

Carbon Black.

5 Questions to Answer Before Testing a Next-Generation Endpoint Security Solution¹

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, SANS has created a guide to evaluating these solutions. The guide outlines the necessary requirements you should look for, as well as how to prepare for a run a test. Once you've defined your Next-Generation Endpoint Security Solution (NGES) requirements, it's time to prepare to evaluate potential products. There are 5 key questions SANS recommends you should answer before conducting a test drive with a product:

1

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

2

What endpoint systems will the 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? Smaller organizations may not have the luxury of larger organizations with 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.*

*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 Carbon Black, we recommend looking at NSS Labs results, as they offer the most comprehensive testing effort there is.

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 my typical operating procedure?

¹ These questions were taken directly from the SANS guide