Essential Requirements for Cloud-Based Endpoint Security

Next-generation endpoint security (NGES) strives to combine prevention, detection, response and IT operations into a single platform, allowing for the consolidation of the endpoint footprint while substantially increasing endpoint protection. For those ready to replace their traditional antivirus with NGES, SANS has developed this evaluation guide for assessing NGES tools against your organization's requirements before making capital investments in NGES.

A SANS Whitepaper

Essential Requirements for Cloud-Based Endpoint Security

The SANS Guide to Evaluating Next-Generation Endpoint Security

Written by **Barbara Filkins**

September 2018

Introduction

Endpoint protection began in the late 1980s with the introduction of the traditional antivirus (AV) that continues today as the first line of defense against known malware. But with the growth of cloud computing and mobile devices, the network perimeter has truly moved to the endpoint, and with that move comes the need for new techniques and tools that can counter threats before they take root.

Traditional AV relies on malware signatures and simplistic behavioral rules to uncover threats to critical information endpoints: servers, applications, workstations and mobile computing devices. It also has a built-in time delay between when a threat is identified and a solution is published. While legacy (or traditional) AV 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.

Closing this "window of vulnerability," defined in the OWASP Testing Guide v4, has become key to endpoint protection. This approach "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."[1]

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

Endpoint protection requires an operations lifecycle approach that seeks to aggressively close the window of vulnerability, driving toward continuous processes for detection, prevention and response, and tuning the tools to ensure that, once detected, patterns of attack never occur again. Modern organizations are looking to replace their current solutions with next-generation endpoint security and operations platforms that use more powerful approaches based on big data and analytics to detect and prevent modern attacks, not just known malware. Next-generation endpoint security (NGES) strives to combine prevention, detection, response and IT operations into a single platform, allowing for the consolidation of the endpoint footprint while substantially increasing endpoint protection.

The dynamics of cloud-based analytics, which allow for near real-time operations, bring an essential dimension to NGES, 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 of NGES 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 of 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, HIPPA or GDPR, to more subjective losses, such as loss of competitive advantage and 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.

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

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 NGES enabled by the predictive cloud include:

- **Up-to-date protection against new attacks and threats.** The threat landscape is changing quicker than 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.

- **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 that support embedded security operations.** Cloud-based next-generation endpoint security platforms need to provide teams with built-in tools that allow administrators to access live endpoints for a wide range of operational tasks, including vulnerability assessment, IT hygiene, query-based investigation, and hands-on remediation. Proactive measures minimize exposure, and reactive operations make sure analysts have what they need when time is of the essence.

Between its better protection and simplified operations, next-generation endpoint security in the cloud offers significantly more value than its predecessors.

For those ready to replace their traditional antivirus with NGES, SANS has developed this evaluation guide for assessing NGES tools against your organization's requirements before making capital investments in NGES. 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.

If you are familiar with the 2017 NGAV Evaluation Guide and its artifacts, the following tools can be adapted to help determine what to look for in a cloud-augmented NGES 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.
- **The "SANS NGAV Request for Proposal/Request for Information template."** 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.

Visualizing Next-Generation Endpoint Security

The starting point for developing an approach to NGES evaluation is being able to visualize what it actually encompasses: understanding where your endpoint security is today, where you would like it to be and the approach you need to most effectively close your current window of vulnerability. Equally important is defining your organization's key requirements, by which you can evaluate and select the best NGES product for your organization.

Endpoint Protection—Yesterday and Today

Figure 1 presents a high-level, side-by-side comparison of the various levels in NGES, moving from a largely manual environment toward one based on continuous capture and monitoring of endpoint information.

Security Phase	Maturity Factors	Level of Endpoint Management			
		Manual	**Consolidation**	**Correlation**	**Continuous**
	Integration	Lowest rate of effectiveness	Alerts, logs consolidated in SIEM	Data correlated across devices	Holistic High rate of effectiveness Automation achieved through workflow, API
Detection		Point in time identification AV signatures Only know malware	Reputation data Algorithms	Single-source threat intelligence Simple indicators of compromise	Patterns and behavior Aggregated multi-vendor threat intel
Prevention		AV signatures Only stop known malware	Privileged account management Basic whitelisting Anti-exploitation	Policy-based by role	Automated tied in with vulnerability management Customizable forms of prevention Moving towards zero-day protection
Response		Reimage machines No root cause analysis	Manual root cause analysis Forensics limited to post mortem	Automated root cause and scope analysis	Attack disruption and containment Automated remediation
	Visibility	Individual polling, scanning	Emerging data standards Metrics Manual review of logs	Accepted data standards Continuous recording of most endpoint data Near real time dashboard	Real-time visibility and continuous recording of endpoint activity to support collaborative defense

RISK DECREASING

WINDOW OF VULNERABILITY INCREASING

Figure 1. Endpoint Protection Evolution

NGES represents an endpoint security architecture oriented toward a cloud-based, big data analytics engine built on data science, machine learning and threat intelligence, and one that can be tuned to provide deep attack context and insight into both known and previously unknown patterns of attack. NGES 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.[2]

Beyond Signatures

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

Vectors for *malwareless* 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.

[2] www.technologydecisions.com.au/content/security/article/new-wave-of-cyber-attacks-using-little-or-no-malware-471763824#axzz4OI

protection and monitoring solutions while taking advantage of the elevated privileges that come with utilities.

NGES 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, NGES 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 NGES 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.

Fully Integrated, Collaborative Security and IT Operations

An organization's security posture depends on more than a strong security policy; it also requires effective operational processes and reliable implementation. Security operations are often overlooked in modern security platforms, yet they can vastly improve an organization's ability to protect its environment and respond to threats.

There are two key operational components that next-generation endpoint security solutions should provide. The first is a live query engine that provides administrators with the ability to query active endpoints in real time for hundreds of data points and deliver comprehensive reports. This capability has wide-ranging value for vulnerability assessments, proactive IT hygiene, compliance, forensic investigation and numerous other functions. The second component is a live response engine that allows professionals to access endpoints through a secure, remote shell for deep investigative and remediation purposes. By embedding security operations directly in the platform, security professionals close the gap between security policy and security implementation.

Evaluation Architecture for NGES

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

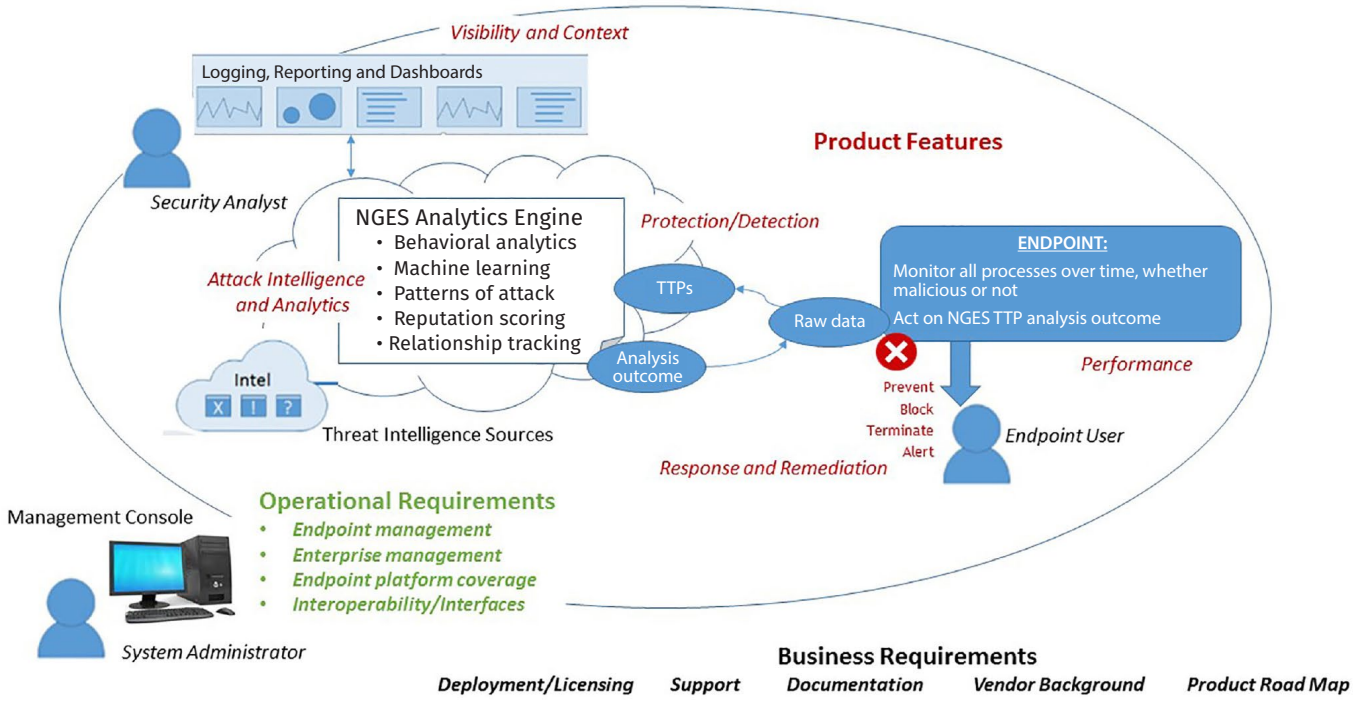

Figure 2. NGES Requirements Visualization

Planning and Preparation

NGES 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, what and how will the product detect attacks, including unknown and malwareless 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 NGES 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 will a cloud-based infrastructure change my typical operating procedure?

Preparing to Evaluate

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 NGES 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.

Attacks today have become far more complex. 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.

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

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

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 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 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 NGES should show
   - Documents the anticipated performance and outcomes based on your preliminary review of the product's features
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.

Q. *My organization is simply not well equipped to conduct our own in-house testing. Can't I just trust third-party assessments of endpoint protection 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. Make sure that these tests take into account attack trends projected over the next 12 months and that they address known and unknown malware, malware variants and malwareless attacks.

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

There are additional considerations when entering the procurement process for acquiring an NGES solution based on cloud services. Table 1 summarizes where these requirements fall in the following tables.

Table 1. Further Considerations for NGES and the Cloud

Area	Things to Consider
Product Features	**Threat Detection:** Look for improved methods for threat detection with continued emphasis on malwareless and fileless 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 is only ever going to be able to detect or predict attacks that have already been seen elsewhere. **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 NGES vendor. **Secure Communication from Cloud to Endpoints:** Make sure that the path from the cloud to the endpoint is encrypted and the method that is used to authenticate an endpoint to the cloud is robust and impervious to attack.
Operational Requirements	**Cloud-Based Management Console:** Advantages include lack of demand on corporate infrastructure (storage, processing and so forth), automatic endpoint updates to maintain the latest security, and standardized policies across all endpoints (which means 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. **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 endpoint(s). Make sure you document the communication demands and understand the potential impact of downtime.
Business Requirements	**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 than the vendor? **Service Levels:** Enforceable service levels become important in a cloud-enabled solution to ensure performance in protection against known threats and attack behaviors as well as unknown threats.

The features and the operational and business requirements for evaluating a cloud-based NGES solution are laid out in the following three tables.

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 NGES 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 NGES solution to determine whether it can block sophisticated, advanced attacks as well as those that are known.
	Available Prevention Methods	Access to multiple forms of prevention, including ability to select and customize based on the specific endpoint (e.g., software developer workstations, where new code is created and tested as opposed to a mobile tablet using a browser to access sensitive data).	Determine whether the product supports methods required by your organization: • Reactive methods—Blacklisting, signatures, behaviors, static and dynamic analysis, sandboxing • Proactive methods—Application control, privilege management, anti-exploitation hardening (ASLR), process and network isolation, default-deny (whitelisting)
	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): • 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 (Attack Disruption)	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 the 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 fileless persistence scenario.
	Custom Rules Development	Provide ability to create rules unique to the organization.	Verify that the product provides an easy-to-use interface for local rule development (i.e., authorized staff members). Ensure that custom rules can be shared internally across the organization and externally as required.
	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: • 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 NGES 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.

(Continued on next page.)

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	Ensure that the product does not filter out data that is unrelated to known threats. Instead, determine that the product can send unfiltered endpoint activity to the cloud for advanced processing and identification of new threats. 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.
	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 NGES 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 NGES, using a cloud-based intelligence and analytics engine.	Gather the following information: • 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.	Require the vendor to demonstrate its support of the following: • Open sharing • Protection of confidentiality when sharing information • Feedback from users • Community participation and research

(Continued on next page.)

Table 2. Product Features/Capabilities (Continued)

Functionality	Short Title	Feature	Evaluation/Criteria
Visibility and Context **Objective:** To determine how the product provides visibility into security events and attack context Can the product provide answers to key questions related to detection, response and remediation, such as: • 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.[3]	Determine what the standard (e.g., minimum) set of data elements is for both activities. 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.
	Response Logging	Log all resulting actions taken in response to detection of malware/malicious behavior.	
	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 NGES 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 (Live Endpoint Query)	Build and customize queries and reports related to endpoint state and activity across the entire organization.	Determine whether the product has the ability to easily: • Query endpoints using a rich query language (similar to the open-source `OSQuery` package). • Collect real-time state from all endpoints (e.g., processes, file changes, registry access, network connections and users). • Deliver reports covering the entire endpoint environment based on the results of any query.
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 affect 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: • 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.

[3] Some of these criteria are paraphrased from ICSA antivirus/spyware certification materials. See www.icsalabs.com

Operational Requirements

Operational requirements go beyond product features. For example, they encompass how a user interacts with the NGES product at the endpoint, as well as 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: • 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 this be tested against malware that is "virtual aware?" What are vendor recommendations on this 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 NGES product.

(Continued on next page.)

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**	Support a cloud-based console.	Evaluate console configuration including the following: • 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-added updates to the console? • How does the vendor communicate the 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: • 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.
	Collaborative Defense	Support workflows involving various security-related roles/groups such as SOC, incident response and forensics.	Evaluate the tools that support the design and implementation of role-based processes that follow best practices or are specific to the organization.

(Continued on next page.)

Table 3. Operational Requirements (Continued)

Functionality	Short Title	Feature	Evaluation/Criteria
Endpoint Management **Objective:** To determine ease of endpoint management, including deployment, configuration and maintenance	**Endpoint Deployment**	Support 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	Support 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	Support 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: • Bandwidth • Uptime • Latency • Redundancy Understand the impact 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 the product and vendor are in compliance with all relevant regulatory or corporate policies. Check the contract for items related to the cloud, including: • 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 Model	Support one or more of the following deployment models: • 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 NGES product solution based on the business requirements of your organization. These requirements should shorten your list of potential vendors to be considered for NGES.

(Continued on next page.)

Table 4. Business Requirements (Continued)

Functionality	Short Title	Feature	Evaluation/Criteria
Support **Objective:** To determine the best support approach for NGES	**Support Structure**	Provide various support tiers: • 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: • 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: • 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. • 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: • 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: • NGES effectiveness against both known and unknown attacks • NGES accuracy against both known and unknown attack • 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 like latency and availability start and stop? Is the NGES vendor responsible for the "last mile" connection from endpoint(s) to the cloud?
	Professional Services	Describe professional services available that are associated with NGES, such as: • 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 NGES deployment.
Documentation **Objective:** To evaluate vendor-provided documentation	**Documentation**	Provide documentation for: • End user • Administrator • Technical specifications • API guides for integration Provide documentation in one or more of the following formats: • Electronic media • Paper • Online	Consider the following in evaluating documentation: • 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?

(Continued on next page.)

Table 4. Business Requirements (Continued)

Functionality	Short Title	Feature	Evaluation/Criteria
Vendor Background **Objective:** To verify vendor experience and statements related to NGES	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.
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 NGES product, both standalone and in conjunction with other tools provided by vendor, if appropriate.	Does the vendor product road map align with your business needs? Does the road map address key elements, such as: • 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. For example, you should hold providers of a cloud-based security solution to the highest standards practical for security, availability, processing integrity, confidentiality and privacy. Without direct access to confirm compliance with these standards, your organization must rely on contractual controls, such as allowing your review of the vendor's SOC 2 audit report, and formal, enforceable service levels.

Additionally, a cloud security provider must provide a robust, multi-tenant environment that isolates information gleaned from each customer while maintaining the privacy of attack data affecting those customers. This puts an emphasis not only on knowing what data is being provided to the cloud from your endpoints, but also on knowing how the vendor will respond in the case of an incident or breach of potentially sensitive data or metadata related to your organization.

Comparing NGES 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.
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 NGES 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.
4. Build a numeric scoring sheet, ideally spreadsheet-based, that can help establish an overall score for how a vendor responds to these requirements.
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.[4] These modern attacks drive home the need for better protection, detection, response and remediation. Phishing, which includes spearphishing and whaling, and ransomware have the most significant impact on organizations.[5]

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

[5] "2017 Threat Landscape Survey: Users on the Front Line," August 2017, p. 2.

Next year, the dominant threat type will be something different. With new types of malware and malwareless exploits popping up constantly, NGES coupled with the cloud will have a vital role in the future of endpoint detection, prevention and response. An NGES 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 NGES- 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 impactful 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 NGES provider.

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

About the Author

Barbara Filkins, a senior SANS analyst, holds several SANS certifications, including the GSEC, GCIH, GCPM, GLEG and GICSP, the CISSP, and an MS in information security management from the SANS Technology Institute. She has done extensive work in system procurement, vendor selection and vendor negotiations as a systems engineering and infrastructure design consultant. Barbara focuses on issues related to automation—privacy, identity theft and exposure to fraud, plus the legal aspects of enforcing information security in today's mobile and cloud environments, particularly in the health and human services industry, with clients ranging from federal agencies to municipalities and commercial businesses.

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

Last Updated: September 21st, 2018

Upcoming SANS Training

Click here to view a list of all SANS Courses

Oil & Gas Cybersecurity Summit & Training 2018	Houston, TXUS	Oct 01, 2018 - Oct 06, 2018	Live Event
SANS DFIR Prague Summit & Training 2018	Prague, CZ	Oct 01, 2018 - Oct 07, 2018	Live Event
SANS Brussels October 2018	Brussels, BE	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Amsterdam October 2018	Amsterdam, NL	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Riyadh October 2018	Riyadh, SA	Oct 13, 2018 - Oct 18, 2018	Live Event
SANS Northern VA Fall- Tysons 2018	McLean, VAUS	Oct 13, 2018 - Oct 20, 2018	Live Event
SANS October Singapore 2018	Singapore, SG	Oct 15, 2018 - Oct 27, 2018	Live Event
SANS London October 2018	London, GB	Oct 15, 2018 - Oct 20, 2018	Live Event
SANS Denver 2018	Denver, COUS	Oct 15, 2018 - Oct 20, 2018	Live Event
SANS Seattle Fall 2018	Seattle, WAUS	Oct 15, 2018 - Oct 20, 2018	Live Event
Secure DevOps Summit & Training 2018	Denver, COUS	Oct 22, 2018 - Oct 29, 2018	Live Event
SANS Houston 2018	Houston, TXUS	Oct 29, 2018 - Nov 03, 2018	Live Event
SANS Gulf Region 2018	Dubai, AE	Nov 03, 2018 - Nov 15, 2018	Live Event
SANS DFIRCON Miami 2018	Miami, FLUS	Nov 05, 2018 - Nov 10, 2018	Live Event
SANS Dallas Fall 2018	Dallas, TXUS	Nov 05, 2018 - Nov 10, 2018	Live Event
SANS London November 2018	London, GB	Nov 05, 2018 - Nov 10, 2018	Live Event
SANS Sydney 2018	Sydney, AU	Nov 05, 2018 - Nov 17, 2018	Live Event
SANS San Diego Fall 2018	San Diego, CAUS	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS Mumbai 2018	Mumbai, IN	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS Rome 2018	Rome, IT	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS Osaka 2018	Osaka, JP	Nov 12, 2018 - Nov 17, 2018	Live Event
Pen Test HackFest Summit & Training 2018	Bethesda, MDUS	Nov 12, 2018 - Nov 19, 2018	Live Event
SANS ICS410 Perth 2018	Perth, AU	Nov 19, 2018 - Nov 23, 2018	Live Event
SANS November Singapore 2018	Singapore, SG	Nov 19, 2018 - Nov 24, 2018	Live Event
SANS Paris November 2018	Paris, FR	Nov 19, 2018 - Nov 24, 2018	Live Event
European Security Awareness Summit 2018	London, GB	Nov 26, 2018 - Nov 29, 2018	Live Event
SANS Austin 2018	Austin, TXUS	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS Stockholm 2018	Stockholm, SE	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS San Francisco Fall 2018	San Francisco, CAUS	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS Khobar 2018	Khobar, SA	Dec 01, 2018 - Dec 06, 2018	Live Event
SANS Santa Monica 2018	Santa Monica, CAUS	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS Nashville 2018	Nashville, TNUS	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS Network Security 2018	OnlineNVUS	Sep 23, 2018 - Sep 30, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced