vmware Carbon Black

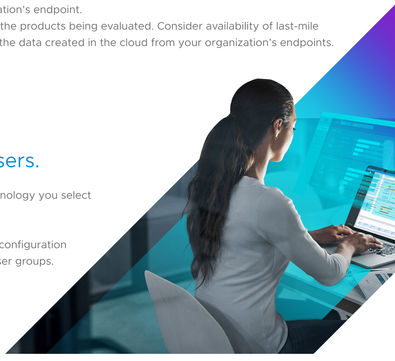
Get More from Your Antivirus Solution

Intrinsic security. Intrinsic advantage.

Is your organization looking at endpoint security solutions? The SANS Institute created a guide to help you evaluate your options. Get insights on the necessary requirement considerations, how to prepare for testing, and seven steps recommended when conducting a test-drive.

1 Configure your evaluation environment.

1. Pick a sample of the different types of machines that you manage (e.g., Windows 7, 8 and 10 workstations, laptops).
2. Image the test machines based on the standard configuration for your organization's endpoint.
3. Familiarize yourself with any cloud console and configuration requirements for the products being evaluated. Consider availability of last-mile connectivity as well as methods for protecting the cloud-based endpoints and the data created in the cloud from your organization's endpoints.



2 Evaluate from the viewpoint of your main users.

Choose a product with easy integration and adoption. It's important that the technology you select doesn't negatively impact your end users or the help desk.

While going through the checklist, be sure to consider attributes such as ease of configuration and the flexibility to create separate but effective security policies for different user groups.

3 Establish possible use cases and objectives:

- 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. 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 When evaluating more than one product, maintain consistency across all the products 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 to rate the functionality from 1-10.

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 Document evaluation results to determine if leading products/vendor needs further consideration.

Again, remember to apply the same standard as you evaluate all products.

Start learning more.

If you'd like to read the full SANS Institute guide, visit

www.carbonblack.com/resources/sans-evaluators-guide-to-cloud-based-ngav