vmware Carbon Black

GET STARTED

Replace AV Buyer's Guide

Adapted from the SANS guide to evaluating next-generation endpoint security

Introduction

Today's businesses face a unique set of security challenges

You need security that works and is easy to implement and manage, but you're working with a limited budget and resources. Many organizations know their current antivirus solution has gaps but don't know where to begin in the search for something new. According to ESG Research, 65 percent of organizations believe that the skill level of their security team could use improvement, and 48 percent use more than 25 security products. This leads to more overworked people and, ultimately, less effective security.

Not every endpoint security solution can meet your needs. Finding the right solution that is easy to deploy, easy to manage and can cost-effectively protect your growing business is critical. To help teams rapidly assess endpoint security options, the SANS Institute created a detailed guide to evaluating solutions, including next-generation antivirus (NGAV). The guide outlines the necessary requirements companies should look for, as well as how to prepare to run a test.

To assist you in rapidly assessing your options for replacing your antivirus software, we've pulled out and adapted key sections from the SANS buyer's guide, including the core evaluation checklist, guiding questions to frame your evaluation and seven steps to conduct your test-drive.

Evaluation Checklist

Critical requirements for securing your business

Protection and detection

- Provide protection that stops all types of modern attacks, not just malware; provide the ability to recognize and kill patterns of malicious behavior*
- Access multiple forms of prevention, including the ability to set different policies for different endpoints, such as remote workers*
- Provide the ability to create, test and quickly deploy policies to improve prevention and reduce false positives*
- Identify and quarantine known and unknown malware
- Protect against fileless attacks, such as Flash exploits, browser vulnerabilities exploits and other techniques that attackers use
- Ensure that NGAV software cannot be disabled or altered by an unauthorized user

*VMware Carbon Black deems these items as exceptionally critical

Cloud-based intelligence and big data analytics

- Pull threat intelligence from multiple sources into a cloud-based intelligence and analytics engine; use this intelligence to identify malicious behavior and increase endpoint protection*
- Capture unfiltered endpoint activity data and efficiently send it to the cloud for analysis
- Incorporate new and evolving technologies into the product offering through the cloud to aggressively identify and block attacks
- Have vendor participation in the threat intelligence community

Visibility and context

- Build and customize queries and reports related to endpoint state and activity across the entire organization*
- Reveal the full chain of processes affected by the malware/malicious behavior*
- Provide visualization tools, using both graphical and plain language presentations for real-time visibility and retrospective analysis of events*
- Log all results/resulting actions from detection of/response to malware/malicious behavior; present all logged information in a human-readable format, independent of the administrative interface
- Integrate with other tools, such as a security information and event management (SIEM) system, for broader detection and response support

*VMware Carbon Black deems these items as exceptionally critical

Performance

- Minimize false-positive events, which happen when the product blocks access to a legitimate program*
- Provide protection, including identification of new, potentially malicious behavior, with minimal impact on the endpoint user experience*
- Have lightweight impact on endpoint system resources

Operational requirements

- Standard and custom integrations with third-party products*
- Consolidated, cloud-based management console for all modules*
- Simple deployment; supports both manual and automated methods of endpoint deployment*
- Collaborative defense; supports workflows for various security-related roles and groups
- Multiple endpoint platforms supported: Windows, Mac and Linux

*VMware Carbon Black deems these items as exceptionally critical

Five Questions to Answer

Before testing a next-generation antivirus solution[1]

Once you've defined your NGAV solution requirements, it's time to prepare to evaluate potential products. There are five key questions SANS recommends you should answer before conducting a test-drive of a product:

1. What is the time frame for the evaluation? What is the urgency for product selection based on the evaluation?

2. What endpoint systems will the next-generation endpoint security (NGES) run on (e.g., production user desktops, company-owned laptops, production servers, etc.)?

3. How much can your organization invest in evaluating performance in a simulated environment that mirrors production? Not all organizations have the luxury of a sophisticated test environment. You may need to evaluate the product strictly based on tests conducted by a third party and/or a limited test on your own equipment.*

4. What are the criteria required for different categories of users (e.g., developers, security analysts, system administrators, endpoint users)?

5. How will a cloud-based infrastructure change your typical operating procedure?

*Standardized tests allow for a side-by-side comparison of security vendors by defining a broad set of attack criteria and applying it equally across many products. Participating in these tests can show how products stack up against one another in similar environments.

At VMware, we recommend looking at NSS Labs results, as they offer the most comprehensive testing effort there is.

1. These questions were taken directly from the SANS guide.

How to Test

Next-generation antivirus solutions

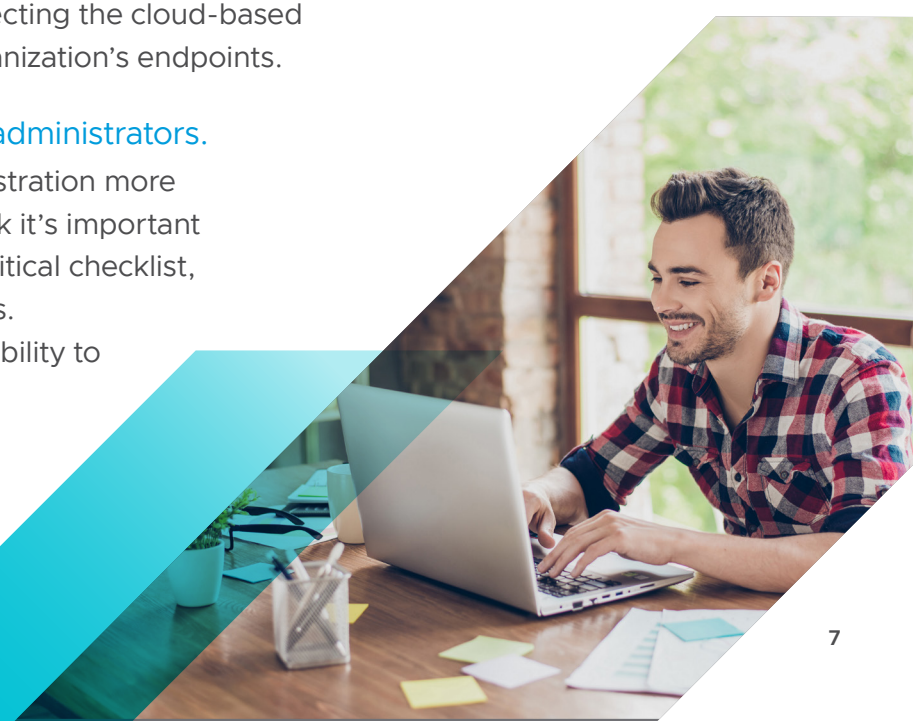
After you've fully prepared to test potential solutions, there are seven steps SANS recommends you should follow when conducting your test-drive.

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 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.

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:

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com