

# JumpStart Guide for Endpoint Security in AWS

Written by **David Hazar**

June 2019

*Sponsored by:*

**AWS Marketplace**  
in conjunction with  
**Optiv**

## Introduction

Endpoint security options and products are continuing to mature. Enterprises and other organizations are moving away from point solutions—antivirus (AV) or anti-malware, host-based intrusion detection systems (HIDSs), file integrity monitoring (FIM) and application whitelisting—toward more robust endpoint protection platforms (EPPs). And many of those EPPs include new, advanced endpoint detection and response (EDR) capabilities. This move is similar to other efforts to consolidate the functionality of multiple security capabilities into a single solution or platform to make it easier for organizations to implement and maintain these technologies.

Just as these firewalls bring the capabilities of many different security appliances into a single solution, EPPs bring the capabilities of many endpoint security agents into a single agent, or at least a single management platform.

Gartner describes EPPs as “a solution deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts.” A wide range of products and solutions falls into this category, in part because there is no strict definition of required capabilities for them to be considered EPPs. That’s why you will find many traditional point solutions from recognizable vendors included in

*Just as next-generation firewalls bring the capabilities of many different security appliances into a single solution, EPPs bring the capabilities of many endpoint security agents into a single agent.*

this category, albeit bundled together with some new solutions or with the addition of some new capabilities. You will also find more recent entrants into the endpoint security market that may have new, innovative approaches to endpoint security but may also lack maturity in more traditional detection and response capabilities.

Selecting and implementing endpoint security in hybrid architectures can be a time-consuming and confusing process. In this paper, we present what customers should consider when evaluating endpoint security technology in the cloud. We discuss a high-level strategy for evaluating these solutions and then discuss implementation options that organizations need to consider when planning to implement these technologies in Amazon Web Services (AWS). We also review why businesses may choose to implement endpoint security in the cloud along with the various needs and capabilities associated with different endpoint security solutions. Lastly, we discuss some of the considerations that should be part of the evaluation process for endpoint security in general, but then take a closer look at the considerations specific to implementing endpoint security in AWS.

Not all companies may choose or be able to implement endpoint security for all of their cloud workloads. Because much of the technology associated with endpoint security is installed and runs as an agent, infrastructure-as-a-service (IaaS) cloud workloads are the most obvious candidates. In AWS, endpoint security solutions typically work with EC2 Instances or virtual machines (VMs) created on VMware Cloud on AWS. While these technologies could technically also be leveraged within containerized environments, such a situation is less typical and other container security technologies may be better suited in this type of environment. This paper focuses on implementation via instances or VMs, but most of the considerations still apply to a containerized environment.

Some cloud service types, such as platform-as-a-service (PaaS), function-as-a-service (FaaS) and software-as-a-service (SaaS), are not supported by many endpoint security technologies. However, the considerations outlined in this paper can help customers determine what protections vendors provide for these service types. There is also a case to be made for leveraging the cloud shared-responsibility model to reduce an organization's security burden if the risk for those workloads does not merit the increased visibility or if an organization feels it cannot provide better protection than the cloud vendor even with the increased visibility. In these situations, leveraging PaaS, FaaS and SaaS cloud services can help.

## Understanding Your Needs

In order to evaluate endpoint security, organizations need to have a solid understanding of what capabilities are must-haves versus nice-to-haves to provide the level of protection and visibility they desire. They must also consider how the endpoint security program will be implemented, operated and maintained. Organizations should avoid purchasing technology if there is not sufficient support, funding, resourcing and processes in place to successfully implement, operate and maintain the technology for years.

After the organization determines and ranks capabilities, it needs to look at existing endpoint security technology, people and processes to understand what is currently in place and whether it is well suited for the cloud. Then, it should investigate alternative technologies, including any cloud-optimized solutions, and catalog the resources and skills that will be required, along with the policies, standards and processes that may need to be updated. This investigation will not be a one-time exercise; these points will be revisited many times throughout the evaluation process before making a choice.

## Implementation Options in AWS

When the cloud was new, the only real option was to leverage technology similar to what an organization was already using on premises, if not the same technology. If you already have a successful and functional on-premises program, this can be an attractive option, but it is not the only option. Review the different options you have available, including cloud-optimized, managed services and licensing options. Then, once you have a rough idea of how you would like to implement endpoint security in AWS, it is time to start building a business case.

### Cloud-Optimized

Organizations may want to look at cloud-optimized solutions for endpoint security in the cloud. Even though performance is a concern in on-premises environments, it is an even larger concern in the cloud. Traditional endpoint security technology is typically not performance-friendly. In on-premises environments, the costs for this overhead are not always as easy to see or calculate because there is usually excess capacity that can be used to compensate for the overhead. In the cloud, however, with on-demand pricing and the detailed metrics, the cost of this overhead is much easier to understand. Many cloud-optimized endpoint security tools focus on creating lightweight agents that offload the processing of data and events to other resources or even to a separate, vendor-maintained cloud environment.

### Managed Services

Another option for implementing endpoint security in the cloud is to leverage a managed service provider that has experience implementing and maintaining these solutions in the cloud. Using such a provider can be a promising option for many organizations but is especially attractive for organizations that have limited cloud experience or that do not already have endpoint security capabilities. Another advantage of managed service providers is that they typically provide skilled resources and bring with them proven processes and existing cloud vendor contacts and relationships to accelerate implementation and add value quickly. They may also supplement the endpoint security technology with human-assisted analysis, custom development or configuration, and even incident response capabilities. These managed service providers can even extend AWS Marketplace solutions directly to customers through Consulting Partner Private Offers and assist with evaluating licensing options.<sup>1</sup>

*Organizations should avoid purchasing technology if there is not sufficient support, funding, resourcing and processes in place to successfully implement, operate and maintain the technology for years.*

<sup>1</sup> Consulting Partners Can Now Resell Software Solutions in AWS Marketplace, <https://aws.amazon.com/marketplace/features/cpprivateoffers>

## Licensing Options

When considering how to implement endpoint security in the cloud, also consider how to license any chosen technology. If you are planning on using existing on-premises endpoint security capabilities, your organization may already have favorable licensing and it may make sense to follow a bring-your-own-license (BYOL) model. Maybe endpoint security is new to your organization, or maybe you want to evaluate a technology without implementing it more broadly. Perhaps you determine you need a different technology for the cloud or your organization favors on-demand pricing or operational cost structures. If any of those scenarios apply to you, you'll be relieved to learn that many of the products are available with on-demand pricing from AWS Marketplace. (AWS Marketplace can still be leveraged for many of these technologies following the BYOL approach as well).

## Needs and Capabilities

Cloud architecture differs from what we are used to in our on-premises environments. In the cloud, almost everything is software-defined—and we do not have complete visibility into our resources and surrounding infrastructure. Also, because commissioning and decommissioning resources are so easy to do and costs are typically accrued based on the amount of time the resource is running, cloud resources tend to have much shorter lifecycles. The capabilities surrounding forensics in the cloud are also much less mature than for on-premises environments, and leveraging endpoint security can provide valuable threat intelligence for an organization's cloud ecosystem that it may not be getting from its PaaS, FaaS and SaaS workloads.

Next, we look at some of the solutions or capabilities that may exist within endpoint protection platforms and then move on to the topics organizations should consider when preparing to implement endpoint security in the cloud.

## Needs and Capabilities

Note the overlap between the solutions listed below. For example, EDR solutions may provide many of the same capabilities as AV/anti-malware or HIDS solutions. Some AV solutions may also include behavior monitoring, and both HIDS and EDR solutions will most likely perform FIM. This overlap in capabilities will be one of the considerations for organizations that choose to utilize more than one solution.



### Endpoint Detection and Response

**The need:** Identifying and protecting against unknown threats

#### Capabilities

- Detecting security incidents
  - Behavior monitoring
  - Analytics
  - Sandboxing

- Containing the incident at the endpoint
- Investigating security incidents
- Providing remediation guidance



## Antivirus/Anti-malware

**The need:** Identifying and protecting against known threats

### Capabilities

- Detecting viruses and malware
  - Signature analysis
  - Behavior monitoring
- Blocking and quarantining the virus or malware
- Alerting users and administrators of infection



## Host-based Intrusion Detection

**The need:** Identifying indicators of compromise

### Capabilities

- Detecting suspect behavior
  - Behavior monitoring
  - Traffic analysis
  - FIM
- Alerting users and administrators of suspect behavior



## File Integrity Monitoring

**The need:** Identifying changes to critical or sensitive files

### Capabilities

- Collecting and storing signature data for policy-defined files
- Offering interval-based or real-time signature validation
- Alerting users or administrators when tracked files are modified



## Application Whitelisting

**The need:** Only allowing approved or authorized, signed software to execute

### Capabilities

- Authorizing software or software signing certificates via policy
- Applying policies to resources
- Blocking or alerting when unauthorized software executes

# General Cloud Endpoint Security Considerations

Regardless of the endpoint security technology or cloud vendor selected, some general business, technical and operational considerations are associated with implementing endpoint security in the cloud. The following sections highlight many of these considerations.

## Business Considerations

	Consideration	Details
	Policies and standards	<p>Traditional endpoint security requirements in policies and standards may not be achievable in the cloud, may not function as intended or may not be cost-effective.</p> <p>Organizations will need to evaluate cloud capabilities to determine what changes need to be made to ensure that compliance with policies and standards is achievable.</p>
	Governance model	<p>Every organization has a unique governance model. Some organizations have very centralized governance over endpoint security, whereas others may follow a more decentralized approach.</p> <p>Organizations will need to decide whether to centralize or decentralize governance over cloud endpoint security. Then, they must determine whether existing governance models used for traditional endpoint security can be extended to the cloud or whether a cloud-specific model is required. Consider that cloud workloads can easily span the globe and that data residency and visibility restrictions may apply in certain regions.</p>
	Reporting and metrics	<p>Providing the right metrics, key performance indicators (KPIs) and key risk indicators (KRIs) to the right stakeholders may require changes that account for cloud architecture.</p> <p>Organizations will need to define reporting requirements specific to cloud workloads and evaluate products against these requirements</p>
	Funding and support	<p>Funding and support for cloud endpoint security may not currently be available. Organizations may not understand the shared responsibility model as it pertains to cloud usage and may assume that endpoint security is provided by the cloud vendor.</p> <p>Organizations will need to understand the requirements and determine the appropriate funding and support model. What is required may differ based on the implementation model the organization chooses (for instance, traditional vs. cloud, BYOL vs. on-demand).</p>
	Risk classification	<p>Not all workloads share the same risk profile. It is important that organizations consider the risk associated with different cloud workloads to enable them to implement controls based on risk.</p> <p>If cost is not a consideration or if the risks are similar for all workloads, then a single approach to endpoint security may be appropriate. If risks vary greatly among workloads or costs are high, however, an organization will need to understand the various risk profiles to determine where to focus or require endpoint security or what to require for each profile.</p>

## Technical Considerations

	Consideration	Details
	Endpoint security capabilities	<p>As organizations update policies and standards to address cloud workloads, they should also identify the technologies they need to comply with these new requirements.</p> <p>Some organizations may choose to be prescriptive about the technologies they use, whereas others may define the required capabilities and allow individual cloud operations teams to select their own technologies as long as they can validate compliance with requirements.</p>
	Supported technology	<p>Some technologies may not be supported for all cloud services or for all platforms running on cloud services.</p> <p>Organizations will need to decide whether they will allow the use of services and platforms that do not support endpoint security requirements, and if so, under what conditions. These decisions should be documented and maintained so they may be consistently applied throughout the organization.</p>
	Agent-based technologies	<p>No matter how lightweight, agent-based technologies decrease performance (most cloud endpoint security technologies are agent-based). In the cloud, they increase costs.</p> <p>Organizations may have a restriction on the number of agents that can be installed on each cloud resource. Organizations need to determine how many non-endpoint security agents are already in place to decide whether they need to consider an increase in their limits. They may also have a specific overhead allowance for agents, which needs to be evaluated during any proof of concept. Performance should be assessed before purchase, before upgrades, when configurations change and at regular intervals. Metrics should include overhead and performance monitoring.</p>
	Active vs. interval-based or asynchronous detection and response	<p>Technologies that provide active detection and response may require more overhead than technologies that scan at given intervals, during off-peak hours or asynchronously via out-of-band analysis engines.</p> <p>Organizations need to decide whether active detection and response are required or acceptable based on their cloud architecture. In particular, the longevity of cloud resources may affect this decision. Short-lived cloud resources may require more active defenses.</p>
	Secure communication	<p>Endpoint security solutions all typically communicate with external components or services. The external services could provide product updates or configuration data. They may also be involved in the analysis of data from the target system.</p> <p>Organizations need to ensure that external communication is authenticated and secured.</p>

## Operational Considerations

	Consideration	Details
	Operational responsibility and model	<p>Operation of cloud resources is substantially different from traditional infrastructure operations. This difference may help determine who is responsible for implementing and configuring endpoint security capabilities.</p> <p>Organizations need to decide how best to implement and configure endpoint security technology and determine which group(s) should be responsible for this task. They also need to determine whether operations should be centralized or decentralized.</p>
	Monitoring and response	<p>While implementation and configuration of endpoint security capabilities may be assigned to an existing cloud operations team, monitoring may be the responsibility of others. Response could be the responsibility of either team.</p> <p>Organizations need to determine who will be responsible for monitoring and responding to endpoint security events. They will also need to evaluate what orchestration and automation of technology, people and processes can be leveraged or integrated into the final solution.</p>
	Processes and procedures	<p>Organizations may have very specific processes and procedures for dealing with endpoint security events related to their traditional on-premises infrastructure. It is likely, however, that these processes and procedures will be different in the cloud.</p> <p>Organizations need to create new operational processes and procedures for endpoint security in the cloud, considering any changes they have made to policies and standards related to cloud or endpoint security in the cloud.</p>

# AWS Implementation Considerations

The general considerations discussed so far can help organizations lay the groundwork as well as secure funding and support for cloud endpoint detection. Now let's take a more detailed look at some specific considerations an organization will need to evaluate before implementing these solutions in AWS.

## Endpoint Detection and Response

The advantage of EDR solutions is that they focus on adding capabilities that allow them to identify unknown threats. If your organization's threat profile includes targeted attacks or advanced threat actors, consider endpoint protection platforms that excel in EDR. You may also consider EDR for high-risk workloads or for performance reasons, because many of these solutions offload processing to other resources. False positive rates may be higher for EDR than some other types of tools.

	Consideration	Details
	Cloud context support	<p>Due to the dynamic nature of the cloud, a resource that existed a few hours ago may not exist now. Because many EDR technologies perform analysis of data or binaries external to the resource itself, there is a chance that when analysis is completed the resource may no longer exist.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"><li>• The additional cloud context (specifically, tags or image IDs) that is captured, retained and used by EDR technology to allow correlation of findings and behavior with resources and the images and image versions used to create those resources</li><li>• The special concerns associated with studying resources that have potentially replaced the original resource from which data was gathered</li></ul>
	Performance and efficiency	<p>Many EDR platforms claim to have lightweight agents that offload analysis and processing tasks to other systems. Customers should analyze the impact and performance on production workloads. Due to the offload architecture, these technologies typically send data and binaries to separate systems or to the vendor's cloud infrastructure to perform analysis. Depending on the cloud regions in use, the transfer of data and binaries to external resources could affect both the performance and the cost of the technology. In addition, depending on the architecture, analyzing the same data and binaries from multiple systems may add additional processing time and reduce efficiency.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"><li>• The architecture of the tools under consideration</li><li>• Performance (CPU, memory, storage and bandwidth utilization) when used with production workloads</li><li>• The amount of data and binaries that will be transferred and to what location(s) the data is being transferred</li><li>• Potential impacts on cost and performance due to bandwidth</li><li>• Performance impact of latency between all cloud regions in use and any identified external resources</li><li>• Efficiency of coordination between agent and analysis engine(s) and efficiency of threat data distribution</li><li>• Support for data compression</li></ul>

## Endpoint Detection and Response (continued)

	Consideration	Details
	Deployment	<p>EDR platforms may require the implementation of multiple components, and these components may need to be installed in multiple zones or regions to support distributed cloud environments. They also require the implementation of agents on the supported endpoints.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• The architecture of the tools under consideration</li> <li>• The installation and configuration procedures for each component and agent</li> <li>• The availability of managed or SaaS components or preconfigured appliances from AWS Marketplace</li> <li>• Effectiveness and responsiveness of support</li> <li>• Any vendor requirements for the use of professional services for installation or configuration</li> <li>• Integration with other AWS technologies for deployment or validation of agent deployment (AWS Systems Manager, AWS Config, Amazon CloudWatch)<sup>2</sup></li> </ul>
	Configuration and maintenance	<p>In order to improve the quality of detection and response, EDR technologies may require extensive configuration and maintenance. Customization of detection rules and response scripts may be available depending on product. In addition, EDR components and agents will need to be upgraded and may also require updates to datasets used for analysis.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• The architecture of the tools under consideration</li> <li>• The upgrade procedures</li> <li>• The procedures for updating any datasets leveraged by analysis engines or agents</li> <li>• Reporting, metrics or alerting available for any out-of-date components, agents or data</li> <li>• Communication protocols and paths to understand required firewall and ACL changes along with any VPC peering or cross-account access</li> <li>• Any vendor requirements for the use of professional services for upgrades or updates</li> <li>• Accessibility to detection rules, scripts and other configuration details (open or proprietary)</li> <li>• Whether the platform allows customers to build or create their own rules</li> <li>• Level of effort to perform customizations to rules, scripts or configurations or to create new rules</li> <li>• Integrations with other AWS technologies (such as AWS Config, AWS Lambda) or configuration management tools (Puppet, Chef, Ansible, SaltStack, CFEngine) to perform updates or upgrades or apply configurations</li> <li>• Secure configuration guides and best practices</li> </ul>
	Detection	<p>Because EDR technologies support detecting both known and unknown threats, organizations should evaluate their effectiveness as part of the selection process.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• Detection rate of any well-known or unknown malware samples, if your organization practices malware analysis and has appropriate analysis environments</li> <li>• Detection methods employed</li> <li>• Available benchmarks or comparisons by third-party evaluators</li> <li>• Product reviews and customer forums</li> <li>• Customer references</li> <li>• Whether detection is real-time, interval-based, asynchronous or configurable for each detection mechanism supported</li> <li>• Whether detection includes detection of non-file-based malware (such as memory resident malware)</li> </ul>

<sup>2</sup> This paper mentions product names to provide real-life examples of how visibility tools can be used. The use of these examples is not an endorsement of any product.

## Endpoint Detection and Response (continued)

	Consideration	Details
	Integration	<p>Many EDR platforms also integrate with other business and security platforms. Understand what integrations are supported out-of-the-box and the level of effort required to build custom integrations.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>Supported plugins and integrations with business and security platforms in use by the organization (such as AWS, ticketing, SIEM, incident response, threat intelligence) and the capabilities of these plugins and integrations</li> <li>API support (such as API-first, REST API available, programmatic API available)</li> <li>Whether the platform allows the customer to build custom plugins or integrations</li> <li>Level of effort required and technology (languages, frameworks, and the like) supported when building custom plugins or integrations</li> </ul>
	Reporting, metrics and alerting	<p>EDR platforms have response capabilities, but not all rules trigger a response. Accessing and viewing what these platforms detect and the actions they take is critical to the security of the organization's endpoints. Taking that action can also aid in the identification of rules or configurations that require modification and can also assist in troubleshooting production incidents that may be caused by the EDR platform (false positive detection and response).</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>Support for centralized logging technologies and communication protocols, including integration with any existing or proposed SIEM technology</li> <li>Out-of-the-box reports and dashboards against current program requirements</li> <li>Ability and level of effort required to create custom measures and metrics</li> <li>Alerting mechanisms and ability to create or modify alerts</li> <li>Supported reporting and alerting formats and delivery mechanisms</li> <li>Integration with AWS reporting and alerting tools (such as AWS Security Hub, Amazon CloudWatch Events, Amazon Simple Notification Service [SNS])</li> <li>Support for data aggregation across regions</li> <li>Supported data export formats</li> </ul>
	Response capabilities	<p>Another distinguishing factor when evaluating EDR technologies is what response capabilities are available in the platform. Understand not only what response abilities exist for both human-assisted and automated response but also what expertise is required to set up, configure and maintain these capabilities.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>Out-of-the-box response capabilities and features</li> <li>Technologies and languages supported for automated response</li> <li>Organization's ability to support automation through identified technologies and languages</li> <li>Auditing and tracking of response actions</li> <li>Integration with AWS response capabilities and APIs</li> </ul>

EDR platforms are becoming more popular as organizations strive to protect themselves against emerging threats and want to acquire more active response capabilities. We have also seen, however, that companies utilizing these technologies are still susceptible to security breaches. Implementing an EDR platform requires more than just the licensing and implementation of the technology components. It requires active monitoring, response, reconfiguration and maintenance. Make sure your organization is aware of the true costs of ownership: training requirements, resource requirements, integration requirements and the costs to update policy, standards, processes and procedures. Also, make sure to thoroughly evaluate reporting, monitoring and alerting capabilities, because these are the most likely to require customization or integration work.



## Antivirus/Anti-malware

The advantage of AV solutions is that they are typically mature products that excel at identifying known viruses and malware using signature-based and other techniques. Although attackers can easily evade these detections, positive identification from these tools indicates a real threat, and false positive rates are low when organizations use signature-based detection. Consider mature AV products if EDR technologies are prohibitively expensive, incapable of detecting known threats, difficult to tune or drags on performance. You still need to complete a performance analysis for AV capabilities because the resource requirements will vary based on architecture and supported detection mechanisms.

	Consideration	Details
	Cloud context support	<p>If investigation of AV detections is delayed, the resource(s) affected may no longer exist in your cloud environment. Also, if a virus or worm is spreading throughout your environment, understanding more about the cloud asset can help speed response to the threat.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• The additional cloud context (such as tags or image IDs) that is captured and retained by AV technology to allow correlation of detections with resources and the images and image versions used to create those resources</li> <li>• The special concerns associated with studying resources that have potentially replaced the original resource from which data was gathered</li> </ul>
	Performance and efficiency	<p>Traditional AV agents are not known for being lightweight and are much more likely to store and process data on the cloud resource itself. Consider how this will affect instance sizing and storage requirements.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• The architecture of the tools under consideration</li> <li>• Performance (CPU, memory, storage and bandwidth utilization) when used with production workloads</li> <li>• Amount of data sent and received from management console(s)</li> <li>• Amount of data stored on disk (such as signature database, logs, quarantine)</li> <li>• Support for data compression</li> </ul>
	Deployment	<p>AV software requires agents and may also report data back to a management console. Update servers may also be used to distribute updates to the software and signature database.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• The architecture of the tools under consideration</li> <li>• The installation and configuration procedures for agents and any management infrastructure</li> <li>• The availability of managed or SaaS components or preconfigured appliances from AWS Marketplace</li> <li>• Effectiveness and responsiveness of support</li> <li>• Any vendor requirements for the use of professional services for installation or configuration</li> <li>• Integration with other AWS technologies (such as AWS Systems Manager, AWS Config, Amazon CloudWatch) for deployment or validation of agent deployment</li> </ul>

## Antivirus/Anti-malware (continued)

	Consideration	Details
	Configuration and maintenance	<p>Traditional AV products are not as configurable as EDR platforms, but it is still important to understand and review configurations on a regular basis. Reviews should be required on changes to the default configuration.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• The architecture of the tools under consideration and the upgrade/update procedures</li> <li>• The procedures for updating signatures</li> <li>• Communication protocols and paths to understand required firewall and ACL changes along with any VPC peering or cross-account access</li> <li>• Reporting, metrics or alerting available for any out-of-date agents or signatures</li> <li>• Any vendor requirements for the use of professional services for upgrades or updates (not common)</li> <li>• Ability to customize scan intervals or manage exclusions</li> <li>• Whether the platform allows customers to add their own signatures</li> <li>• Availability and content of secure configuration guides and best practices</li> </ul>
	Detection	<p>Traditional AV technologies focus primarily on known threats. It is important for organizations to evaluate their effectiveness as part of the selection process.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• Detection methods of any known malware samples available, if your organization practices malware analysis and has appropriate analysis environments</li> <li>• Available benchmarks or comparisons by third-party evaluators</li> <li>• Product reviews and customer forums</li> <li>• Customer references</li> <li>• Whether detection is real-time, interval-based, asynchronous or configurable for each detection mechanism supported</li> <li>• Whether detection includes detection of non-file-based malware (memory resident malware, for example)</li> </ul>
	Integration	<p>Traditional AV platforms have historically operated independently of other technologies and systems with the exception perhaps of log aggregation technologies, but it is still important to understand what integrations are supported out-of-the-box and the level of effort required to build any custom integrations.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• Supported plugins and integrations with business and security platforms in use by the organization (such as AWS, ticketing, SIEM, incident response, threat intelligence) and the capabilities of these plugins and integrations</li> <li>• API support (API-first, REST API available, programmatic API available, to name a few)</li> <li>• Whether the platform allows the customer to build custom plugins or integrations</li> <li>• Level of effort required and technology (such as languages or frameworks) supported when building custom plugins or integrations</li> </ul>

## Antivirus/Anti-malware (continued)

	Consideration	Details
	Reporting, metrics and alerting	<p>AV software will detect and attempt to neutralize a high percentage of well-known threats in your environment. Nevertheless, implement adequate reporting, metrics and alerting to respond quickly when you see new threats in your environment, because the extent of the automated response may be limited to killing processes and quarantining malware. Enhance the effectiveness of the technology by supporting defined standards and goals.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• Out-of-the-box reports and dashboards against current program requirements</li> <li>• Ability and level of effort required to create custom measures and metrics</li> <li>• Alerting mechanisms and ability to create or modify alerts</li> <li>• Supported reporting and alerting formats and delivery mechanisms</li> <li>• Integration with AWS reporting and alerting tools (such as AWS Security Hub, Amazon CloudWatch Events, Amazon SNS)</li> <li>• Support for data aggregation across regions</li> <li>• Supported data export formats</li> </ul>

There are many mature options when evaluating AV solutions. However, not all of these vendors have focused on optimizing their technology for the cloud. Take this into consideration when evaluating your current on-premises AV technology against other options for implementation in cloud environments. Performance and reporting may be the biggest considerations when implementing AV in the cloud.

## Host-based Intrusion Detection

HIDS capabilities will be included with EDR solutions and bundled with other EPPs even if they may not advertise themselves as EDR solutions. Consider an EPP or product that focuses on HIDS if 1) EDR is prohibitively expensive or negatively affects performance, and 2) you want to detect indicators of compromise (IoCs). You will still need performance analysis for HIDS capabilities, because the resource requirements will vary based on the detection mechanisms supported and your architecture. HIDS may also offer more visibility into network traffic, depending on product capabilities.

	Consideration	Details
	Cloud context support	<p>If investigation of HIDS detections is delayed, the resource(s) affected may no longer exist in your cloud environment. Understanding more about the cloud asset can help speed response to the threat.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• The additional cloud context (tags or image IDs) that is captured and retained by HIDS technology to allow correlation of detections with resources and the images and image versions used to create those resources</li> <li>• The special concerns associated with studying resources that have potentially replaced the original resource from which data was gathered</li> </ul>
	Performance and efficiency	<p>Because of the move to EDR, traditional HIDS agents may not be optimized for cloud. Consider how this will affect instance sizing and storage requirements.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• The architecture of the tools under consideration</li> <li>• Performance (CPU, memory, storage and bandwidth utilization) when used with production workloads</li> <li>• Amount of data sent and received from management console(s)</li> <li>• Amount of data stored on disk (logs)</li> <li>• Support for data compression</li> </ul>

## Host-based Intrusion Detection (continued)

	Consideration	Details
	Deployment	<p>HIDS software requires agents to identify indicators of compromise and may also report data back to a management console.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• The architecture of the tools under consideration</li> <li>• The installation and initial configuration procedures for agents and any management infrastructure</li> <li>• The availability of managed or SaaS components or preconfigured appliances from AWS Marketplace</li> <li>• Effectiveness and responsiveness of support</li> <li>• Any vendor requirements for the use of professional services for installation or configuration</li> <li>• Integration with other AWS technologies (such as AWS Systems Manager, AWS Config, Amazon CloudWatch) for deployment or validation of agent deployment</li> </ul>
	Configuration and maintenance	<p>HIDS agents and corresponding policies or rules will need to be tuned to eliminate false positives and may require custom rules or policies to monitor specific configurations or logs. They will also require regular maintenance and updates/upgrades.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• The architecture of the tools under consideration</li> <li>• The upgrade procedures</li> <li>• The procedures for updating any datasets leveraged by agents</li> <li>• Reporting, metrics or alerting available for any out-of-date agents or policies</li> <li>• Communication protocols and paths to understand required firewall and ACL changes along with any VPC peering or cross-account access</li> <li>• Any vendor requirements for the use of professional services for upgrades or updates</li> <li>• Accessibility to detection rules, scripts and other configuration details (open or proprietary)</li> <li>• Whether the platform allows customer to build or create their own rules</li> <li>• Level of effort to perform customizations to rules, scripts or configurations or create new rules</li> <li>• Integrations with other AWS technologies (such as AWS Config and AWS Lambda) or configuration management tools (Puppet, Chef, Ansible, SaltStack, CFEngine) to perform updates or upgrades or apply configurations</li> <li>• Secure configuration guides and best practices</li> </ul>
	Detection	<p>HIDS technologies require the implementation of agents on the supported endpoints. They may also require the provisioning and deployment of management consoles and centralized update servers or appliances.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• Detection methods employed</li> <li>• Data and services included for monitoring and detection</li> <li>• Available benchmarks or comparisons by third-party evaluators</li> <li>• Product reviews and customer forums</li> <li>• Customer references</li> </ul>
	Integration	<p>HIDS software may support integration with other reporting and alerting capabilities.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• Supported plugins and integrations with business and security platforms in use by the organization (such as AWS, ticketing, SIEM, incident response, threat intelligence) and the capabilities of these plugins and integrations</li> <li>• API support (such as API-first, REST API available, programmatic API available)</li> <li>• Whether the platform allows the customer to build custom plugins or integrations</li> <li>• Level of effort required and technology (languages and frameworks) supported when building custom plugins or integrations</li> </ul>

## Host-based Intrusion Detection (continued)

	Consideration	Details
	Reporting, metrics and alerting	<p>HIDS technologies focus on detection. For that reason, reporting, alerting, monitoring and response procedures are crucial.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• Out-of-the-box reports and dashboards against current program requirements</li> <li>• Ability and level of effort required to create custom measures and metrics</li> <li>• Alerting mechanisms and ability to create or modify alerts</li> <li>• Supported reporting and alerting formats and delivery mechanisms</li> <li>• Integration with AWS reporting and alerting tools (such as AWS Security Hub, Amazon CloudWatch Events, Amazon SNS)</li> <li>• Resources and processes to support monitoring of reports and response to alerts</li> <li>• Support for data aggregation across regions</li> <li>• Supported data export formats</li> </ul>

HIDS can provide insight into what is happening on your endpoints when more advanced endpoint detection and response is not available. However, if cloud endpoints have short lifecycles, HIDS may not provide as much value unless enough cloud context is available to determine which detections or events are relevant to similar cloud endpoints or the cloud endpoint that replaced the endpoint on which the initial event occurred.

## File Integrity Monitoring

FIM may be included in many of the other EPP solutions, but you may consider it as a point solution if integrity is significantly more important than confidentiality and availability, and if the capabilities of the solutions included in your EPP do not meet your needs. FIM may become less important as organizations move toward more immutable workloads, where most sensitive files reside on read-only portions of the file system and more consistently leverage PaaS for back-end storage technologies (such as Amazon RDS, Amazon S3).

	Consideration	Details
	Reporting, metrics and alerting	<p>File integrity monitoring typically affects performance much less than other endpoint security technologies because it is focused only on the integrity of files. Performance should still be evaluated before using these technologies in the cloud, especially when other security agents are also installed.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• The architecture of the tools under consideration</li> <li>• Performance (including CPU, memory, storage and bandwidth utilization) when used with production workloads</li> <li>• Amount of data sent and received from management console(s)</li> <li>• Amount of data (such as file hash/signature database, logs) stored on disk</li> <li>• Support for data compression</li> </ul>

## File Integrity Monitoring (continued)

	Consideration	Details
	Deployment	<p>FIM software requires agents to identify changes to monitored files and may also report data back to a management console.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• The architecture of the tools under consideration</li> <li>• The installation and initial configuration procedures for agents and any management infrastructure</li> <li>• The availability of managed or SaaS components or preconfigured appliances from AWS Marketplace</li> <li>• Effectiveness and responsiveness of support</li> <li>• Any vendor requirements for the use of professional services for installation or configuration</li> <li>• Integration with other AWS technologies (such as AWS Systems Manager, AWS Config, Amazon CloudWatch) for deployment or validation of agent deployment</li> </ul>
	Configuration and maintenance	<p>Configuration and maintenance of FIM software may be less cumbersome than the other solutions we have discussed, but all solutions require some degree of configuration and maintenance.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• The architecture of the tools under consideration</li> <li>• The upgrade procedures</li> <li>• Reporting, metrics or alerting available for any out-of-date agents</li> <li>• Communication protocols and paths to understand required firewall and ACL changes, along with any VPC peering or cross-account access</li> <li>• Any vendor requirements for the use of professional services for upgrades or updates</li> <li>• Level of effort to configure policy that determines which files to monitor</li> <li>• Integrations with other AWS technologies (such as AWS Config and AWS Lambda) or configuration management tools (Puppet, Chef, Ansible, SaltStack, CFEngine) to perform updates or upgrades or apply configurations</li> <li>• Secure configuration guides and best practices</li> </ul>
	Integration	<p>FIM software may support integration with other reporting and alerting capabilities.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• Supported plugins and integrations with business and security platforms in use by the organization (such as AWS, ticketing, SIEM, incident response, threat intelligence) and the capabilities of these plugins and integrations</li> <li>• API support (including API-first, REST API available, programmatic API available)</li> <li>• Whether the platform allows the customer to build custom plugins or integrations</li> <li>• Level of effort required and technology (languages and frameworks) supported when building custom plugins or integrations</li> </ul>
	Reporting, metrics and alerting	<p>If a monitored file is changed, human intervention is typically required to determine the cause and whether it was an approved change. Adequate reporting and alerts are needed to facilitate this process.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• Out-of-the-box reports and dashboards against current program requirements</li> <li>• Ability and level of effort required to create custom measures and metrics</li> <li>• Alerting mechanisms and ability to create or modify alerts</li> <li>• Supported reporting and alerting formats and delivery mechanisms</li> <li>• Integration with AWS reporting and alerting tools (such as AWS Security Hub, Amazon CloudWatch Events, Amazon SNS)</li> <li>• Resources and processes to support monitoring of reports and response to alerts</li> <li>• Support for data aggregation across regions</li> <li>• Supported data export formats</li> </ul>

FIM is one of the easier technologies to implement for most organizations. Depending on the configuration, however, the number of files being monitored and the amount of change in the organization, the number of resources required to follow up on alerts can be excessive. Continuous tuning and integration with change management can help reduce to a manageable level the number of alerts requiring human interaction.

## Application Whitelisting

Application whitelisting protects endpoints by either ensuring that only known software is allowed to execute or notifying administrators when unapproved software is executed on endpoints. This protection may be accomplished by validating hashes or signatures associated with the software or by validating software-signing certificates against the policies defined by the organization and assigned to each endpoint. Application whitelisting makes the exploitation and installation phases of the attack kill chain much more difficult. Consider application whitelisting if your environment has a high degree of homogeneity or if your organization’s deployment processes are mature and would support automating the development and maintenance of the whitelist policies. Caution: Application whitelisting technologies may not prevent attacks against known vulnerabilities in whitelisted applications, so be sure to follow good vulnerability management practices.

	Consideration	Details
	Performance and efficiency	<p>Application whitelisting solutions generally do not affect performance as much as other endpoint security solutions—as long as they are configured correctly. If they are misconfigured and block legitimate applications or services, the performance impact is significant. Changes to rules and to cloud resources should be thoroughly tested before deployment.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• The architecture of the tools under consideration</li> <li>• Performance (CPU, memory, storage and bandwidth utilization) when used with production workloads</li> <li>• Amount of data sent and received from management console(s)</li> <li>• Support for data compression</li> </ul>
	Deployment	<p>Application whitelisting solutions typically require agents and a management console to update and distribute configurations and receive alerts from agents.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"> <li>• The architecture of the tools under consideration</li> <li>• The installation and configuration procedures for agents and management infrastructure</li> <li>• The availability of managed or SaaS components or preconfigured appliances from AWS Marketplace</li> <li>• Effectiveness and responsiveness of support</li> <li>• Any vendor requirements for the use of professional services for installation or configuration</li> <li>• Integration with other AWS technologies (such as AWS Systems Manager, AWS Config, Amazon CloudWatch) for deployment or validation of agent deployment</li> </ul>

## Application Whitelisting (continued)

	Consideration	Details
	Configuration and maintenance	<p>Configuration and maintenance of whitelisting policies is critical to the successful use of application whitelisting. In enterprise environments, standardization and automation can help reduce this burden. Automated testing can validate changes to the whitelist or cloud resources before release into production environments.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"><li>• The architecture of the tools under consideration</li><li>• The upgrade procedures</li><li>• The procedures for updating whitelists</li><li>• Reporting, metrics or alerting available for any out-of-date agents or policies</li><li>• Communication protocols and paths to understand required firewall and ACL changes along with any VPC peering or cross-account access</li><li>• Any vendor requirements for the use of professional services for upgrades or updates</li><li>• Level of effort to create and maintain whitelists and any assistance provided by technology</li><li>• Integrations with other AWS technologies (such as AWS Config or AWS Lambda) or configuration management tools (Puppet, Chef, Ansible, SaltStack, CFEngine) to perform updates and upgrades or to apply configurations</li><li>• Secure configuration guides and best practices</li></ul>
	Reporting, metrics and alerting	<p>In order to respond quickly to outages caused by whitelists and aid in the identification of attempted exploits and unauthorized installations, evaluate the reporting and alerting features available.</p> <p><b>Evaluate:</b></p> <ul style="list-style-type: none"><li>• Support for centralized logging technologies and communication protocols including integration with any existing or proposed SIEM technology</li><li>• Out-of-the-box reports and dashboards against current program requirements</li><li>• Ability and level of effort required to create custom measures and metrics</li><li>• Alerting mechanisms and ability to create or modify alerts</li><li>• Supported reporting and alerting formats and delivery mechanisms</li><li>• Integration with AWS reporting and alerting tools (such as AWS Security Hub, Amazon CloudWatch Events, Amazon SNS)</li><li>• Support for data aggregation across regions</li><li>• Supported data export formats</li></ul>

Application whitelisting is a mature, layered security control that can be leveraged to reduce the impact of vulnerabilities in cloud environments and make exploitation of cloud resources more difficult. Because standardization is more common in the cloud, application whitelisting may be more achievable and easier to maintain. Heavy use of automation and DevOps principles can also help ease the burden of ongoing configuration and maintenance.

## Making the Choice

To summarize, the key considerations for implementing endpoint security in AWS are:

- Cloud context
- Efficiency
- Ease of use
- Reporting
- Ease of integration
- Effectiveness

### Have a Plan

By defining and understanding their cloud architecture, risk profile, business requirements and available resources along with understanding any gaps, organizations will be in a good position to determine which considerations outlined above are most important to them. Based on those considerations, organizations should develop a proof-of-concept test plan and evaluation matrix. The test plan and matrix should include a ranking of importance for each consideration, and where possible, acceptance thresholds. When the test plan is complete, the organization should identify two or more representative cloud environments in which to conduct the test. They should identify any additional technology they may need to aid in the evaluation of certain considerations. For example, evaluating the performance and efficiency of agents will most likely require additional setup and configuration, and, depending on the platform, performance monitoring tools may be required.

### Consider Partners

As organizations build out their cloud and cloud security strategy and plan, they may want to consider working with partners to accelerate their efforts or fill any gaps in knowledge or resources that are identified. All consulting partners may extend AWS Marketplace third-party solutions directly to customers through Consulting Partner Private Offers (CPPOs). Not every organization will be able to find resources with deep cloud experience and even experienced cloud technologists may only have experience in specific industries or with specific cloud vendors.

### Test and Evaluate

With the plan and any additional requirements in place, the technology should be installed in the test environment, configured and monitored to gather enough data to evaluate each consideration. Every step of the process should be measured. Organizations, if possible, should avoid allowing vendors to install and configure the technology for the proof of concept unless they will be installing and managing the solution after purchase as well. At a minimum, technical resources should be available to observe these processes.

After the proof-of-concept test, organizations should evaluate the results against the test plan and acceptance thresholds. Use the collected and documented results to compare functionality, cost and other factors to determine the best solution(s) to employ.

## Conclusion

Endpoint security for IaaS cloud workloads is an important part of an organization's cloud security strategy. Not only does it provide additional protections for these workloads, but it also provides additional visibility into cloud resources and the actual threats that exist in an organization's cloud environments. While many organizations are still concerned about the performance impacts and associated costs, cloud endpoint security vendors have matured, and cloud-optimized solutions are more accessible.

Fortunately, many of these solutions are offered on-demand, which makes evaluating these products and services much easier than it was in the past. To get started, you may want to review what products are available in AWS Marketplace or through a SaaS model to jump-start your evaluation process.

## About the Author

[David Hazar](#) is a SANS analyst, instructor and co-author of SANS MGT516: Managing Security Vulnerabilities: Enterprise and Cloud. He also is an instructor for SANS SEC540: Cloud Security and DevOps Automation. With close to 20 years of broad, deep technical experience gained from a variety of hands-on roles serving the financial, healthcare and technology industries, his current areas of focus include vulnerability management, application security, cloud security and secure DevOps. He holds the CISSP, GWAPT, GWEB, GMOB, GCIA, GCIH, GCUX, GCWN, GSSP-.NET and GSTRT certifications.

## Sponsor

SANS would like to thank this paper's sponsor:



in conjunction with



### About Optiv

Optiv is a market-leading provider of end-to-end cybersecurity solutions. Optiv helps clients plan, build and run successful cybersecurity programs that achieve business objectives through our depth and breadth of cybersecurity offerings, extensive capabilities and proven expertise in cybersecurity strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology. Optiv maintains premium partnerships with more than 350 of the leading security technology manufacturers.