefender Antivirus Plus (rated 4.5* by PCMag)
Webroot SecureAnywhere AntiVirus,
(rated 4.5* by PCMag, and is an Editors' Choice.)
- (this may constitute a reason to change to Bitdefender, or add ransomware defense separately.)

Anti-Ransomware operates by placing bait files for detection, or depends upon heuristic methods of detection.

For a full discussion, refer to the article

<https://www.pcmag.com/roundup/353231/the-best-ransomware-protection>
That includes the Test Report Ranking Chart that's on the next slide:

The Best Ransomware Protection of 2018

When ransomware turns your most important files into encrypted gibberish, and paying big bucks to get those files back is your only option, you're in big trouble. One of these top-performing anti-ransomware utilities is your best bet for staying safe.



By Neil J. Rubenking January 26, 2018 4:12PM EST

89 SHARES



Product	Bitdefender Antivirus Plus	Webroot SecureAnywhere AntiVirus	Acronis Ransomware Protection	CheckPoint ZoneAlarm Anti-Ransomware	Trend Micro Antivirus+ Security	CyberSight RansomStopper	Bitdefender Anti-Ransomware	Cybereason RansomFree	Malwarebytes Anti-Ransomware Beta	Trend Micro RansomBuster
Lowest Price	\$24.00 SEE IT	\$18.99 SEE IT	Free SEE IT	\$1.99 SEE IT	\$24.95 SEE IT	\$0.00 MSRP	Free SEE IT	\$0.00 MSRP	\$0.00 MSRP	\$0.00 MSRP
Editors' Rating	★★★★★ EDITORS' CHOICE	★★★★☆ EDITORS' CHOICE	★★★★☆	★★★★★ EDITORS' CHOICE	★★★★☆	★★★★☆	★★★★☆	★★★★☆	★★★★☆	★★★★☆
Behavior-Based Detection	✓	✓	✓	✓	✓	✓	—	✓	✓	✓
Prevent File Modification	✓	—	—	—	✓	—	—	—	—	✓
Prevent All File Access	—	—	—	—	—	—	—	—	—	—
Recover Files	—	✓	✓	✓	✓	—	—	—	—	✓
Vaccination	—	—	—	—	—	—	✓	—	—	—
Read Review	Bitdefender Antivirus Plus Review	Webroot SecureAnywhere AntiVirus Review	Acronis Ransomware Protection Review	CheckPoint ZoneAlarm Anti-Ransomware Review	Trend Micro Antivirus+ Security Review	CyberSight RansomStopper Review	Bitdefender Anti-Ransomware Review	Cybereason RansomFree Review	Malwarebytes Anti-Ransomware Beta Review	Trend Micro RansomBuster Review

Attributions, explaining Meltdown & Spectre:

(1) The Parallax: Eye on Security News, <https://www.the-parallax.com/2018/01/04/meltdown-and-spectre-what-to-do/>

(2) Article in PC World online “Meltdown and Spectre FAQ's”

<https://www.pcworld.com/article/3245606/security/intel-x86-cpu-kernel-bug-faq-how-it-affects-pc-mac.html>

(3) There is also a link to a 27-minute video narrative/interview.

<https://www.pcworld.com/video/84775/what-you-need-to-know-about-meltdown-and-spectre>

References for additional reading:

(4) Intel Corporation, White Paper explaining Spectre&Meltdown:

<https://newsroom.intel.com/wp-content/uploads/sites/11/2018/01/Intel-Analysis-of-Speculative-Execution-Side-Channels.pdf>

well written and mostly understandable.

(5) Wikipedia: <http://wikipedia.org> on “Meltdown,” “Spectre,” and “Speculative execution.”

Reference Reading on Meltdown & Spectre (continued)

(6) Article written by Leo Notenboom, “Ask Leo” website:
<https://askleo.com/need-spectre-meltdown/>

Spectre and Meltdown enable malware to use a side channel attack to obtain forbidden data. In this article he explains side channel attack methods by the analogy of pulling playing cards, on request, from a pack of playing cards, where he has pocketed some of the cards for faster access – speculative execution.

References: Anti-virus Test Reports:

- (7) Simon Edwards Labs: Home Anti-Malware Protection, Oct-Dec 2017, a pdf file. download it from <https://selabs.uk/en/reports/consumers>; (scroll down to it). A comprehensive and well written report on their testing of anti-malware software, running Windows 10.
- (8) AV-comparatives reports:
(but as of now the latest Summary Report available is Dec. 2016)
- Real World Protection Bar Graph, July-Nov. 2017 (*)
 - Performance Test (degree of burden upon p.c. speed)
- https://www.av-comparatives.org/wp-content/uploads/2017/10/avc_per_201710_en.pdf
- (9) The AV-test December 2017 test results, Windows 10:
<https://www.av-test.org/en/antivirus/home-windows/>

(*) display slide is included in the body of this presentation

Reference Reading about Ransomware Protection:

(10) PCMag online, January 26, 2018 article:

<https://www.pcmag.com/roundup/353231/the-best-ransomware-protection>.

The bottom half of the article has a short description of each anti-ransomware product tested. Clicking on the red product name opens up a full test review on each one individually.