EINPRESSWIRE

AV-Comparatives explains the importance of independent IT-security testing labs to enterprise security

Independent labs have the facilities to cope with the evolving threat landscape

Logo AV-Comparatives

INNSBRUCK, TYROL, AUSTRIA, August 27, 2021 /EINPresswire.com/ -- When looking for an endpoint protection product to secure a business network, there is a wide variety of solutions available. These include endpoint security (antivirus), and endpoint protection and response systems, which allow administrators to detect, analyse and respond to suspicious programs, processes and events. In a recent statement, AV-Comparatives has explained why reports from independent testing labs are essential when it comes to choosing the right security product for an enterprise network.

AV-Comparatives is one of the best-known testing labs, and is certified as one of the few EICAR-Trusted labs, as well as being ISO-certified. It undergoes a thorough examination each year, to verify that it is independent and unbiased.

> “
> Testing security products is what independent testing labs do. They have the expertise and experience to deal with new technologies and newly-evolving threats.”
>
> *Peter Stelzhammer, co-founder, AV-Comparatives*

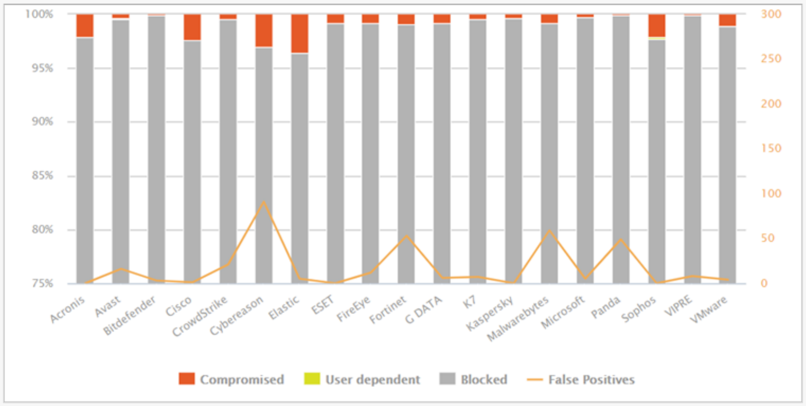
What sort of attacks do enterprise security products have to cope with?

The threat landscape is complex, and constantly evolving. Various different types of malware – viruses, worms, trojans, botnets, ransomware and so on – have been around for some time, but are constantly being redeveloped to evade detection. In recent times, there has been a marked increase in advanced persistent threats (APTs). These are complex, targeted attacks, principally aimed at infiltrating enterprise networks.

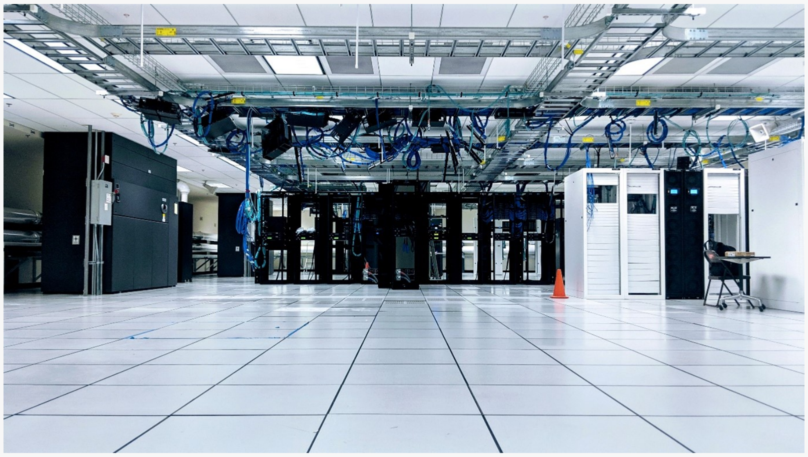
Why do independent testing institutes have the advantage?

Independent testing labs have the resources to focus on testing responses to the ever-changing threat landscape. They can also analyse malware for similarities with other samples, so as to produce relevant and balanced test-sets. Professional test labs also have the ability to run tests with thousands of samples.

Meaningful comparison of multiple security products requires all the products to be tested under identical conditions and at the same time. For example, all products have to scan a malware sample simultaneously, because otherwise one vendor would have longer to update its program's malware definitions (locally or in the cloud). Given that some malware auto-mutates every time it's downloaded, checks need to be made to ensure that all tested products are confronted with exactly the same file. The sophisticated lab setup and methodologies used by independent labs ensure a level playing field for all products.



Malware Test results for different AV products 2021



Source: Taylor Vick/Unsplash

As well as there being various types of threat, there are also multiple ways in which threats can reach a device: Internet, email, LAN or external drive. Modern security software employs multiple protection mechanisms to ensure that systems are not compromised. Simply scanning inactive malware samples on an external drive won't by a long way prove if a product can protect a system from that threat. It might blacklist the site from which the file was originally downloaded, or use its behavioural detection mechanisms to identify and stop it after it has been executed. Good testing labs use a variety of different comparative testing methods to answer the all-important question: "How well do the tested products protect the system?".

Why are performance testing and false-positives testing important?

It is a fact of life that security programs can create false alarms, i.e. wrongly detect harmless programs and processes as malicious. In a business network, this can create huge disruption. Essential business software might be disabled, or IT staff might waste time trying to control an outbreak when there isn't one. False-positives tests by independent testing labs ensure that security programs don't protect the network at the expense of constant false alarms.

Another possible downside of security software is that it can slow down the systems it protects. If it puts the brakes on operations like file copying or archiving, it can cause frustration and reduce the productivity of staff. Independent tests of security software measure the performance reduction caused by endpoint security software, to ensure that it isn’t a drag on productivity.

Testing security products is what independent testing labs do. They have the expertise and experience to deal with new technologies and newly-evolving threats. AV-Comparatives recommends reading the free AV test reports of some independent testing labs before deciding which enterprise security product to buy. Their own test reports can be downloaded here:

https://www.av-comparatives.org/enterprise/

Peter Stelzhammer
AV-Comparatives
+43 720 115542
media@av-comparatives.org
Visit us on social media:
Facebook
Twitter
LinkedIn