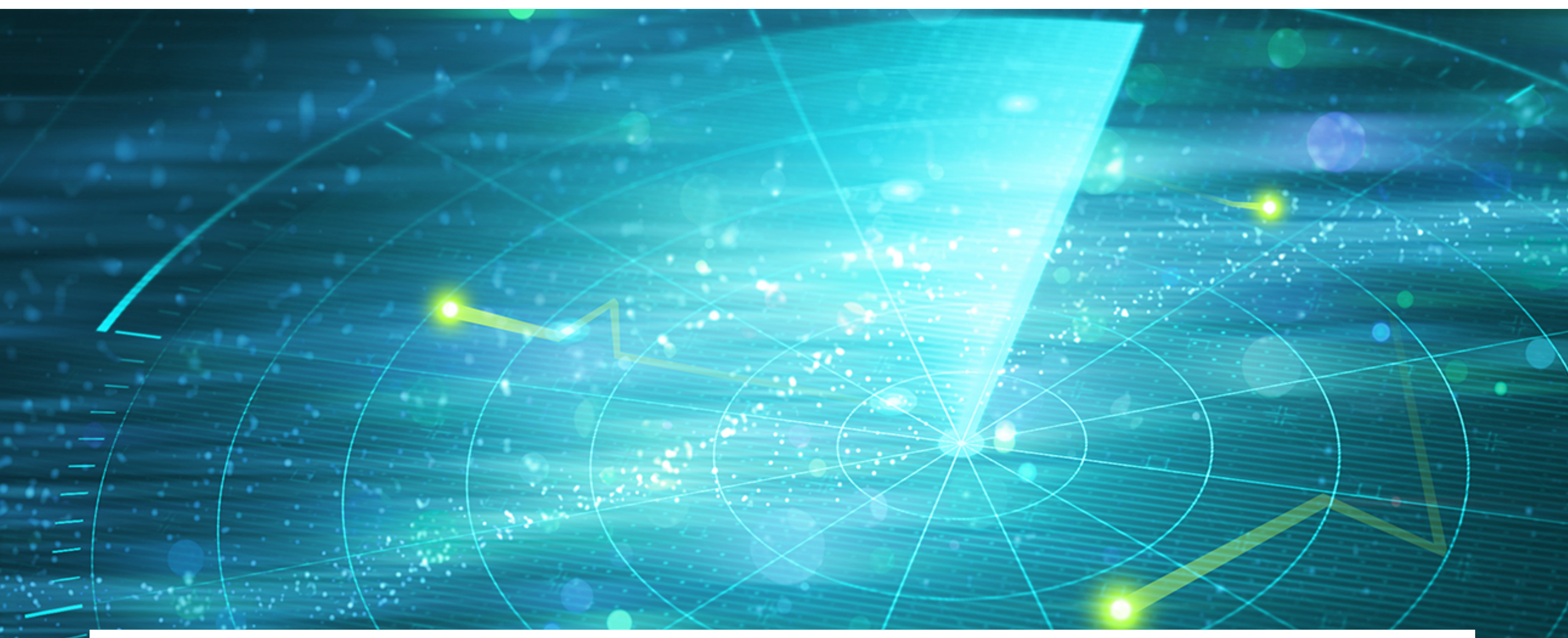
eset®
Digital Security
Progress. Protected.



Choosing Endpoint Protection:
Here's What to Consider

Endpoint protection is one of the most important parts of a multilayered cybersecurity approach. Choose a solution that's reliable, doesn´t interfere with your systems, and lets you focus on your business. To decide which suits you, do your own research and refer to reviews by established and reputable organizations. Here are a few things to consider:

Detection rates

You want your security software to be able to detect all the threats that enter your network. The problem is, of course, that most malware is designed to evade detection. Therefore, you won't always know if something has penetrated the software's defenses unless your systems slow down or start behaving erratically. Better to regularly audit your network traffic for any issues!

When it comes to determining detection rates of solutions, independent test results might be your best guide here. You can check real-world tests conducted by trusted organizations with a proven track record, such as AV-Comparatives. Be especially wary of vendors who provide you with malware samples to test with— they tend to be customized, so their products automatically mark them as malicious. And if you are planning on using real malware for testing purposes, keep it safe and use a dedicated test machine that's isolated from the rest of your network, with no valuable data stored on it.

Incidence of false positives

A false positive is an alert on a file or link that isn't actually malicious. Some in the security industry maintain that they're not a big deal—but they are. 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. By choosing a product that keeps marking false positives, you'll be spending a lot of time chasing down nonexistent threats, and possibly reimaging and restoring systems that don't need to be touched at all.

System footprint

Security software varies widely in the amount of system resources required in terms of memory, disk space, processor load, and network impact. During your evaluation, keep an open ear to user complaints. If antivirus updates or system scans noticeably impact system performance, you'll hear about it as users see their systems slow down and it affects their ability to get their work done.

System slowdowns aren't a price you have to pay for having security. And you shouldn't have to upgrade older machines just to run the security software. AV-Comparatives regularly does performance testing to compare what impact endpoint solutions have on machines they are running on.

Ease of management and maintenance

Pay special attention to this one. You don't want to have to wear out your shoes running from one device to another to configure, administer, upgrade, and maintain the security across all the systems in your environment.

Look for the ability to manage all endpoints (desktops, servers, virtual machines, and even managed mobile devices) **from a central console**, push out updates, automate routine tasks such as creating and deploying configurations, and quickly create the reports you need.

Managing IT security from the cloud is convenient and easy. It's also cost effective, because there is no need for additional hardware or software. With **a cloud-based console** you can connect anytime from your favorite browser.

Support response

In case you run into any problems, it's best to have a place where you can search for solutions. Look for a knowledgebase that covers a variety of scenarios. It should be easy to navigate and detailed enough to quickly provide information on the necessary steps. If you need further assistance, there should be a simple way to contact technical support.

To sum it up, **here are the main things to look for** when choosing an endpoint solution: **The highest possible detection rate, lowest incidence of false positives, negligible impact on systems, easy management from a cloud console, and high-quality support.**

But there are also other things to consider, such as ease of deployment or costs. If your company uses devices with more than one operating system, also look for a solution with cross-platform support. No matter whether you use Windows, macOS, or Linux, be sure your desired solution has you covered. Don't rush—choosing an endpoint security solution is not just a technical decision, but a business decision as well.

Where to look for reviews and ratings of endpoint protection:

AV comparatives	AV-Comparatives: Independent tests of antivirus software
SE Labs	SE Labs: Quarterly reports on endpoint protection and breach response solutions
virus BULLETIN	Virus Bulletin: The latest research and information for the security community
G2	G2: Website offering over one million user reviews of software including endpoint security services
GetApp	GetApp: Premier online resource for businesses exploring software as a service products