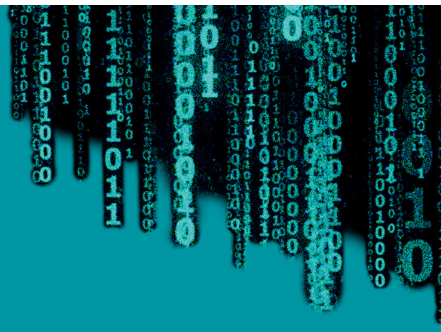
ENJOY SAFER TECHNOLOGY®

THE SECURITY EXPERTS' GUIDE TO CHOOSING THE RIGHT ENDPOINT PROTECTION



The security of your organization, your data and your end users rides on your choice of an endpoint security solution. But if you wear multiple hats (and what IT pro doesn't these days?) you can't be an expert in everything. Make the wrong decision about security, and you'll spend much more time than you ever expected in administering and managing the solution, cleaning up after infections and handling user complaints. That's why we've put together this guide, so you can make an expert choice of your own. It will help you avoid the potential pitfalls and make the best possible decision for your organization and those who will manage it.

Starting your research

Experts always recommend that you do an on-site evaluation, in your own environment, to be sure you end up with a product that doesn't conflict with the processes running on your systems. More about that later. But first, you need to come up with a shortlist of products to test. Here are some tips to help you distill the facts from the marketing hype.

Knowing what's in the name. As you begin your research, you'll find that products variously call themselves antivirus, antimalware or endpoint security. The term antivirus is still what most people call the products you'll be looking at, even though modern products have evolved to detect and defend against much more than viruses. The term antimalware describes protection against the broader types of threats. Endpoint security is broader still. But here's the point: Regardless of the name, most products protect against all malicious threats including malware, ransomware and viruses. So don't get hung up on product labels.

Getting beyond the buzzwords. You'll also run into terms such as heuristics, expert systems, neural networks, reputational analysis and others that draw from artificial intelligence, or least sound like they do. Vendors also tout what they're doing in the cloud, whether it's detection, management, telemetry collection, licensing or a combination of some or all of these. Don't just rely on buzzwords per vendor; get a solid explanation of the technology from each. ESET's blog WeLiveSecurity is a great resource for understanding many of these terms. Once you sift through the buzzwords, you will likely find that the products use similar technology. What they call them is unimportant. The key is how well they implement them.

Reviews (rave and otherwise). Product reviews have their place, but keep in mind that some online review sites serve up paid reviews that are often based on only a superficial look at the product. Sources such as the Spiceworks community and Gartner Peer Insights are good sources for unbiased reviews based on real-world experience.

The role of independent testing

Third-party testing services throw a battery of malware against security products in a controlled environment. Products that consistently score well should be the ones on your shortlist.

When you visit these sites, don't just look at the most recent results. Look at reports and studies over the course of several years. Keep in mind that test results are only valid for the period in which the tests were performed, and in the configuration and environment chosen by the tester. Sometimes a product tests poorly

because of a quirk in the testing methodology or test platform. Look at the results over a few years and see if the solution has a consistent track record of success.

Established and well-respected testing organizations we recommend are ***AV-Comparatives***, ***SE Labs*** and ***Virus Bulletin***, for the following reasons:

- Each has a different methodology to its testing, so they collectively give you a well-rounded look
- All have been testing security products for many years (Virus Bulletin has been testing products since the 1990s)
- They test not only detection, but also incidence of false positives and impact on system performance (more about these below)

Tips for the test drive

Once you have your shortlist, here are tips from security experts about setting up a successful trial. Follow this advice and make sure you are asking the right questions and testing the right things, and don't overlook something that you'll regret later.

First of all, should you even set up a trial for a product at all? There's a trend among IT pros to dispense with testing, but security experts always recommend testing your endpoint solution first. You want to be sure that a product performs well in your environment and works with your systems, and that technical support is there when you need it—before you commit to rolling it out to all of your systems and enter a multiyear contract.

How many products to test? Three is a good number because of the sheer amount of time it takes to properly test each product in sequence. You could consider testing more products if you have a large enough organization and enough IT staff to test in parallel.

How to test. Contact each vendor and arrange for a 30-day trial. For each, pilot to a small group of cross-departmental test users. You don't want just "power users" and IT/technical types, but also nontechnical, regular folks. Also, test across users who use various line-of-business software, proprietary software, legacy programs and other "one-offs" throughout your organization. Take the time to evaluate thoroughly by accounting for all the use cases in your environment.

Key considerations: What to look for

During your online research, in communicating with vendors and in trying out the software for yourself, here are the key items that the experts look out for.

Detection rates. Of course, you want your security software to be able to detect all the threats that enter your network. Because most malware is designed to evade detection, you won't always know if something has penetrated the security software's defenses unless a user's system slows down or shows erratic behavior, or you regularly audit your network traffic. Independent test results might be your best guide here. Be leery of vendors who provide you with malware samples to test with—typically their samples are created specifically so that only their products detect them as malicious. And if you are going to be using real malware to test with, be safe and use a dedicated test machine that's isolated from the rest of your network with no valuable data.

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. 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. If you ultimately choose a product that finds 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 consumed 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 impact 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.

Compatibility. Make sure the solution works well with your essential line-of-business applications and other software, tools and services you use in your organization. If computers crash while performing certain tasks, that is a major problem—likewise, if you have trouble installing the software, or can't install it at all due to a noncompatible OS. Pay special attention to older hardware—are there conflicts with specific software or hardware, and does it work unobtrusively without bogging down performance?

Costs/functionality. Price is always a consideration. While most security software detects the various forms of malware, some vendors charge extra for ransomware protection, so make sure to ask vendors what is included. Also take a look at the total value of the package. Capabilities like protection against malware on USB drives, web control for blocking threats on malicious sites, and a software firewall for locking out malicious network traffic or preventing threats from spreading add extra layers of security and are worth having.

Ease of management and maintenance. Pay special attention to this one. You don't want to have to wear out your shoes running from machine to machine to configure, administer, upgrade and maintain the security across all the systems in your environment. Look for the ability to manage all endpoints from a central console, push out updates, automate routine tasks such as creating and deploying configurations, and quickly create the reports you need.

Mobile security. It is inevitable that mobile devices are being used for your business—whether you furnish the devices to your employees, have a formal bring-your-own-device program or policy, or don't have a policy at all. Look for and test the ability to secure all the platforms your employees carry—whether they're for Android, Windows or iOS. Also, centralized management is a must for mobile. If the solution has the ability to lock and unlock devices remotely and wipe those that are lost or stolen, that's a big plus because you might avoid the cost of a separate mobile device management tool.

Ease of deployment. When you set up your test, pay attention to the amount of time it takes to get the solution up and running correctly. Does it automatically remove the previous antimalware solution? If not, you could have a time-consuming headache when it's time to go live organization-wide. In addition, if the solution is preconfigured for best practices right out of the box, you'll save yourself a lot of tweaking and tuning.

Support response. Put the vendor's support system to the test. During your trial period, make a few calls and open tickets on typical scenarios. How easy is it to communicate and get to a resolution? If the support is outsourced to a support center located overseas, how easily and quickly do these resources understand and resolve your concerns?

Tips for testing technical support

The last item above is critical—good tech support is like an insurance policy for your security solution. What happens when you're staring at an issue on an executive laptop the day before your president flies out on a business trip? You want to know ahead of time that your vendor's technical support will pull you through. Here are a few expert tips for putting tech support to the test:

- Set up a computer with the wrong network settings, don't uninstall the previous antimalware software before installing the evaluated product, or find some other way of "breaking" the installation. Then call support and ask for troubleshooting help.
- Disable the security software on a machine, deliberately infect it, then ask support to walk you through the steps to clean it.
- Try any other scenarios that proved to be a pain point with your current solution, and see if the prospective vendor handles it any better (or worse).

Don't be hesitant about invoking technical support during your free trial. You want to know how they'll be able to respond to issues before you have a problem with software for which you've invested in a multiyear license.

Accounting for business impacts

Once you've made your decision, there is still some due diligence to do, such as reviewing the contract for hidden gotchas, confirming support for older operating systems, and asking about future OS releases during the lifetime of the contract. These details underscore an important point: Choosing an endpoint security solution is not just a technology decision, but a business decision. The cost of a security solution and the protection it offers are important elements of the decision. But don't overlook hidden costs such as the impact on the productivity of your workers and the time it takes IT to administer and manage it. Those are important to evaluate, too, so you can make an expert security and business decision that is well-rounded, thorough and informed.

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.

See our ***independent testing results*** and get more details on ***ESET solutions for small business.***

For over 30 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit ***www.eset.com****.*

ENJOY SAFER TECHNOLOGY®