ESET® Digital Security
Progress. Protected.

9 signs that your endpoint security isn’t working well

How do you know when your IT security isn’t up to par?

Take a look at this list. If any of these nine signs sound familiar, it’s time to re-evaluate your current endpoint protection.

1 Scans and updates slow your system to a crawl.

One of the leading complaints about endpoint security is that it negatively impacts speed and performance. Some endpoint security solutions will indeed slow your systems and impact productivity.

When evaluating solutions, be sure to check independent test results that measure performance and system impact. Look for the lowest numbers, which indicate light footprint solutions that won’t affect speed or cause interruptions.

ESET consistently earns the top score of Advanced+ in the AV-Comparatives Performance Test, confirming its light footprint.

2 Employees complain about using the antivirus solution.

If resentment builds up, employees will eventually bypass the solution altogether on their company-issued or bring-your-own devices, which can affect both performance and security for the whole network.

3 Your solution is underperforming.

It isn’t detecting viruses or other pieces of malware or it’s flagging non-malicious files as malware; it has a high footprint that equals slower scanning; it creates AV storms on virtual machines or has high bandwidth usage that bogs down the entire network.

4 Your solution alerts on too many files or links that aren’t actually malicious.

Alerting on multiple files or links that are not actually malicious results in a high rate of so-called false positives.

Even one false positive can cause serious problems. If an antivirus solution is configured to immediately delete or quarantine infected files, a false positive in an essential file can render the operating system or crucial applications unusable.

Even if false positives don’t shut down your system, each one requires an investigation that wastes valuable IT resources.

ESET is well-known throughout the industry for an extremely low rate of false positives.

5 Removing malicious files and dealing with false positives is too complicated.

A study by the Ponemon Institute found that:

- **Security personnel waste 25% of their time responding to false positives**
- **Organizations see false positives as the #1 “hidden” cost of endpoint protection**

You need a solution that delivers silent quarantines and automatic removal of malicious files, not more work for your IT team.

6 Infections come back after you've removed them.

This means the solution isn't doing a good job of cleaning or updating its detection often enough.

7 It's difficult to manage the solution across all your platforms and devices.

In today's environments, you need a security solution that's easy to manage so the burden of protection is minimal. Look for an endpoint security product that includes remote administration, so you can control your entire network of workstations, servers and smartphones from a single location.

For example, the ESET PROTECT management console enables you to:

- **Secure data and devices for all employees, wherever they are**
- **Manage ESET products on workstations, servers and mobile devices in a networked environment from one central location**
- **Manage via the cloud or on-premises**

8 Security event alerts or pop-up prompts interrupt presentations and sales demonstrations.

This impedes productivity. Every employee needs uninterrupted computer access. This means having a malware solution with a "silent" or "presentation" mode that's easy to use, as well as a dependable tool to restore regular mode when the presentation is over.

9 Getting technical support and customer service is inconvenient, or communicating with the vendor is difficult.

If it's challenging to get reliable, customer-oriented support or you're having any issues with call centers outside the U.S., that will impact productivity for IT teams and end users. It will also contribute to frustrations that could lead employees to circumvent your security solution, opening their devices—and your network—to cyberattacks.

ESET is known for customer-focused, U.S.-based tech support that's there when you need it.

The ESET advantage

For 30+ years, ESET has been a pioneer in the field of heuristic detection. We protect more than 400,000 businesses and 110 million users around the world with technology that predicts emerging viruses and allows us to create defenses before they do any damage.

Ideal for small businesses, ESET solutions mean lower costs, with built-in security features that other vendors charge for and a light footprint that keeps older computers running smoothly. Built for ease of use, our endpoint security includes single console management and can be deployed to Android, PC and iOS in minutes. Secure data and devices for all your employees—even your remote workforce—quickly and easily.

Learn more about ESET solutions for small business.

ESET Digital Security Progress. Protected.