How to Test Next-Generation Antivirus Solutions
Introduction

Deciding on an endpoint security solution can be a difficult task. Many organizations know their current security has gaps but don’t know where to begin in the search for something new. To help with this, the SANS Institute created a guide to evaluate these solutions. The guide outlines the necessary requirements you should look for, as well as how to prepare to run a test. After you’ve fully prepared to test potential solutions, there are seven steps SANS recommends you should follow when conducting your test-drive.
1. Configure your evaluation environment.

- Pick a sample of the different types of machines that you manage (e.g., Windows 7, 8 and 10 workstations, laptops).

- Image the test machines based on the standard configuration for your organization’s endpoint.

- Familiarize yourself with any cloud console and configuration requirements for the products you are evaluating. This should include an analysis of how the point-to-point requirements that can affect communication will work. Consider availability of last-mile connectivity, which will not normally be accounted for by the cloud-based solution, as well as the methods for protecting the cloud-based endpoint and the data and/or metadata created in the cloud from your organization’s endpoints.

2. Evaluate from the viewpoint of your main users: endpoint users and administrators.

There is nothing more frustrating than choosing a product that makes administration more difficult and/or generates constant calls to the help desk. At VMware, we think it’s important to ensure technology doesn’t impact your end user. As you go through the critical checklist, pay particular attention to the items that impact your administrators and users. Top-of-mind considerations should include ease of configuration and the flexibility to create separate but effective security policies for different user groups.
3. Establish possible use cases and evaluation objectives, including:

- Phishing attack
- Infected bring-your-own-device (BYOD) equipment or machine
- Latent ransomware
- Targeted or insider threat

Testing for an infected BYOD equipment or machine requires malware to exist on a machine prior to installing the next-generation antivirus (NGAV) solutions you will be testing. Be sure to take proper precautions to isolate any machine you knowingly expose to malware from the rest of your environment.

For ransomware, test packages exist that can effectively simulate ransomware in your environment without actually exposing your machines to the risks involved in running real ransomware. If you do decide to test with real ransomware, ensure proper precautions are taken to isolate your testing machines or lab from the rest of your environment.
4. If evaluating more than one product, try to maintain consistency across all the products being evaluated.
For each use case, develop a well-defined scenario that:

- Outlines the steps in the use case
- Accounts for what the NGAV should show
- Documents the anticipated performance and outcomes based on your preliminary review of the product’s features

For example, the steps of a well-defined ransomware scenario might include delivery of ransomware > ransomware package running > ransomware package being stopped. You might expect the NGAV to show delivery vector, storage location of ransomware files, attempted encryption, how it was detected or identified, and adequate information to enhance security policy for future scenarios. During testing, monitor the endpoints being tested for their performance and any impact the tested products may have on standard performance. Apply this same scenario to each proposed solution individually.

5. Create a scorecard that allows you to rate (on a 1–10 scale) the functionality of the product in meeting operational requirements. Again, remember to apply the same standard as you evaluate all products.
Download this solution brief for VMware’s suggested product checklist.

6. Create appropriate evaluation documents and scripts based both on the scenario(s) and previous product evaluation results.

7. Conduct the evaluation, document results and determine the leading product(s) and vendor(s) for further consideration.
Start Learning More
If you’d like to read the full SANS guide, visit carbonblack.com/sans-evaluation-guide.

Join us online: