SANS

Analyst Program

**Whitepaper**

# Cloud-Native Application Protection Platforms (CNAPPs) Buyers Guide

Written by **Dave Shackleford**

March 2023

sysdig

©2023 SANS™ Institute

# Introduction

As the pace of cyberthreats and breaches accelerates, enterprise security teams struggle to manage risks and protect their environments against the evolving tactics and techniques attackers use to target cloud deployments. The cloud now brings a broader footprint of technology and assets into scope for security teams to discover, monitor, and protect. The constant and uncharted way in which workloads and cloud services are provisioned creates an expanding and dynamic attack surface that is hard to secure with tools and processes designed for legacy data centers. Security teams now have dynamic workloads with 10–100 times more containerized compute instances, large volumes of cloud assets with dynamic activity to track, and messy, overly permissive identity and access management (IAM) permissions to manage. Existing tools have not kept up with new tactics used by attackers in the cloud, leading to a weakened security posture. As a result, trying to develop, implement, and maintain a sound approach to cloud security has challenged many teams.

This rapid expansion of the potential attack surface has led to many cloud vulnerabilities, misconfigurations, and security weaknesses. As more resources and sources of data increase, so does the burden of processing data into useful knowledge that can be applied to identifying and remediating threats. Security, operations, and application teams are bombarded and overwhelmed by the number of alerts and vulnerabilities they face, leaving organizations with long exposure windows to critical vulnerabilities. Managing these vulnerabilities requires significant additional context about cloud workloads and application design, too, and it is difficult for teams to prioritize which containers and packages actually present significant risks. This becomes especially critical as more organizations take advantage of DevOps practices common in the cloud (such as continuous integration and continuous deployment or delivery [CI/CD]). Empowered developers are configuring infrastructure at will and deploying containerized applications with the click of a button. These practices can put organizations at risk because security is rarely integrated in the development environment, and many security teams may not have visibility into deployment practices and new vulnerabilities that can arise.

**In the cloud, attack patterns are different, with fewer traditional endpoint-focused attacks and many more attacks focused on the interconnectedness of software-based infrastructure.**

Bad actors are adapting to this new landscape and taking advantage of the growing vulnerabilities and security weaknesses. As more organizations are born in the cloud or move there, the threat landscape has evolved to take advantage of these security gaps. In the cloud, attack patterns are different, with fewer traditional endpoint-focused attacks and many more attacks focused on the interconnectedness of software-based infrastructure, including identity assignment and orientation (both users and non-human, or machine, identities), application packages and libraries, exposed APIs, and more. Additionally, the dark web is a source for stolen credentials and sophisticated

tools and techniques to quickly compromise cloud environments with valid credentials, find and exploit vulnerabilities, and move laterally across workloads and clouds to extract maximum return from any breach. The changes in the attacks, attackers, and overall threat landscape call for new and better approaches to detection and response for cloud workloads, applications, and environments overall.

**The cloud necessitates a significant overhaul of many tools, services, processes, and skills that security operations teams have relied upon for years.**

The cloud necessitates a significant overhaul of many tools, services, processes, and skills that security operations teams have relied upon for years. These need to be updated as the security industry progresses further into PaaS and IaaS cloud deployments, whether entirely native or hybrid in nature.

As shown in Figure 1 and detailed earlier, several factors drive this need to update and change technologies and processes for a cloud security operations team. Security solutions, processes, and the security team skills need to evolve to effectively mitigate risk across cloud and containers.

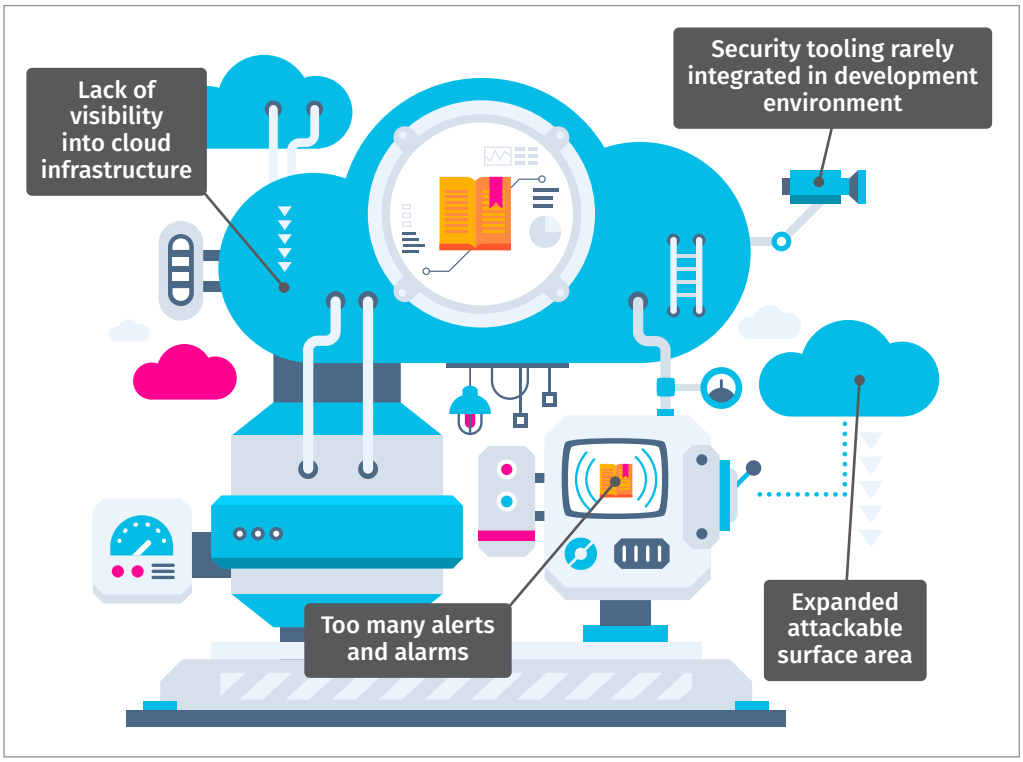


*Figure 1. Factors Driving the Need to Update Technologies in Cloud Environments*

## Why Cloud and Container Security Should Be a Priority

With a wide range of existing security challenges and day-to-day operational requirements across both on-premises and cloud infrastructures, some decision makers may debate the level of urgency to address cloud and container security. There's no question, however, that breach numbers have risen (an estimated 1,802 data breaches in the United States alone in 2022[1]), as has the total cost of breaches (averaging $4.35 million per breach globally, according to IBM[2]).

Previously, the security community observed a steadily increasing savviness about cloud infrastructure and technologies in attacks against the cloud, and many of these focused heavily on misconfiguration "blind spots" in cloud environments that weren't adequately covered by security controls and monitoring. They emphasized new technologies such as containers, Kubernetes, and serverless that many security teams still don't fully understand or protect. Another big concern is "cloud sprawl," which significantly expands the potential attack surface overall. Few organizations feel confident that they know about every account, asset, and service in use across the cloud landscape, and this lack of inventory visibility could prove disastrous.

[1] "Annual number of data compromises and individuals impacted in the United States from 2005 to 2022," www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

[2] "Cost of a Data Breach 2022: A Million-Dollar Race to Detect and Respond," www.ibm.com/reports/data-breach/

In short, today's attackers have realized that focusing on the cloud makes sense because security has often been behind the curve in adapting security operations, detection, and response to cloud workloads. Some recent examples since the start of 2022 include the following:

- Attackers are hiding malware in legitimate-looking images stored in Docker Hub, according to researchers at Sysdig. The most common malware types were related to cryptomining (37%), followed by embedded secrets (17%) such as frequently used SSH keys, AWS credentials, and other authorization tokens.[3]
- The Denonia malware targets AWS Lambda serverless functions and associated services and infrastructure. Coded in Go, Denonia includes cryptomining components and focuses on the exploitation of account credentials.[4]
- Cryptomining botnet LemonDuck exploits misconfigured Docker APIs. This botnet installs malicious containers and terminates competing cryptomining code if detected.[5]
- TeamTNT threat actor(s) allegedly compromised more than 10,000 Docker, Kubernetes, and Redis devices during a cloud-focused campaign called Chimaera, according to researchers with the Sysdig Threat Research Team (TRT). TeamTNT is a sophisticated, cloud-savvy threat actor that leverages obfuscation and masking techniques for network traffic and requests, taps into cloud APIs to access sensitive information such as IAM credentials in AWS EC2 metadata, and uses evasion tactics to avoid early detection in container images.[6]
- In the same report, the Sysdig TRT also found that DDoS and cryptomining attacks involving cloud workloads have increased in tandem with geopolitical conflicts such as the Russia–Ukraine war. A pro-Russian hacktivist group called Killnet has been detected targeting cloud assets of numerous NATO countries with DDoS attacks. Infected container images were frequently noted as a means to rapidly ramp up botnets used in launching them.

What is the impact of not addressing these challenges? In the 2022 SANS Cloud Security Survey, more than half of the respondents indicated their top concerns in the cloud include unauthorized compute instances or components within workloads, poorly configured or accessible APIs (particularly for complex cloud services like Kubernetes), lack of visibility, and an inability to detect and respond to cloud intrusion scenarios.[7] All of these have been proven factors in many of the most notable cloud incidents to date. If cloud and container security isn't addressed, here are a few consequences many organizations are likely to experience:

- Without updating detection and response tools and capabilities to address containers and cloud workloads, most security operations teams will be too slow to detect these threats or will be exposed to critical vulnerabilities in production. Hijacking of APIs, insertion and execution of malicious cryptomining and other malware, and suspicious cloud workload behaviors should be detected as quickly as possible to facilitate rapid response efforts.

---

[3] "Analysis on Docker Hub malicious images: Attacks through public container images," https://sysdig.com/blog/analysis-of-supply-chain-attacks-through-public-docker-images/

[4] "Denonia: First Malware Targeting AWS Lambda," www.securityweek.com/denonia-first-malware-targeting-aws-lambda

[5] "LemonDuck Cryptomining Botnet Hunting for Misconfigured Docker APIs," www.hackread.com/lemonduck-cryptomining-botnet-misconfigured-docker-apis/

[6] "2022 Sysdig Cloud-Native Threat Report," https://dig.sysdig.com/c/pf-2022-cloud-native-threat-report?x=u_WFRi#page=1 (Registration required)

[7] "SANS 2022 Cloud Security Survey," March 2022, www.sans.org/white-papers/sans-2022-cloud-security-survey/

- The pace of change and updates to cloud workload components and assets like container images has accelerated. As vulnerabilities are announced, it's critical that vulnerability management programs are updated to keep up with new packages, operating systems, and other cloud-native services. Without real-time visibility into what workloads and components are in use and planned for use, security teams will be unable to prioritize fixes and will likely spend significant time triaging vulnerabilities (which can slow down testing and deployment processes).
- Many incident response teams have not prepared and updated their tools and workflows to properly address cloud workloads. This oversight can result in excessive time collecting and analyzing event data and other artifacts, which in turn leads to longer response time and decision making on appropriate response actions (containing attacks, remediating root cause, and validating compliance violations).

All cloud and container security trends inevitably include APIs and orchestration services and tools (Kubernetes likely being the best known). These are prime vectors for misconfiguration, exposure, and overallocation of privileges (and thus top targets for attacks), so the security community is seeing more emphasis on threat intelligence, vulnerability analysis and alerting, and remediation guidance for these in particular.

## Traditional Security Controls and Tools Are Insufficient

Many traditional tools and controls used on-premises don't work well in the cloud. Unfortunately, some organizations don't even see the need to reevaluate their security controls stack in light of cloud-based infrastructure and deployment practices. Doing nothing about cloud and container security is certainly always an option, but it invariably results in a security strategy and technology capability that fall farther and farther behind over time.

Several dominant themes explain why many traditional security technologies aren't best suited to cloud workloads and environments, all of them intimately tied to the trifecta of prevention, detection, and response. One is visibility. Visibility into cloud services, identities, workloads, and orchestration services such as Kubernetes helps security teams detect modern threats. Most traditional tools can create blind spots in these areas. The first of the Center for Internet Security (CIS) Critical Security Controls is entirely focused on shoring up this lack of visibility by maintaining a sound inventory of systems operating within the environment. The security concept "You can't secure what you don't know about" holds true in any environment, and this control has been the highest priority control since the list's inception.

The second CIS Critical Security Control focuses on gathering and maintaining an inventory of software running on workloads. Although this inventory serves as a sound starting point for any conversation about visibility and tracking assets in a cloud environment, there's much more to do. Most organizations rely on many types of controls for security visibility in the cloud. What follows is a partial list of them.

- **Network visibility—**The types of traditional controls often used to achieve network visibility include network firewalls, network intrusion detection and prevention, and network detection and response (NDR). With software-based network configuration and controls tied to workloads and deployments, many of these tools may not be suitably integrated to facilitate understanding of a Kubernetes-based network configuration, for example, or the specific traffic targeting or originating from a container running in leading IaaS and PaaS environments.
- **Application visibility—**Application visibility relies on tracking events and behaviors at scale as workloads communicate within the cloud environment as a whole in addition to the local application logs on individual systems and containers. Developing true application visibility requires deep integration with cloud workloads and orchestration services with robust alerting and reporting.
- **Workload visibility—**Deep workload visibility will require vulnerability monitoring and intelligence, configuration assessment capabilities for a variety of workload types, and visibility into container image configuration and runtime event monitoring.
- **Pipeline and infrastructure as code (IaC) visibility—**Another critical aspect of cloud and container security visibility is the posture of workload definitions and configuration options, as well as any related services and supporting elements needed for successful deployment and operation (orchestration and IAM, for example). In most mature organizations, this type of visibility will require integration into DevOps pipelines, with build integration and rapid analysis of IaC templates and files.

Most traditional tools used for vulnerability inspection and threat surface analysis, as well as operating system and application component evaluation and monitoring in real time, are not well-suited to cloud-based workloads and services. Many rely on network scanning, which is minimally effective in a dynamic, ephemeral environment like the cloud, or on agents that affect performance and increase costs. Many traditional tools also send many discrete alerts and signals but lack context (who, what, when, where, why) for fast response in cloud-based applications and workloads.

The second prevalent reason many traditional on-premises tools don't work well in the cloud can be summed up with a question that any security professional should recognize:

*"What are we looking for and what do we do about it?"*

Many security operations center (SOC) and incident response teams have built playbooks for several attack models and variants that incorporate endpoint detection and response (EDR), network visibility, alerts, and events feeding back to a central monitoring team, and more. Conceptually, some of these same attacks may occur in the cloud, but the modality of the attacks and how they're detected will need to shift. For example, an attacker may execute a malicious command via the AWS CLI that modifies a cloud storage node such as an S3 bucket or interacts with cloud-native Kubernetes services. No traditional EDR or on-premises monitoring solution would detect this in real time and alert on it (or block it entirely) because these services and capabilities don't exist there. The team at MITRE has worked to evolve its ATT&CK models to better incorporate IaaS and PaaS solutions in leading cloud service providers, and tooling for detection and response should be equipped to detect and respond to new and modified attack elements such as the following:[8]

- Modification and implantation of cloud container images
- Deployment of unauthorized assets such as new Kubernetes clusters and pods compromised with unauthorized cryptomining code
- Manipulation of roles and identity assignments within workloads

For comprehensive coverage of both PaaS and IaaS environments with real-time visibility, artifact identification and forensic evidence collection, and cloud-native response actions that likely require deep integration with cloud provider APIs, both agent-based and agentless cloud-centric security tooling will be needed. For more insight into real-world use cases, the SANS whitepaper, "A Comprehensive Approach to Cloud Threat Detection and Response" may prove valuable.[9]

Lastly, the dynamic nature of development and deployment, along with the more ephemeral nature of containers and cloud-native workloads and applications, is leading to a more rapidly changing environment. New solutions are needed to keep pace with this explosion of cloud services. In addition, with the desire to embed security controls earlier in the development pipeline (the "shift left" philosophy), we'll need controls that can adapt to modern cloud-enabled technology stacks and don't slow down development efforts.

*Ultimately, point products don't work.* Often organizations consider multiple point solutions or even choose vendors that stitch together a workflow from multiple acquisitions. Regardless of the approach, these tools don't communicate with each other and share context. Teams are stuck wading through disparate vulnerability findings, posture violations, or threats, forcing them to deal with issues as one-offs vs. addressing them as a priority stacked-rank list based on risk and impact.

---

[8] "Cloud Matrix," MITRE, https://attack.mitre.org/matrices/enterprise/cloud/

[9] "A Comprehensive Approach to Cloud Threat Detection and Response," June 28, 2022, www.sans.org/white-papers/comprehensive-approach-cloud-threat-detection-response/ (Registration required)

# What to Look for in a Solution

Security operations and cloud engineering teams need comprehensive visibility into workloads, cloud activity, and user behaviors in real time. The number of signals that the security team has to quickly make sense of is exploding, due to the rapid adoption of containers/Kubernetes and cloud services. The unmanageable volume of both high- and low-fidelity signals ultimately begs the question: How do I focus on the most critical risks in my cloud-native infrastructure?

This is where having deep knowledge of what's running *right now* can help you shrink the list of things that need attention first. Simply put, knowledge of what's running (or simply what's in use) is the necessary context needed by security and DevOps teams to take action on the most critical risks first. Ultimately, this context can be fed back early in the development lifecycle to make "shift-left" better with actionable prioritization.

Ideally, teams will be able to unify these capabilities and goals in a single framework and platform, providing a unified view of all application and workload deployments. For organizations seeking a capable, comprehensive, cloud-native application protection platform (sometimes referred to as a CNAPP solution), several important capabilities and attributes should ideally be in place. Although a comprehensive checklist of features to look for in a CNAPP solution is offered in the Appendix to this paper, this section takes an in-depth look at a few of them.

## User Experience

The first categorical area to evaluate with these solutions is the user experience. Many solutions today are not intuitive and may be difficult to work with. Adding operational burden or clumsy interfaces into the mix for security teams is less than ideal, to be sure. A mature solution should offer the following in the realm of user experience:

- Unified security and risk dashboards that also encompass both cloud workloads and Kubernetes-orchestrated services and workloads (in the cloud or on-premises, ideally). These dashboards should present themes and event information that include threat detection, vulnerability management, and security posture management for all facets of the workload infrastructure.
- Deployment simplicity is also a major consideration, and agentless cloud workload onboarding is rapidly becoming the standard for enterprise platforms in this space.
- Although not absolutely necessary, aggregated security findings and remediation suggestions/solutions can simplify investigations and operational changes for security operations and cloud engineering teams.

## Cloud Workload Protection

One of the core areas where cloud-centric security solutions need to shine is workload protection. Mature solutions should include the following capabilities:

- A unified asset inventory that includes Kubernetes and cloud resources
- Vulnerability scanning for all container images at runtime and registries, container hosts, and virtual machine instances
- Flexible vulnerability reporting, along with runtime in-use exposure filtering for any vulnerabilities; vulnerabilities and/or policy violations can be added to an "accept" or "exceptions" group to minimize alert fatigue
- Easy integration into CI/CD pipelines to help automate vulnerability scanning and reporting
- Integration of external vulnerability feeds, with a unified vulnerability inventory that can validate and help prioritize vulnerabilities across both cloud workloads and any Kubernetes-based workloads
- Workload image configuration rules enforceable in policies and simple-to-implement base image remediation
- Simple and flexible policy creation for configuration settings and vulnerability remediation across all resources, with both runtime remediation and IaC remediation capabilities
- Support for serverless workload protection, but this hinges on whether serverless (functions-as-a-service, or FaaS) workloads are present
- Real-time detection of malicious activity on workloads, with continuously updated rules and integrated threat feeds (as desired/needed)
- Strong investigation and forensics capabilities such as evidence capture, automated investigation/forensics actions, and secure shell access into compromised workloads for analysts
- Machine learning to augment and enhance detection capabilities
- Vulnerability management
- Configuration management
- Runtime security/incident response

## Cloud Security Posture Management

Many significant security incidents occur due to poor hygiene in cloud workload and service configuration management. Ensuring that cloud infrastructure is properly locked down and maintained is critical, and a cloud-native application protection platform should include the following features:

- Policy-as-code support for custom policies (ideally supporting standards such as Open Policy Agent [OPA]), and a sound library of out-of-the-box policies that align with industry frameworks and compliance/regulatory requirements to detect and configure settings in any cloud. Policies should be consistently analyzed and enforced in IaC and runtime environments.
- Detection of configuration drift when it occurs across all types of cloud workloads and orchestration services
- Identity and access management analysis capabilities that evaluate permission usage and suggest least permissive identity and access policies
- Identification and analysis of user attributes and settings that indicate risky configurations such as lacking multifactor authentication (MFA), exposed or overly permissive cloud access keys, lack of access key rotation, and so forth
- Detailed and flexible reporting on all policies and configuration states within cloud environments, preferably with both industry framework and out-of-the-box compliance reports and customization options
- Vulnerability management
- Configuration management
- Permissions/entitlement management

## Cloud Detection and Response

Along with workload protection and posture assessment, cloud detection and response has rapidly surged to the forefront of priorities when it comes to evaluating cloud-native application protection platforms. As mentioned earlier, many enterprise security teams struggle with adapting on-premises tools and workflows for detection, investigations, forensics, and more into cloud-native scenarios. Platforms should support the following:

- Real-time detection of malicious activity and cloud behaviors, with continuously updated rules and integrated threat feeds (as desired/needed)
- A flexible rule language for custom rules, along with a catalog of out-of-the-box detection rules from the provider
- Machine learning to augment and enhance detection capabilities
- Unified detection across cloud, containers, and Kubernetes, and support for multiple cloud provider environments and services

- Strong investigation and forensics capabilities such as evidence capture, automated investigation/forensics actions, and secure shell access into compromised workloads for analysts
- Event enrichment and forwarding to third-party security tools and platforms (such as SIEM)
- Detection and analysis of Kubernetes network events
- Detection and response capabilities for hosts, managed container services (e.g., AWS Fargate), and serverless workloads if these platforms are in use
- Agentless scanning and threat detection

### Enterprise-grade Platform

Lastly, any best-in-class cloud-native application protection platform should be enterprise grade and capable of protecting large, complex cloud deployments in numerous provider environments. Key things to look for include:

- Minimal reliance on the GUI, with strong support for CLI and APIs to facilitate automation and integration across tools, services, and environments
- Strong, flexible support for role-based access control (RBAC) and single sign-on (SSO) federation capabilities
- Scalability across extremely large environments with thousands of nodes and millions of resources
- Logging and auditing capabilities for the platform itself

## Wrapping Up: Benefits of Cloud-Native Application Protection

There is a wide variety of technical and security-focused benefits to choosing and implementing a cloud-native application protection platform. Some of the most important include:

- Gaining deep visibility across both traditional and cloud-based workload environments through virtual machine and instance events and behaviors, as well as those within cloud workloads such as containers. Cloud event data is also ingested to provide context.
- Improvements in the most important security operations metrics such as mean time to detect (MTTD) and mean time to respond (MTTR). Leading solutions can help to detect threats in real time (seconds) and also improve detection rates with fewer false positives. With automated rules and policies for performing forensics and investigations, along with added context about events and behaviors, response times can be significantly reduced, as well.

- Rapidly detecting and remediating vulnerabilities in workload host platforms and containers with deep integration into CI/CD pipelines and runtime environments alike. This feature can help to accelerate and streamline vulnerability management practices. Leading solutions can also generate IaC remediation code in common formats such as AWS CloudFormation, Terraform, or Kubernetes YAML.
- Integration and automation with CLI and API-based access to cloud services and other security tools and platforms

In addition to these technical benefits, there are definitive business-oriented benefits that can provide enormous value to organizations quickly and over the long term. Organizations can safely and securely accelerate their pace of innovation into cloud-based infrastructure, knowing that they have tools and controls in place that were designed for these types of workloads and services. At the same time, overall security posture will improve and risk will be reduced, which is important to internal stakeholders, regulators, investors, and customers. With the rapid increase in notable cloud attacks and breaches, there's widespread (and valid) concern that due care be taken to ensure cloud deployments are as secure as possible. Cloud workload protection can help to boost operational capacity and productivity by automating many sometimes-cumbersome security processes and requirements, as well as more operational needs such as repairing and remediating issues on the fly. In many cases, these tools can even help to reduce operational and capital expenses, as well—unification of controls and capabilities across numerous cloud and workload types can dramatically improve efficiency for a variety of teams.

As you're looking to select a capable, mature platform to help your organization protect workloads in the cloud, minimize vulnerability exposure and configuration weaknesses, and automate security processes and controls, be sure to keep these key themes and capabilities in mind.

# Appendix: Shopping Checklist

## 1.1 User Experience

A robust, mature user experience is critical for any solution that will be in daily use by security operations teams and others. The cloud-native application protection platform should offer:

| | Required | Desired |
|---|---|---|
| Unified security and risk dashboards across cloud, containers, and Kubernetes | X | |
| Agentless cloud onboarding | X | |
| Prioritized list of security findings aggregated based on root cause | | X |
| Remediation guidance and methods (e.g., open a pull request on the IaC source, automated actions to kill/stop containers, etc.) | | X |
| Fully configurable policy engine | X | |
| Other tool/process/platform integrations | | X |

## 1.2 Cloud Workload Protection

The cloud-native application protection platform should be capable of protecting cloud workloads across the lifecycle with the following capabilities:

| Vulnerability Management | Required | Desired |
|---|---|---|
| Container image vulnerability scanning at runtime | X | |
| Host vulnerability scanning (VMs) | X | |
| Image registry vulnerability scanning | X | |
| CI/CD integration for vulnerability management and IaC security | X | |
| Software bill of materials (SBOM) creation | X | |
| Vulnerability definition and validation of policies across cloud and Kubernetes | X | |
| Policy enforcement via admission controller | X | |
| Unified vulnerability inventory | X | |
| Integrated external vulnerability feeds | X | |
| Vulnerability prioritization based on actual package usage by workloads | X | |
| Support for image configuration rules in policies | X | |
| Vulnerability reporting | X | |
| Image layer analysis | X | |

| Configuration Management (Containers/Kubernetes) | Required | Desired |
|---|---|---|
| Misconfiguration detection across Kubernetes, containers, and hosts | X | |
| CIS benchmarks (Kubernetes, Docker, Linux) | X | |
| Unified asset inventory that includes Kubernetes and cloud resources | X | |
| IaC security for Kubernetes (scanning for misconfigurations in IaC manifest) | X | |
| Policy and/or risk violation acceptance | X | |
| Policy violation remediation at source (IaC) or on the runtime environment | X | |

| Runtime Security/Incident Response | Required | Desired |
|---|---|---|
| Real-time detection of malicious activity | X | |
| Continuously updated OOTB rule coverage | X | |
| Integrated threat feed | X | |
| Flexible rule language to support custom detections | X | |
| Multilayered protection with machine learning capabilities as complement to rules-based detection | | X |
| Detection and prevention of container drift | X | |
| Deep visibility into and forensics of security events | X | |
| Detailed and actionable forensics data capture | X | |
| On-demand shell access into compromised workload | X | |
| Support for Linux hosts | | X |
| Agentless scanning and/or threat detection | | X |
| Runtime policies with automated actions (kill, stop, pause a container) | X | |
| SIEM integrations | X | |
| Incident response system integrations (e.g., PagerDuty, Slack) | X | |
| Real-time file integrity monitoring | X | |
| Cloud, Kubernetes, and host activity correlation (e.g., trace a kube exec session down to process/file/network activity) | | X |

| Other | Required | Desired |
|---|---|---|
| Kubernetes network security analysis | X | |
| Serverless support | | X |

## 1.3 Cloud Security Posture Management

Continuous monitoring, detection, and remediation of cloud security misconfiguration is an important set of capabilities for any mature cloud workload and cloud-native application protection platform. The solution should offer:

| Cloud Vulnerability Management | Required | Desired |
|---|---|---|
| Vulnerability scanning for cloud hosts (e.g., EC2 instances) | X | |
| Vulnerability prioritization | X | |
| Jira/ticketing integration | X | |

| Configuration Management | Required | Desired |
|---|---|---|
| Misconfiguration detections across multiple cloud providers | X | |
| Misconfiguration scanning in IaC manifests (IaC security) | X | |
| Configuration drift detection (from IaC to running resources) | X | |
| Remediation at the source (with an automated pull request) | | X |
| Policy-as-code support for custom policies (preferably OPA-based) | X | |
| Policy violation remediation at source (IaC) or on the run-time environment | X | |
| OOTB policies for industry benchmarks and regulatory compliance frameworks | X | |
| Unified asset inventory that includes Kubernetes and cloud resources | X | |
| Compliance reporting | X | |
| Policy and/or risk violation acceptance | X | |
| Attack path analysis | X | |
| MITRE risk mapping | X | |

| Permissions/Entitlements Management | Required | Desired |
|---|---|---|
| Identification of risky user attributes such as no MFA, access keys not rotated, etc. | X | |
| Permission usage evaluation (and suggest least permissive identity and access policies) | X | |
| Least privilege access policies (CIEM) based on runtime access patterns | X | |

## 1.4 Cloud Detection and Response

Detection and response capabilities related to intrusions and cloud-centric attacks are important features. The cloud-native application protection platform should offer:

| | Required | Desired |
|---|---|---|
| Real-time detection of malicious activity | X | |
| Managed policies that are continuously updated | X | |
| OOTB policies for security and compliance frameworks (e.g., MITRE, SOC2, PCI, etc.) | X | |
| Integrated threat intelligence feed (e.g., malicious IPs) | X | |
| Flexible rule language to support custom detections | X | |
| Multilayered protection with machine learning capabilities, complementing rules-based detection | | X |
| Workload, identity, and cloud service detections | X | |
| SaaS app detections (e.g., Okta logs, Microsoft Office 365, Github, etc.) | | X |
| Real-time stream detection of anomalous cloud activities | X | |
| Deep visibility into and forensics of security events | X | |
| Detailed and actionable forensics data capture | X | |
| On-demand shell access into compromised workload | X | |
| Automatic tuning of policies and rules to minimize false positives | X | |
| Forwarding of security events to third-party security and operations tools | X | |
| Event enrichment from cloud and other environmental contexts | X | |
| Support for Linux hosts | | X |
| Serverless support | | X |
| Agentless scanning and/or threat detection | | X |
| Support for all major cloud, Linux, and Kubernetes vendors | | X |

### 1.5 Enterprise-Grade Platform

Mature solutions often have enhancements and additional features that integrate and align with API use; scripting and automation functionality; support for identity and access management capabilities such as federation and privilege assignment, auditing, and logging; and support for large-scale deployments. The cloud-native application protection platform may offer:

| | Required | Desired |
|---|---|---|
| API/CLI first platform | | X |
| Single sign-on (SSO) with SAML support | | X |
| Support for role-based access control (RBAC) | | X |
| Support for hyper-scale environments—more than 100,000 nodes/100 million resources | | X |
| Platform audit | X | |
| eBPF-powered runtime security | X | |
| Agentless cloud security | X | |
| Alerting/notifications integrations | X | |
| Event forwarding into various SIEM platforms | X | |

## Sponsor

**SANS would like to thank this paper's sponsor:**