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 requirements considerations, how to prepare for testing, and seven steps recommended when conducting a test.

Get More from Your Antivirus Solution

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).
   - Import the standard configuration for your organization’s environment.
   - Familiarize yourself with any cloud-container configuration requirements for the products being evaluated. Consider availability of lab infrastructure, connectivity to the cloud-based environment, and the role and impact of this infrastructure on your organization’s security.

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, remember to consider the 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
   - Collection incident or outside attacker
   - Malware infections
   - Testing for an infected BYOD equipment or machine

   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 the same scenario to both evaluation solutions to isolate.

4. When evaluating more than one product, maintain consistency across all the products evaluated.
   - For each use case, develop a well-defined scenario.
   - Define the steps in the use case.
   - Document the expected performance and outcomes based on your preliminary review of each product’s features.

   For example, the steps of a well-defined evaluation 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 the same scenario to both evaluation solutions to isolate.

5. Create a scorecard to rate the functionality from 1-10.
   - Remember to apply the same standard as you evaluate all products.

6. Create appropriate evaluation documents and scripts based on the scenario(s) and previous product evaluation results.
   - If you’d like to read the full SANS Institute guide, visit www.carbonblack.com/resources/sans-evaluators-guide-to-cloud-based-ngav.