**ATP: live test against data theft and encryption malware**

**For consumer users, all their vacation photos and other memories are often lost – for corporate users, the entire future of the company may be at stake. When info stealers or ransomware attackers strike, data ends up in the hands of strangers or is professionally encrypted to a large degree. Strong protection software for consumer users and corporate users ought to avert these scenarios. But does it really work? The Advanced Threat Protection test – or ATP test for short – provides clear answers. In this live test, the testers feed 10 very dangerous attackers into the systems and observe what happens step by step. The latest test involving 16 protection packages covers the full spectrum: from perfect defense, right down to encryption and data theft.**

When an info stealer or ransomware strikes, the scenario is always quite similar at the beginning. A phishing e-mail usually comes with an attacker inside. Many are of the opinion that once it enters the Windows system, the outcome is inevitable: either the attack is detected by the security software or not. But that's not quite true. Because even if security software fails in the initial step, this does not mean that all is lost. Good security software not only consists of a detection engine, but also has many other modules that support each other in terms of protection and often work in perfect coordination to fend off malware in further attack steps.

This capability is revealed in the Advanced Threat Protection (ATP) test. In 10 live scenarios, the ATP test follows step by step how 5 ransomware samples and 5 info stealers attack the Windows test systems. Detecting that the malware has entered the system or is being launched is merely the first defensive step. The interesting question is if, despite non-detection, other modules stop the malware in later stages and ultimately fend it off. Negligible damage sometimes remains, such as a residual text file or image file. Other cases do exist, however, where the battle rages to the bitter end and individual data is stolen or encrypted. But that is still an acceptable outcome in an emergency compared to a total loss.

**16 security solutions in the ATP test**

The current evaluation involved 8 security packages for consumer users and 8 endpoint solutions for corporate users. All products were tested in March and April 2025 under Windows 10 Professional.

The packages for consumer users came from Avast, AVG, Avira, F-Secure, Kaspersky, McAfee, Microsoft and Norton. The endpoint solutions were from Acronis, Avast, Kaspersky (with 2 versions), Microsoft, Microworld, Trellix and WithSecure.

In the table, each solution is assigned a protection score – a maximum of 35 points is possible. For each ransomware sample detected and stopped completely, up to 3 points are awarded, and for each info stealer, up to 4 points. With 5 variants per attack type, half point scores can also be awarded in the total of 10 scenarios.

The laboratory describes the sequence of defensive actions in a matrix according to the MITRE ATT&CK standard. If a product does not immediately detect the attacker, further defensive actions can take effect and thus stop the attack. The test shows exactly at which step this occurs – or doesn't occur.

**The latest attack techniques used in the test**

In the recent March-April ATP test, a special attack technique was used, which all malware samples in the 10 scenarios in the lab exploited:

**MSBuild (Microsoft Build Engine):** The trusted Windows tool is part of the .NET Framework and Visual Studio. It is used to create (compile) executable applications from project files (.proj, .csproj etc.).

Attackers, however, inject malicious code into a project file and offer it for compilation by the user. During this process, the malicious code is executed as fileless malware in the memory and can thus bypass protective measures, as MSBuild is considered a trusted application.

**ATP: here's how well consumer user products performed**

In the March-April ATP test, there were some negative surprises among the products for consumer users. Of the 8 packages examined, only 3 products provided a seamless defense in all 10 scenarios, thus receiving the maximum 35 points: Kaspersky, McAfee and Microsoft.

Norton recognized 9 attackers, but an info stealer was still able to carry out its evil plan. This led to a 3.5 point deduction. The 10th malware, a ransomware, went unnoticed – another 3 points lost. Norton still achieved 28.5 points for the protection score.

It was a grueling test for the packages from Avast, AVG, Avira and F-Secure. All packages recognized only 8 out of 10 attackers. The products allowed one info stealer and one ransomware sample to pass through without resistance. Interestingly, the malware samples are the same in all cases. Overall, these products lost 7 points and ended up with a protection score of 28 out of 35 points.

All tested products earned the "Advanced Certified" certificate from AV-TEST, as they achieved 75 percent of the maximum 35 points (26.5 points).

**ATP: here's how well the corporate user products performed**

Although the solutions for corporate users performed much better in the test than products for consumer users, there were some issues. The 5 products from Acronis, Kaspersky (both versions), Microsoft and Microworld completed the test without errors and scored the full 35 points for their protection score.

WithSecure's endpoint package also logged all 10 attackers, but had problems afterwards. The already identified info stealer was only stopped in further steps. This cost a one-point deduction, with a final score of 3 out of 4 points. There was also a problem with one ransomware and the loss of further points. Here as well, the attacker was recognized, but not stopped immediately. WithSecure's product only succeeded in subsequent steps. This resulted in 33 out of 35 points for WithSecure's protection score.

The Trellix endpoint solution detected 9 out of 10 attackers. While an info stealer went about its work undetected, a ransomware was discovered but not stopped. In the end, the test system was encrypted. All in all, Trellix scored 28.5 out of 35 points.

Avast's business solution fended off 8 out of 10 attackers without any limitations. In one instance involving an info stealer and ransomware, the solution had to concede, and the attackers commandeered the test systems undisturbed. The result was 28 out of 35 possible points for the protection score.

All the evaluated solutions were able to receive “Advanced Approved Endpoint Protection” certification, as they achieved 75 percent (at least 26.5 points) out of 35 points for the protection score. Only Acronis did not receive the certificate, as this is reserved for products [also certified in the regular monthly test and fulfilling the criteria there](https://www.av-test.org/en/antivirus/business-windows-client/).

**Conclusion: punishing ATP test leaves its mark**

As seen in the table, some of the products for consumer users suffered a devastating loss of points. The packages from Kaspersky, McAfee and Microsoft proved, however, that it is still possible to achieve flawless security. They completed the test with top scores with 10 recognized and fended off attackers, attaining 35 points on the protection score.

The result for company products was significantly better, yet far from perfect. Acronis, the two Kaspersky versions, Microsoft and Microworld worked completely error-free, thus earning the maximum 35 points for the protection score.

Although some products detected the attackers in the respective scenario, they only prevented the disastrous work of the malware in subsequent steps. Conversely, sometimes the defense failed, even though the malware was already identified.

Many of the products tested nonetheless proved that the teams of developers working in security companies are doing a good job and are still a decisive step ahead of the attackers.

Ein Bild, das Text, Screenshot, Software, Schrift enthält.

KI-generierte Inhalte können fehlerhaft sein.

**Security packages for consumer users in the ATP test**

In the latest Advanced Threat Protection test under Windows 10, not all security solutions proved effective against the attackers.

Ein Bild, das Text, Screenshot, Software, Schrift enthält.

KI-generierte Inhalte können fehlerhaft sein.

**Endpoint solutions in the ATP Test**

Among the protection solutions for corporate users, 5 of the 8 solutions examined withstood the attacks in all 10 scenarios.

**The 10 test scenarios**

All attack scenarios are documented according to the standard of the MITRE ATT&CK database. The individual sub-techniques are listed in the MITRE database for “Techniques”, for example “T1566.001” under “Phishing: Spearphishing Attachment“. Each test step is thus defined among the experts and can be logically understood. In addition, all attack techniques are explained, along with how successful the malware is.