

An Evaluator's Guide to Cloud-Based NGAV

The SANS Guide to Evaluating Next-Generation Antivirus

Written by **Barbara Filkins**

Enhanced to Cover Cloud Implementations:
February 2018

Introduction

Since it was first introduced in the late 1980s, antivirus (AV) has been the first line of defense against known malware. Traditional AV relies on malware signatures and behavioral analysis to uncover threats to critical information endpoints: servers, applications, workstations and mobile computing devices. Research over the past 10 years, however, continues to indicate that traditional antivirus products are rarely successful in detecting smart malware, unknown malware and malware-less attacks.¹

This doesn't mean, however, that antivirus is "dead," as market researchers have been claiming since at least 2007.² Antivirus still remains the most effective means of capturing certain impactful events, according to the 2016 SANS Endpoint Security survey. In it, antivirus, along with IPS alerts, caught 57 percent of impactful events that had occurred at respondents' organizations.³

Rather than dying, antivirus is actually growing up.⁴ Today, organizations look to spend their antivirus budget on replacing current solutions with next-generation antivirus (NGAV) platforms that use more powerful approaches to prevention and detection in

A traditional AV solution is limited to detecting only the malware it knows. If the threat is not known, not analyzed and not recorded in the **DAT** file, or if the **DAT** file is not updated, or if the attack doesn't use malware in the first place, the protection offered is nonexistent for that class of threats.

¹ www.forbes.com/sites/thomasbrewster/2015/08/26/netflix-and-death-of-anti-virus/#424e9d0b3256

² www.pcworld.com/article/130455/article.html

³ "Can We Say Next-Gen Yet? State of Endpoint Security," www.sans.org/reading-room/whitepapers/analyst/next-gen-yet-state-endpoint-security-36827, p. 12.

⁴ www.cnet.com/news/antivirus-isnt-dead-its-growing-up



order to stop modern attacks, not just known malware. NGAV takes a system-centric view of endpoint security, examining every process on every endpoint to algorithmically detect and block the malicious tools, tactics, techniques and procedures on which attackers rely.

The typical “window of vulnerability,” defined in the OWASP Testing Guide v4, “does not provide enough time for patch installation, since the time between a vulnerability being uncovered and an automated attack against it being developed and released is decreasing every year.”⁵ While legacy (or traditional) antivirus can still effectively inoculate an endpoint against known threats, the process behind developing a signature for a new threat is time consuming, taking days or weeks, during which new and more nefarious threats will emerge.

The dynamics of cloud-based analytics, which allow for near-real-time operations, bring an essential dimension to NGAV, disrupting the traditional attack model by processing endpoint activity as it happens, algorithmically looking for any kind of bad or threatening behavior, not just for malicious files.

The coupling between NGAV and cloud-based analytics is key. Securing the corporate infrastructure has become a board-level issue due to the risks presented to the business, especially as material costs to the organization increase. These risks range from whole-scale disruption to business operations (e.g., ransomware or denial-of-service attacks) and significant fines imposed due to lack of compliance with such regulations as Sarbanes-Oxley, HIPAA or Europe’s General Data Protection Regulation (GDPR), to more subjective losses, such as loss of competitive advantage or reputational damage. As these risks have become significant market drivers, so has the emphasis on being able to prevent, detect, contain and mitigate these threats quickly and effectively.

So, to be truly effective, companies need a consolidated tool set that can protect their endpoints from emerging threats much faster than traditional methods. The use of real-time analytics operating in the cloud enables a much more dynamic, proactive approach to endpoint security than the traditional, reactive, signature-based antivirus technologies.

Advantages of NGAV enabled by the predictive cloud include:

- **Up-to-date protection against new attacks and threats.** The threat landscape is changing more quickly than can be met by the best timeline to patch, configure and/or enhance corporate endpoints if these services are maintained in-house, especially for larger organizations. Use of the cloud allows lightweight endpoint security updates to be applied to assets anywhere, whether located on the internal corporate network, in cloud instances (private or public), at branch offices or by remote workers.
- **Better analytics available anywhere and anytime.** Connected to the cloud, every endpoint becomes a threat detector. A threat discovered in one part of the world can be immediately communicated across an entire universe of connected endpoints.

⁵ www.owasp.org/images/1/19/OTGv4.pdf, p 11.

- **Learning by “community consensus.”** The more information and data is fed into a cloud-based analytics platform, the better the organization’s insight into the endpoints within a community, ultimately yielding better security for every community organization. If one organization is being attacked, intelligence derived from that attack can be quickly and effectively shared to protect every endpoint across the entire community.
- **Easier, more flexible management.** Cloud-based, intelligent processing makes it easier for administrators to operate by eliminating manual effort, resource-intensive signature updates and complicated policy management—not to mention all the infrastructure and hardware required to run a traditional antivirus system.
- **Real-time critical processes, such as incident response.** If an intrusion does occur, a cloud-based NGAV solution can immediately give remote incident responders both the right information and the ability to take action. There would be no need for time-consuming delays to ship equipment or book flights. Incident response analysts can start working right away and remediate issues much more swiftly, especially when time is of the essence.

Based on its better protection and simplified operations, next-generation endpoint security in the cloud offers significantly more value than its predecessors. Since the initial publication of this “Guide to Evaluating Next-Generation Antivirus” in 2016, SANS has noted the need to help organizations focus on what is needed to procure NGAV solutions. For this reason, we have updated this guide with a step-by-step process for procuring NGAV, including guidance for conducting a proof of concept (POC), and are now including expanded coverage for cloud-based analytics as part of an NGAV solution.

For those ready to replace their traditional antivirus with NGAV, SANS has developed this evaluation guide for assessing NGAV tools against your organization’s requirements before making capital investments in NGAV. If you are familiar with the 2016 version of this guide, the following steps remain the same, with an added emphasis on what to look for in a cloud-augmented solution.

Here’s the lineup:

- **[The original, updated Evaluation Guide.](#)** Review this document to establish your overall road map and help resolve any remaining questions you may have on the procurement process after reviewing the tools and templates developed for step-by-step procurement.
- **[The “SANS Step-by-Step Guide for Procuring Next-Generation Antivirus.”](#)** This is a separate document, built on the original Evaluation Guide. It contains actionable steps to help your organization make an informed decision regarding selection of your NGAV solution, placing your enterprise in a better position to understand and mitigate any risks associated with moving the selected solution into production.

What features should you be looking for in a cloud-enabled NGAV product? How will it integrate into your operational environment? What should you look for in a vendor?

- The **“SANS NGAV Request for Proposal/Request for Information template.”** The RFP/RFI template is also included in the **“Step-by-Step Guide”** as Appendix A. You can use this document to shape your vendor selection process and provide a structured method for evaluating prospective vendors and products.
- **“The NGAV RFP Evaluation Master Template.”** This Excel spreadsheet provides instructions for scoring your detailed NGAV requirements, as well as for comparing vendor responses.

Our goal is to help you design an actionable and transparent procurement process that enables your organization to feel confident in its selection of a key component in the protection and defense of its business and critical assets.

Visualizing NGAV

The starting point for developing an approach to NGAV evaluation is being able to visualize what next-generation AV actually encompasses. This is aided both by understanding the differences between traditional and next-generation AV, and the enhancements offered by NGAV. Equally important is defining your organization’s key requirements, by which you can evaluate (and select) the best NGAV product for your organization.

Traditional AV and Beyond

Figure 1 presents a high-level, side-by-side comparison of NGAV with traditional AV, summarizing how NGAV can help avoid many of the inherent limitations in traditional AV protection in the detection of malware, both known and unknown.

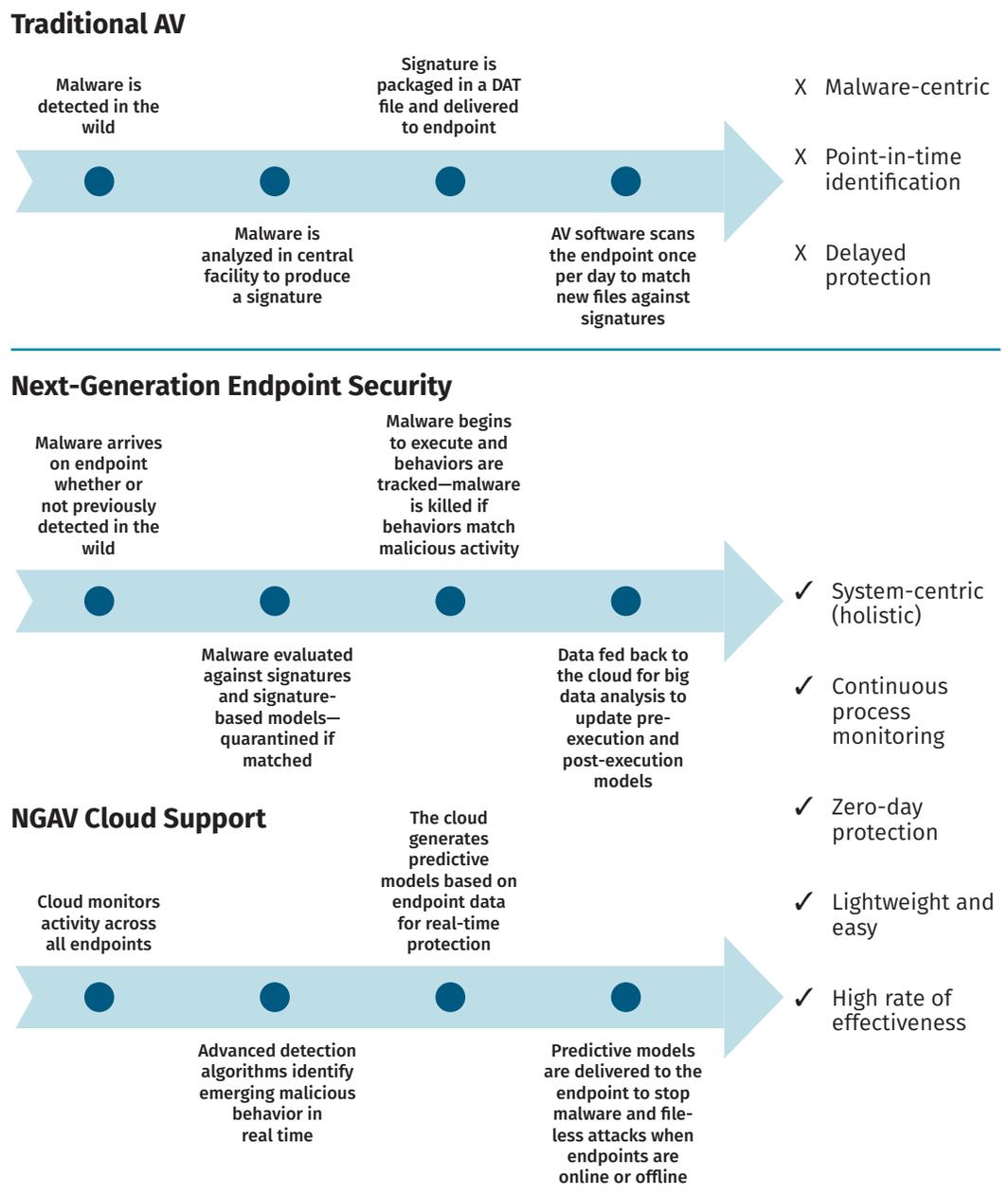


Figure 1. Traditional AV versus NGAV

But NGAV provides more than malware-centric protection and detection. It is a new class of endpoint security—architected around a cloud-based, big data analytics engine built on data science, machine learning and threat intelligence, and that can be tuned to provide deep attack context and insight into both known and previously unknown patterns of attack. NGAV can detect and act on the malicious compromise of system processes by analyzing the process directly in memory, which is critically important, given that modern attacks increasingly may involve no malware to avoid traditional AV detection.⁶

Beyond Signatures

For example, using binaries increases the chance of detection. Attackers are turning to memory-based exploits, for example launching attacks against a running system process, such as **iexplore.exe** or **javaw.exe**, and avoiding any footprint on the storage system for the AV or file integrity monitoring tools to catch. Attackers are using powerful scripting tools, such as PowerShell, and legitimate administration applications, such as **PSEXEC** and **TeamViewer**, to access and control victim hosts, easily evading traditional protection and monitoring solutions while taking advantage of the elevated privileges that come with utilities.

NGAV capabilities also reach beyond use of indicators of compromise (IoCs), metadata such as virus signatures, IP addresses, file hashes and URLs—all of which demonstrate that potentially malicious activity has occurred.

Big Data Analytics in the Cloud

Using advanced data science, machine learning, artificial intelligence and highly scalable, cloud-based analytics, NGAV solutions can actually determine relationships between patterns of behavior to detect the tactics, techniques and procedures (TTPs) used by attackers.

From TTPs, the specific, identifiable patterns of malicious activity, discovered through analysis and correlation of files and behavior, such as listening on a given service port, memory scraping or code injection, an NGAV solution can actually (re)construct a chain of events, visualizing what the actual attacker might be up to, as opposed to looking at individual, discreet events. TTPs can be saved and re-used to block future, similar attacks. Matched to endpoint activity, these patterns help set the activity into context and support policies at the endpoint for protection, detection or response.

Vectors for *malware-less attacks* can include memory-based attacks, as well as exploits initiated through stolen credentials, script-based or command-line (e.g., PowerShell) attacks, and remote login. The attacker is able to “blend” into the organization as quickly and thoroughly as possible, avoiding capture by traditional AV, which is looking for known, detectable malware or exploits occurring on endpoints.

Q. Is it safe to replace AV completely?

A. Every organization is different and has to assess the effect for itself. That said, AV and NGAV have matured enough to transition easily into existing infrastructures, although some products may require you to stick to their suite of tools for secure interoperability, and such requirements should be included in your evaluation.

⁶ www.technologydecisions.com.au/content/security/article/new-wave-of-cyber-attacks-using-little-or-no-malware-471763824#axzz40I

Evaluation Architecture for NGAV

Figure 2 provides an overview of how NGAV components are related in a high-level reference architecture that illustrates the three basic sets of requirements needed to fully evaluate an NGAV.

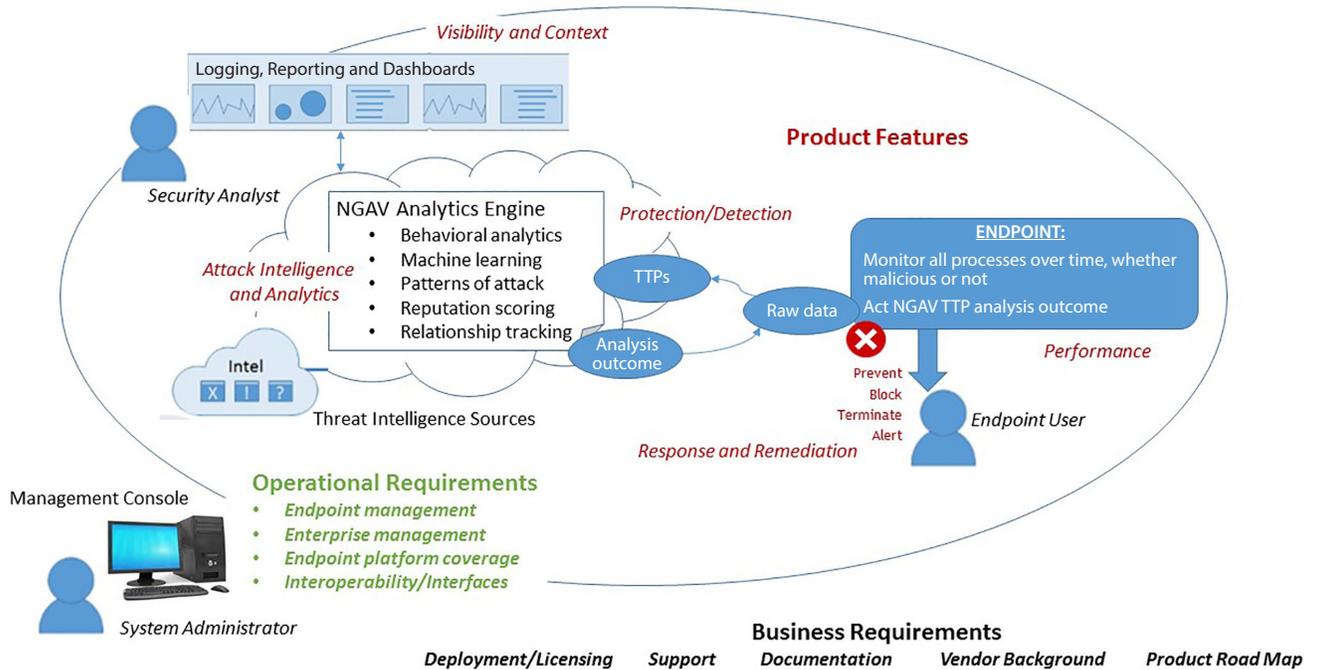


Figure 2. NGAV Requirement Visualization

Planning and Preparation

NGAV requirements can be thought of as three interrelated families:

- **Product Features**—How well do the product features and capabilities meet the functional and technical requirements defined by the organization? For example, how will the product detect attacks and what will it find, including unknown and malware-less attacks, etc.?
- **Operational Requirements**—How well will the product align with the operational needs and requirements of the organization, including coverage of endpoints deployed within the organization, interoperability with existing network and security infrastructure, and management?
- **Business Requirements**—What are the business requirements (and assumptions), such as cost versus terms of coverage, ease of use, compliance and so forth?

With requirements in hand, start planning your evaluation.

While every organization's structure and business drivers are different, there are key common planning considerations to develop your evaluation framework:

- ✓ What is the time frame for the evaluation? What is the urgency for product selection based on evaluation?
- ✓ What endpoint systems will the NGAV run on (e.g., production user desktops, company-owned laptops, production servers, etc.)?
- ✓ 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.
- ✓ What are the criteria required for different categories of users (e.g., developers, security analysts, system administrators, endpoint users)?
- ✓ How should I evaluate the replacement of traditional AV with NGAV? Should I run my evaluation alongside existing AV for comparison? When should I feel comfortable shutting off traditional AV?
- ✓ How will a cloud-based infrastructure change my typical operating procedure?

Preparing to Evaluate: What regulatory compliance policies or policy frameworks should my NGAV solution be adhering to?

Once requirements are defined, it's time to plan how you will evaluate/verify those requirements, given some of the constraints identified in your planning process.

Procedurally, many ways exist to conduct an evaluation, including:

- **Inspection.** Examine product documentation.
- **Demonstration.** Discuss implementations, view product demonstrations by the vendor or participate in limited hands-on experimentation with a demo version of the product.
- **Analysis.** Analyze test results reported by a reputable third party.
- **Testing.** Actually test the product in a preconfigured environment that simulates your production environment.

Organizations with limited resources usually conclude their evaluation and selection of products with just "kicking the tires," using the criteria laid out in the next section together with the inspection, demonstration and analysis methods described. However, this guide also provides a framework for organizations that want to take the next obvious step: a "test drive" to formally test the NGAV in an environment that simulates enterprise conditions, assess the product against one or more probable scenarios, and rate the outcomes based on the viewpoints of both the administrator (detection and remediation) and the endpoint user (operational impact, education) experiences.

Q. How much of a security expert do I need to be to assess an NGAV product?

A. The more you understand security, the more extensively you'll be able to evaluate an NGAV product. Everyone needs AV, so your organization should build in some kind of capacity to evaluate products in your environment or an emulated one.

Attacks today are far more complex, and so is NGAV. So you need testing to deal with known and unknown malware, signature and signature-less attacks, integration with intelligence, response, and many other automated capabilities and features. It takes a combination of skills, tools, techniques and safe testing zones to truly evaluate at this level—something many IT organizations simply don't have in-house.

Conducting the Test Drive

Using the criteria laid out in the next section, SANS recommends the following evaluation steps:

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 the 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 the availability of "last mile" connectivity, which will not normally be accounted for by a cloud-based solution, as well as the methods for protection of the cloud-based endpoint and the data and/or metadata created in the cloud from the 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.
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
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
5. Create a scorecard that includes operational requirements and the functionality needed on a 1–10 basis. Again, remember to apply the same standard as you evaluate all products.

Q. My organization is simply not well equipped to conduct our own in-house testing. Can't I just trust third-party assessments of AV products?

A. For testing the system against malware, third-party assessments are generally trustworthy and are definitely more secure than trying to run malware in your environment to test. Unfortunately, these tests are designed around known malware. NGAV must be tested against unknown malware, malware variants and malware-less attacks.

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.

Q. Should I be conducting my own tests with live malware?

A. Don't test with live malware unless you have taken the steps to follow best practices: Isolate your environment and do not conduct extended tests where malware can exist for long periods of time. Make sure that the product you are testing is properly configured.

SANS Evaluation Guide

Acquiring cloud services needs additional guidance to supplement the NGAV procurement process SANS has published to date. Table 1 summarizes where these requirements fall in the following tables.

Table 1. Further Considerations for NGAV and the Cloud

Area	Things to Consider
Product Features	<p>Threat Detection: Look for improved methods for threat detection with continued emphasis on malware- and file-less attacks. Ensure that the solution detects executable-based threats as well as advanced attacks that don't use malware. If a cloud platform is only collecting and analyzing data from known threats, it will be able to detect or predict only attacks that have already been seen elsewhere.</p> <p>Data Collection: Endpoint data is sent to the cloud to provide a complete contextual picture for real-time prevention, detection, remediation and response. Ensure that the data being collected and analyzed is evaluated for risk in terms of incidents or breaches related to the NGAV vendor.</p> <p>Secure Communication from Cloud to Endpoints: Make sure that the path from the cloud to the endpoint is encrypted and the method used to authenticate an endpoint to the cloud is robust and impervious to attack.</p>
Operational Requirements	<p>Cloud-Based Management Console: Advantages include lack of demands on corporate infrastructure (storage, processing and so forth), automatic endpoint updates to maintain the latest security, and standardized policies across all endpoints (no configuration drift when dealing with multiple update servers). However, make sure that you do not take these features for granted. Check the vendor's approach to communicating the changes inherent with updates and the impact on administrative workflow.</p> <p>Endpoint Communications: To create a holistic monitoring system where endpoints within a community function as "threat detectors," you need bidirectional communication of threat information between endpoints and the cloud. This, however, puts a renewed emphasis on "last mile" communication between the cloud and the various endpoint(s). Make sure you document the communication demands and understand the potential impact of downtime.</p>
Business Requirements	<p>Compliance: Evaluate not just whether the vendor supports all relevant organizational needs, but whether its cloud solution is also compliant. Has the vendor undergone a successful SOC 2 assessment? Do the contract terms also allow a client to request an independent audit of the vendor and its cloud provider, if different from the vendor?</p> <p>Service Levels: Enforceable service levels become important in a cloud-enabled solution to ensure performance in protecting against known threats and attack behaviors, as well as unknown threats.</p>

The features and the operational and business requirements for evaluating NGAV are laid out in the following three tables. These have been enhanced with further considerations for the cloud as outlined in Table 1.

Product Features

The starting point for an evaluation is whether the product itself has the necessary set of basic features, independent of how it will be operated. Table 2 provides a guide for evaluating the functionality and feature capabilities of NGAV products.

Table 2. Product Features/Capabilities

Functionality	Short Title	Feature	Evaluation/Criteria
Protection/ Detection Objective: To determine how each product protects against and/or detects modern attacks	Prevention Architecture	Prevention architecture operates on attackers' tools, tactics, techniques and procedures, not just on malware.	Validate the architecture of the NGAV solution to determine whether it can block sophisticated, advanced attacks as well as those that are known.
	Known Malware Detection/Prevention	Identify and quarantine known malware and variants per named list.	Evaluate the following for each endpoint platform to see if they fall within desired boundaries. (Note: Use results either from your in-house testing or from attributable, independent third parties): <ul style="list-style-type: none"> • Catch rate for known malware (e.g., a signature file exists) • Catch rate for unknown malware (e.g., no known signature, zero-day attacks) • False positive rate across each platform for all attacks
	Unknown Malware Detection/Prevention	Identify and quarantine unknown malware and variants.	
	Malicious Process Detection/Prevention	Recognize patterns and kill those processes that are executing malicious behaviors (e.g., perform behavioral analysis of binaries using TTPs).	
	Exploit Protection/ Detection	Protect against Flash exploits, browser vulnerabilities exploits and other techniques that attackers use.	Determine success rate for discovery and disruption of potential attacks related to critical vulnerabilities (e.g., Flash exploits, critical browser vulnerabilities—especially those recently patched). Actions may include blocking the exploit, delivering a file payload or the process injections or replacements that might result in a file-less persistence scenario.
	Independent Controls Detection/ Prevention	Provide separate controls for threat detection and attack prevention so that threats can be detected for later assessment.	Validate that the product has independent controls for detection and prevention.
	Protection Policies	Provide different protection policies for different groups of endpoints. For example: <ul style="list-style-type: none"> • Developers • Knowledge workers • Servers • Cloud 	Validate that the product can create groups of endpoints and establish security policies independent of one another.
	Tamper Protection	Ensure that NGAV software cannot be disabled or altered by an unauthorized user.	Validate that the software cannot be turned off by a user who does not have the proper authority to do so.

Table 2. Product Features/Capabilities (Continued)

Functionality	Short Title	Feature	Evaluation/Criteria
Cloud-Based Intelligence and Big Data Analytics Objective: To determine how the vendor “future-proofs” its product against new attacks through big data processing and cloud analytics	Endpoint Data Capture	Capture endpoint activity data and efficiently send it to the cloud for analysis.	<p>Ensure that the product does not filter out data unrelated to previously known threats. Instead, determine that the product can send unfiltered endpoint activity to the cloud for advanced processing and identification of new threats.</p> <p>Confirm the types of information being gathered and analyzed from your endpoints. Confirm that data collection is limited to just the bare essentials for delivering effective protection (e.g., transmit and store only endpoint activity metadata (such as process start/stop times, network connection activity, etc.) and ignore potentially sensitive or regulated data residing on the endpoint.</p>
	Extensible Analytics	Incorporate new and evolving technologies into the product offering through the cloud to aggressively identify and block attacks.	Validate that the vendor delivers detection, intelligence and analytic capabilities through the cloud and that cloud updates have an immediate impact on NGAV efficacy.
	Use of Threat Intelligence	Use threat intelligence to identify malicious behavior and increase endpoint protection over time.	Verify how threat intelligence is incorporated into the product, including how it supports the identification of malicious behavior and demonstrates improved endpoint protection over time.
	Threat Intelligence Sources	Gather threat intelligence from multiple sources for integration into NGAV, using a cloud-based intelligence and analytics engine.	<p>Gather the following information:</p> <ul style="list-style-type: none"> • Number and types of data sources used, both internal and external • Methods by which intelligence information is disseminated • Methods used to evaluate and reuse new threat data
	Threat Intelligence Community	Evaluate participation of the vendor in the threat intelligence community.	<p>Require the vendor to demonstrate its support of the following:</p> <ul style="list-style-type: none"> • Open sharing • Protection of confidentiality when sharing information • Feedback from users • Community participation and research

Table 2. Product Features/Capabilities (Continued)

Functionality	Short Title	Feature	Evaluation/Criteria
<p>Visibility and Context</p> <p>Objective: To determine how the product provides visibility into security events and attack context</p> <p>Can the product provide answers to key questions related to detection, response and remediation, such as:</p> <ul style="list-style-type: none"> • How did the attack start? • What happened prior to detection? • Where else does this attack apply? • What could the impact have been? • Should I do anything to recover? • Are there holes I should close? 	Detection Logging	Log all results from detection of malware/malicious behavior. ⁷	Determine what the standard (e.g., minimum) set of data elements is for both activities.
	Response Logging	Log all resulting actions taken in response to detection of malware/malicious behavior.	Determine whether the administrator can customize (e.g., easily add additional data elements) this minimum set for correlation with other enterprise tools, such as a security information and event management (SIEM) system.
	Logging Formats: Readability	Present all logged information in human-readable format, independent of the administrative interface.	Request a representative sample of logs produced in the NGAV system.
	End-to-End Process Logging	Reveal the full chain of processes affected by the malware/malicious behavior.	Determine whether the presentation provides insight into the spawning process (for earlier detection on future occurrences), as well as subsequent lateral movement to know where and when to block such malicious behaviors.
	Visualization	Provide visualization tools, using both graphical and plain language presentations for real-time visibility and retrospective analysis of events.	Review report output to determine ease of interpretation for real-time dashboards and/or reports for both endpoint users and administrators.
	Integration of Visibility and Context Functionality	Provide interface capability (e.g., API) for integration with other tools, such as a SIEM system, for broader detection and response support.	Determine whether the product has a demonstrated integration with external third-party tools (e.g., API for interfacing with a SIEM).
Query Development	Customize queries and reports related to activity across the entire organization.	Determine whether the product has the ability to easily: <ul style="list-style-type: none"> • Collect activity for all binaries (e.g., processes, file changes, registry access, network connections). • Query and report across the entire organization based on custom IoCs. 	

⁷ Some of these criteria are paraphrased from International Computer Security Association (ICSA) antivirus/spyware certification materials. See www.icsalabs.com.

Table 2. Product Features/Capabilities (Continued)

Functionality	Short Title	Feature	Evaluation/Criteria
Response and Remediation Objective: To support response and remediation starting at the endpoint	Detection of Malware	Delete malware or temporary files.	Review product response and remediation capabilities to determine: <ul style="list-style-type: none"> • How well the product automates its support for these processes • Ease of manual intervention when it is required • Ability to interoperate with other response/ remediation tools
	Response Action: Stop	Stop malicious network activity at the endpoint.	
	Response Action: Quarantine	Quarantine systems safely and accurately.	
	Response Action: Secure Shell	Provide secure access to log in to any endpoint for remediating actions.	
	Blacklist Files	Provide for blacklisting of newly discovered malicious files.	
Performance Objective: To deploy a solution that has little or no impact on endpoint user productivity; or lightweight impact on endpoint system resources, regardless of whether it is in a homogenous (e.g., all Windows) or cross-platform environment	Endpoint User Experience: Impact	Provide protection, including identification of new, potentially malicious, behavior, with minimal impact on the endpoint user experience.	Determine how efficiently vendor processes work when examining new samples. For example: Is there a perceptible slowdown or an increase in false positives that would inhibit users?
	False-Positive Rate	Minimize false-positive events, which happen when the product blocks access to a legitimate program.	Validate that protection meets goals on diverse system environments, including developer systems, which contain a lot of internally produced and/or third-party software; and servers that are tightly controlled and rarely change.
	Endpoint System Resource Impact	Have lightweight impact on endpoint system resources.	Gather the following information to assess potential impact on endpoint response: <ul style="list-style-type: none"> • The amount of system memory (RAM) consumed on each endpoint platform • The amount of system CPU processing capacity consumed on each endpoint platform • The amount of system storage (i.e., SSD or hard disk drive space) consumed on each endpoint platform Test against baseline functionality alone (i.e., all other functionality disabled) and also with full functionality enabled.

Operational Requirements

Operational requirements go beyond product features. For example, they encompass how a user interacts with the NGAV product at the endpoint, as well how an administrator manages the product within the organization. Table 3 provides a guide to key requirements and evaluation criteria.

Table 3. Operational Requirements

Functionality	Short Title	Feature	Evaluation/Criteria
Endpoint Platform Coverage Objective: To determine compatibility with and scalability across enterprise endpoints by type and attributes	Endpoint Platform(s) Supported	Support named enterprise platforms. (Note: List platform types, associated operating systems and, if practical, other attributes, such as the organization’s standard endpoint image and/or hardware configuration, whether virtual or physical.)	Determine the limitations (if any) of any platforms currently implemented in the organization or requirements for any endpoints being procured: <ul style="list-style-type: none"> • Will additional memory be required? • Are there any applications (e.g., traditional AV agents) or processes with which the product will conflict? • Have any conflicts or actions that the product might take (e.g., stop other critical processes from running) been documented adequately by the vendor? • Are there any issues with nontraditional devices? • Can you “test drive” the product under your specific software in your test environment? • Don’t forget your virtual environments, such as Citrix-based thin client workstations: Can they be tested against malware that is “virtual aware?” What are vendor recommendations on these topic?
	Scalability and Growth	Support current number and types of endpoints and projected growth.	Review whether there will be any product-related performance limitations for the number of endpoints in the organization. Determine whether the product will scale to meet growth projections without issue.
Interoperability and Interfaces Objective: To determine the ability of the product to integrate with existing tools/ security tools in the organization	Standard Integration: Third-Party Products	Have endpoint detection and response (EDR) standard methods to interface/integrate with other external tools or platforms.	Determine whether the vendor currently supports standard interfaces allowing integration with external enterprise tools or platforms used in the organization.
	Custom Integration: Third-Party Products	Have standard specifications for interfacing the product with other enterprise EDR, workflow and security tools defined in your environment (e.g., IT ticketing and Windows AV systems).	Determine capabilities (e.g., API for SIEM systems) for developing custom interfaces and whether professional services are available to develop these if needed. If your organization is an application software provider, make sure that any custom programming will work with the NGAV product.

Table 3. Operational Requirements (Continued)

Functionality	Short Title	Feature	Evaluation/Criteria
Enterprise Management Objective: To determine whether the product's approach to enterprise management fits organizational expectations concerning ease of use, customization and interoperability with other enterprise tools	Management Console: Configuration	Supports a cloud-based console that runs on vendor servers.	Evaluate console configuration, including the following: <ul style="list-style-type: none"> • Does the vendor solution require any on-premises support? Ideally, there should be no infrastructure management demands. • How are updates accomplished that maintain the latest product functionality and most current security? • How often does the vendor release value-adding updates to the console? • How does the vendor communicate changes associated with these updates that may affect administrative workflows?
	Management Console: Usability & Customization	Provide a well-designed, easy to use and (if required) customizable user interface to the management console.	Evaluate overall console design from the perspectives of overall ease of use, simplicity of navigation, access to major features in an emergency, and richness of integrated help functions. Evaluate the ability of the management console to customize the user interface and reporting features to meet your specific needs.
	Scanning	Provide support for both automated (i.e., scheduled time/frequency set by admin) and on-demand scans (i.e., initiated by admins) for protected devices.	Evaluate ease of establishing both automated and on-demand scans by administrators with various skill levels. Evaluate how long it takes for each type of scan to complete.
	Status Monitoring	Support status monitoring, which includes: <ul style="list-style-type: none"> • Dashboard that reflects the overall status of connected endpoints • Status of each individual endpoint • Alerts and warnings related to the detection of malware/malicious behavior 	Review capabilities for monitoring overall status (i.e., a dashboard that reflects all endpoints), as well as the ability to quickly drill down on a given endpoint if there is an issue. Determine how the console alerts the admin to the details of problems on an endpoint (e.g., client out of date, unresolved malware detection, protection disabled). Determine whether the product provides any mechanisms to remediate or fix a problem identified in an alert or warning (e.g., remove, deactivate or reactivate a device from the management console).
	Audit Logging	Monitor and collect system health statistics to provide proof of agent uptime and show policy compliance.	Validate that appropriate audit logs are created and accessible in accordance with policy.

Table 3. Operational Requirements (Continued)

Functionality	Short Title	Feature	Evaluation/Criteria
Enterprise Management Objective: To determine ease of endpoint management, including deployment, configuration and maintenance	Endpoint Deployment	Supports both automated and manual methods for initial deployment of endpoint protection agents, such as remote push or emailing a link to users with local installation on the client.	Evaluate the impact of automated updates on end users, their devices and their work. For example: What is the impact if the update fails or is otherwise interrupted? Evaluate how easy it is for an endpoint user to trigger and install a manual update.
	Endpoint Configuration and Update	Supports a variety of methods to configure and update endpoints, including automated (centrally administered), local (controlled by endpoint user), or offline (doesn't have to be connected to the enterprise network) methods.	Review the endpoint processes and procedures related to configuration, including engine/signature/algorithm updates, scheduled/nonscheduled updates, and online/offline updates. For each configuration method needed, determine whether endpoint users can accomplish configuration on their own or whether they will need additional help. Evaluate the overall impact of the endpoint update process in terms of frequency and user productivity. Evaluate the effectiveness of cloud-based deployment. Does the product effectively push standardized policies across all endpoints, resulting in little or no drift of configurations, as can happen when dealing with multiple update servers?
	Endpoint Communications	Supports bidirectional communication of threat information between endpoints and the cloud for holistic and robust monitoring.	Determine the communication requirements to maintain real-time communication between endpoints and the cloud: <ul style="list-style-type: none"> • Bandwidth • Uptime • Latency • Redundancy Understand the impacts when the communication link fails, taking into account the length of the failure and the effect on business continuity.

Business Requirements

Finally, consider the business requirements—those factors directly tied to what the product will cost to deploy and the potential to accrue benefits. Table 4 provides a look at the features and criteria you should use to evaluate your long-term relationship with the vendor, especially in terms of support and responsiveness to your organization’s evolving needs.

Table 4. Business Requirements

Functionality	Short Title	Feature	Evaluation/Criteria
Complies with Regulatory Requirement Objective: To ensure that the product can meet any regulatory or corporate compliance requirements	Compliance Validation	Support the needs of the business relative to compliance mandates or directives.	Confirm that the product and vendor are in compliance with all relevant regulatory or corporate policies. Check the contract for items related to the cloud, including: <ul style="list-style-type: none"> • What is the status of related data centers (e.g., are they SOC 2-compliant)? • Does the contract allow for third-party audits? • Does the vendor provide its self-audit results on customer request? • What are the vendor procedures for incident response and breach notification? Consider Qualified Security Assessor (QSA) validation.
Deployment and Licensing Objective: To determine overall costs associated with NGAV	Deployment Model	Support one or more of the following deployment models: <ul style="list-style-type: none"> • Cloud-based delivery • Appliance • Other 	Evaluate the trade-offs (e.g., costs/benefits) of the various deployment models offered by the vendor. Determine staffing requirements for each model, for example, and compare those needs with your staffing goals. Also determine which model best supports the way your endpoints are deployed and the business functions they’re performing. Determine whether initial deployment will require the vendor to use third parties or professional services Find out how long initial deployment will take and whether the process will disrupt any production services in your organization.
	Licensing	Provide various licensing options (e.g., price tiers), including a description of what is included in the maintenance and support agreement for each.	Use this information to determine the overall ROI or TCO for the NGAV product solution based on the business requirements of your organization. These requirements should shorten your list of potential vendors to be considered for NGAV.

Table 4. Business Requirements (Continued)

Functionality	Short Title	Feature	Evaluation/Criteria
Support Objective: To determine the best support approach for NGAV	Support Structure	Provide various support tiers: <ul style="list-style-type: none"> • Standard business hours • 24x7, excluding or including national holidays • Expedited service 	Before making a decision on support levels, evaluate vendor responses to the following questions: <ul style="list-style-type: none"> • What are the hours for each support level? • Is local support/support provided by a third party available? • Can you reach a live person when you need help?
	Product Training	Provide product training: <ul style="list-style-type: none"> • Course(s) for both end users and administrators • Variety of delivery options, such as web-based, electronic media-based, instructor led, on-demand and/or custom training 	Evaluate the training available. <ul style="list-style-type: none"> • Who provides training? • How well does training meet organizational expectations and skill levels? • Do the delivery options support the organization’s needs? • Can the training be recorded to support a “train the trainer” approach?
	Service Level Agreements (SLAs)	Provide standard SLAs that include: <ul style="list-style-type: none"> • Service desk responsiveness • Professional services • Validation or assurance of product performance 	Determine whether the vendor provides a guarantee on software performance or support SLAs? Can the vendor’s SLAs be tailored to meet organizational business needs? What are the assurance levels—both standard targets and actual values—encountered by clients for: <ul style="list-style-type: none"> • AV effectiveness against both known and unknown attacks • AV accuracy against both known and unknown attacks • Latency (Can scan time be achieved within 60 seconds?) • Service availability (Is the service available 24x7 except for scheduled downtime?) What are the SLA boundaries? In other words, where does responsibility for items such as latency and availability start and stop? Is the NGAV vendor responsible for the “last mile” connection from endpoint(s) to the cloud?
	Professional Services	Describe professional services available that are associated with NGAV, such as: <ul style="list-style-type: none"> • Project planning/management • Interface development • Managed security service provider (MSSP) or security operations center (SOC) services 	Evaluate services that can enhance the effectiveness of the NGAV deployment.
Documentation Objective: To evaluate vendor-provided documentation	Documentation	Provide documentation for: <ul style="list-style-type: none"> • End user • Administrator • Technical specifications • API guides for integration Provide documentation in one or more of the following formats: <ul style="list-style-type: none"> • Electronic media • Paper • Online 	Consider the following in evaluating documentation: <ul style="list-style-type: none"> • Is the external documentation (i.e., manuals and online knowledge base as opposed to built-in help) clear, correct and understandable? • Does your organization have the right to copy documentation if needed? Or, do you have the right to record it? • Can your organization tailor the documentation to its needs if necessary (e.g., custom logo, customization for organizational workflow)? • Are there additional costs associated with documentation or customization?

Table 4. Business Requirements (Continued)

Functionality	Short Title	Feature	Evaluation/Criteria
Vendor Background Objective: To verify vendor experience and statements related to NGAV	Vendor Stability	Has been in business for several years with an established client installed base. Consider the factors your organization routinely uses to assess vendor stability and background.	Ask the vendor for several reference clients. Contact them and consider their experiences as they relate to your pre-identified business requirements. Does the vendor product road map align with your business needs?
Product Road Map Objective: To determine whether the vendor's growth path for the product aligns with your organizational needs	Product Road Map	Has a product road map for its NGAV product, both standalone and in conjunction with other tools provided by vendor, if appropriate.	Does the road map address key elements, such as: <ul style="list-style-type: none"> • Segmented security policy • Threat detection • Application control • Incident response • Threat hunting

Keep in mind that a cloud-based solution may require additional scrutiny in some areas, especially in the areas of confidentiality, integrity, and availability of files and processes in a more open environment, often governed by regulatory standards. Confirm what contractual controls are available from the provider. For example, will the vendor allow your review of its SOC 2 audit report? Are the formal service levels really enforceable? Will the vendor allow you to conduct an independent third-party audit?

Additionally, you need to understand what data is being released from your endpoints to support the analytics required for continued protection as well as the metadata generated from that data. Ask whether the cloud security provider utilizes a multi-tenant environment, how they secure individual customer data and, at the same time, ensure the privacy of attack data involving those customers. Be sure to review the plans and procedures that outline how the vendor will respond in the case of an incident or breach of potentially sensitive data or metadata related to your organization.

Comparing NGAV Solutions

If you end up with two or more vendors in close contention, follow a scoring process, such as the one described here, to determine which solution may be best for your organization:

1. Translate and customize these evaluation tables into a formal statement of requirements you can use to score vendor technical responses. (See Appendix A, Section 5.0 of the [“SANS Step-by-Step Guide for Procuring Next-Generation Antivirus.”](#))
2. Determine what requirements you feel are mandatory (essential or “must have”) versus optional (interesting or “nice to have”), and assign a weight to each requirement based on the importance of the requirement to your organization. Because NGAV solutions are commercial offerings, vendors may

offer some product features or support services that were not accounted for in your requirements. The SANS evaluation process accounts for this in the weighting process for scope and business need.

3. Define a rating scale that can account for how a vendor's solution will meet your requirements, as well as other important factors, such as whether the feature is demonstrable now or in a time frame defined by the vendor's product road map for its solution. (See Appendix A, Section 5.0 of the "[SANS Step-by-Step Guide for Procuring Next-Generation Antivirus](#).")
4. Build a numeric scoring sheet, ideally spreadsheet-based, that can help establish an overall score for how a vendor responds to these requirements. (See "[SANS NGAV RFP Evaluation Master Template](#).")
5. Construct a request for proposal (RFP) structure through which each vendor can provide additional, supporting product information plus actual pricing and support information in a manner that easily establishes alignment with your requirements.
6. Evaluate the completeness of each vendor response against the technical and operational requirements. Review whether and how the pricing and support structure for each vendor meets your organization's needs
7. Select the top vendor based on the overall numeric score and on how competing vendors meet your requirements, as well as their pricing and support structures. Negotiate pricing to meet your needs in terms of support and service.
8. Develop the contract (or accept the vendor's contract) and negotiate any legal terms and conditions.
9. Finalize the award, deploy the product and go!

Consider asking each vendor to score itself and then evaluate the responses against your own scoring based on the evaluation criteria. Compare the scores to help select the leading candidate.

Conclusion

Media headlines related to the billions of dollars lost each year by victims of zero-day exploits, spearphishing and sophisticated malware attacks are a constant reminder of modern cyber threats. Phishing (72%), spyware (50%), ransomware (49%) and Trojans (47%) are the leading threats seen by the respondents to the 2017 SANS Threat Landscape Survey.⁸ These modern attacks drive home the need for better protection, detection, response and remediation, with phishing, including spearphishing and whaling, and ransomware having the most significant impact on organizations.⁹

⁸ "2017 Threat Landscape Survey: Users on the Front Line," www.sans.org/reading-room/whitepapers/analyst/2017-threat-landscape-survey-users-front-line-37910, p. 4.

⁹ "2017 Threat Landscape Survey: Users on the Front Line," p. 2.

Next year, the dominant threat type will be something different. With new types of malware and malware-less exploits popping up constantly, NGAV coupled with the cloud will have a vital role in the future of endpoint detection, prevention and response. An NGAV provider can update machine learning algorithms in the cloud, allowing the most updated protective methods to be immediately available to endpoints. Organizations can avoid—even eliminate—time-consuming update processes. Ultimately, the NGAV- and cloud-coupled solutions might even tilt the advantage to the defenders or at least balance the playing field against the attackers.

Keep in mind, however, that a cloud-based solution may require a different emphasis on how you approach protecting your endpoints. Your organization may eliminate initial and ongoing hardware and software investments and, to some extent, help refocus valuable staff resources on more effective and challenging security activities.

Measures such as total cost of ownership and return on investment won't disappear, but the related line items may shift to new areas of emphasis. Don't neglect budgeting for needed long-term infrastructure commitments related to telecommunications, managing support contracts and maintaining a knowledge workforce to oversee your NGAV provider.

The keys are: first, to avoid the hype, and second, to evaluate the many products claiming to be next-gen AV. This guide should help readers design an effective evaluation program.

About the Author

Barbara Filkins, a senior SANS analyst who holds the CISSP and SANS GSEC (Gold), GCIH (Gold), GSLC (Gold), GCCC (Gold) and GCPM (Silver) certifications, has done extensive work in system procurement, vendor selection and vendor negotiations as a systems engineering and infrastructure design consultant. She is deeply involved with HIPAA security issues in the health and human services industry, with clients ranging from federal agencies (Department of Defense and Department of Veterans Affairs) to municipalities and commercial businesses. Barbara focuses on issues related to automation—privacy, identity theft and exposure to fraud, as well as the legal aspects of enforcing information security in today’s mobile and cloud environments.

SANS would like to thank Carbon Black for its support of this paper.