

The 10 Questions You Must Ask Your Endpoint Security Vendor

We all like to make good decisions. In the business environment, those decisions can save us time, money, and lots of headaches. Based on our experience working with companies and just about every business endpoint security product, here are the ten questions we suggest you ask your endpoint security vendor before you buy. Your decision will impact you and your company over the coming years.

1. How is the product going to reduce the time, pain, and cost of managing IT security in my company?

What to look for in an answer: Confidence that the product is going to effectively stop threats through simple-to-create policies, and help prevent users from making costly mistakes that you have to clean up. After all, prevention is the best protection. Choose products designed to make your job easy and be sure to consider total cost of ownership in addition to initial purchase cost.

2. I already have an endpoint security product; why should I change now?

What to look for in an answer: Don't just fall into the renewal trap. Can you save money and provide better protection with fewer headaches? Does your current product give you the level of protection that you need for your user base in the office, at home, and on the road? Threats have evolved; is the product that you purchased, perhaps years ago, still the best choice for your needs today? If you've been burned by your current solution, now is a great time to bolster your protection for the coming years.

3. Is the product designed to meet the needs of me and my business?

What to look for in an answer: Is the product easy for you to manage? You want a product that handles the needs of all of your endpoints, anytime and anywhere, with effective centralized management to ease the administrative burden and cost of protection. Look for a product that's truly designed for small businesses, not a complex enterprise product that's been scaled down but remains full of unnecessary complexity. Become confident that you and your end users will be comfortable with it.

4. How do I ensure all the systems in my company are protected?

What to look for in an answer: The product should support all your endpoints, desktops and servers, and mobile PCs and home PCs that might connect via VPN. And it must provide a variety of defenses: anti-virus, anti-spyware, heuristic capabilities, and perhaps even data leakage prevention. Don't forget about Microsoft Windows 7 and your e-mail server and gateway security when making your decision.

5. What is the impact on operations?

What to look for in an answer: Moving to a new solution is often easier than upgrading your current product. This is a perfect opportunity to regain control of endpoints. Look for products with swift, easy, hands-off, and flexible deployment, including the ability to silently and automatically remove your old security products. Can the product discover all the computers on your network, both those managed by Active Directory and those outside it? Look for simple policy creation and enforcement. Also, you shouldn't have to be a security expert; the product should do the heavy lifting and provide you with wizards to guide you along.

6. How effective is the product, particularly against diverse new threats and for data protection?

What to look for in an answer: Seek an all-in-one, managed suite to protect against today's complex Web-based threats in a cost-effective manner. Does the product help prevent valuable data loss with policy enforcement and device control? Does the product provide real-time protection with frequent updates or cloud-based services? In other words, has the product made the transition from protecting against yesterday's threats like e-mail borne viruses to the new threats and compliance requirements of today?

7. What will my typical day be like with the product?

What to look for in an answer: You're looking for simplicity here—a product that protects your company and communicates clearly. Ask about the dashboard, automated alerts, and reporting tools available to make your job easier. Do these tools provide the right level of information to keep you informed when necessary? Can you schedule reports and send them in the right formats? Can you see all of your endpoints in a single interface?

8. Will the product confuse or annoy my users?

What to look for in an answer: If your users are happy, then you're happy. Make sure the software performs well when doing on-access and on-demand scans and minimizes use of system resources. The product should stay out of the user's way to lessen the number of service calls. As the administrator, you need the flexibility to provide most users transparent protection while giving other users more control over their security environment.

9. What kind of support exists when I have a problem?

What to look for in an answer: Support is not just a checklist item. Gaining access to the right person on the other end of the line can be the difference between quickly solving a problem and a weekend of pain. Ask about—or better yet, try out—the support options to experience typical wait times and to determine for yourself how effective support will be for you. Also keep in mind whether there are additional charges to get help, and whether Web, chat, and phone support are available. Consider how your reseller can help you, too.

10. Where can I get additional information to help me make a decision?

Search for first-hand accounts in blogs and forums from others like you and from industry experts. Seek third-party validation for effectiveness—particularly tests that focus on real-world, whole-product testing rather than simplistic synthetic tests. Ask your reseller specific questions that pertain to your situation.



Independent evaluations of technology products

Contact: info@cascadialabs.com
www.cascadialabs.com



This document, prepared independently by Cascadia Labs in September 2009, was sponsored by Kaspersky Lab. Cascadia Labs aims to provide objective, impartial analysis of each product based on hands-on testing in its security lab.