



E-BOOK

Cloud Security 101: Financial Services

A Primer on CSPM, CDR, CWPP, and CNAPP for
Security Practitioners in Financial Services



Table of Contents

03	Chapter 01 Securing Customers' Money in a Cloud-First World	15	Chapter 05 Shared Responsibility Model for the Cloud
04	Chapter 02 Traditional Security Tools Are Not Effective in the Cloud	16	Chapter 06 Unified Container and Cloud Security With Sysdig
05	Chapter 03 Key Cloud Security Solution Categories: CSPM, CDR, CWPP, and CNAPP		
12	Chapter 04 Five Key Considerations When Evaluating a Cloud Security Solution		



CHAPTER 01

Securing Customers' Money in a Cloud-First World

Life was simpler when financial service providers' IT environments were restricted to on-premises data centers: self-contained fortresses with one way in and one way out. But these days, with more and more financial organizations moving applications and data to the cloud — and cybercriminals already hard at work there — detecting threats is less like defending an ancient fortress and more like securing Disneyland. Like an amusement park, distributed infrastructure based on cloud technologies consists of many attractions, multiple types of consumers, countless interactions, and varying entrances and exits. But there's nothing fun about it for security teams, DevOps, and cloud operations teams. In fact, with so many temptations for bad actors and so much at stake, it's an environment that demands highly intelligent security technologies and constant vigilance.

For financial services organizations, the stakes are especially high. Customers expect the highest standards of security and privacy when it comes to their money, and regulators have their backs. Keeping pace with compliance requirements is a huge and ongoing challenge for security teams, who are already under pressure to do more with less and minimize delays to product rollout in a fiercely competitive market. The spectrum of threat actors exists nonetheless, and any organization's systems are likely to be targeted irrespective of company size or vertical. It's imperative to be vigilant to keep watch for insecure configurations lurking deep within a cloud stack and new threats that emerge to exploit vulnerabilities. So, is cloud security possible or is it pie in the sky?

Traditional Security Tools Are Not Effective in the Cloud

The first, most important thing to understand about cloud security is that traditional security tools, like endpoint detection and response (EDR), cannot keep you safe in the cloud. No matter how effective these tools may have been in an on-premises environment, they can't provide the coverage, speed, or context necessary for cloud security.

When traditional EDR solutions are deployed in the cloud as a “good enough” tool, analysts are impacted with a flood of disparate detections to investigate. These detections are limited in scope and lack full visibility or context into a threat, which massively increases the time it takes for an analyst to respond to the threat, increasing the likelihood of a major security incident.

For many modern threats, EDR tools may completely miss initial access and privilege escalation. These tools will generally pick up on lateral movement, but by then, a security incident has already occurred. This leaves analysts unable to effectively respond to threats. The only thing analysts can do at that point is comb back through their EDR logs, searching for breadcrumbs of information to try and get any sense of what happened.

Essentially, traditional EDR tools were developed to secure Windows endpoints, and are fundamentally not designed or suited for the challenges of cloud security.

Key Cloud Security Solution Categories: CSPM, CDR, CWPP, and CNAPP

Are your teams up to speed about security in the cloud? If not, you aren't alone. According to Gartner®, "50% of the participating organizations indicated that there is a lack of internal knowledge about security in cloud-native DevSecOps."^[1] And this is happening as new terms, categories, and technologies are surfacing daily. But regardless of how many new buzzwords come along, there are three well-established cloud security categories to be aware of: CSPM, CDR, and CWPP.

What is CSPM?

CSPM is a set of controls that detect when your deployed accounts and resources deviate from security best practices. The different standards that are part of the CSPM controls allow you to continuously evaluate all of your cloud accounts and workloads to quickly identify areas of cloud drift and platform misconfigurations. It provides actionable and prescriptive guidance on how to improve and maintain your organization's security posture.

Cloud Security Posture Management (CSPM) tools unify the security use cases of protecting the cloud control plane (by enabling monitoring for misconfigurations), tracking cloud resources, and verifying the configurations of the cloud tenant. These tools enhance cloud security by identifying insecure configurations, which enables organizations to address gaps and design a more secure architecture. Some CSPM solutions also offer remediation and other extended capabilities, though most organizations use CSPMs for compliance purposes and auditing only.

“Through 2025, more than **99% of cloud breaches** will have a root cause of preventable misconfigurations or mistakes by end users.” ^[2]

CSPM tools ensure that cloud settings align with best practices. This enables cloud teams to map out-of-the-box frameworks controls and benchmarks, and save time when addressing things like:

- Data storage exposed directly to the internet
- Lack of encryption on databases
- Lack of multi-factor authentication enabled on critical system accounts

By notifying teams when violations occur, CSPM tools enable teams to take action and prioritize remediation.

1 Gartner, "Emerging Technologies: Future of Cloud-Native Security Operations," Mark Wah, Charlie Winckless, 17 November 2021.

2 Gartner, "Hype Cycle™ for Cloud Security, 2021," Tom Croll, Jay Heiser, 27 July 2021

Figure 1

Key cloud security capabilities consolidated into a unified platform



What is CDR?

As was discussed above, in the dynamic environment of the cloud, traditional detection and response techniques cannot keep up. Security teams end up being too fragmented across diverse roles and responsibilities to effectively cooperate and keep up with the pace of cloud security risks, which also slows down DevOps teams.

As financial services organizations continue to migrate their workloads to the cloud, there is also a growing need to collect, process, monitor, and act upon information from an assortment of cloud security telemetry sources. This presents unique visibility challenges for security, making it difficult to monitor your high-value cloud assets.

To solve these problems, the market is starting to mature and coalesce around unifying cloud security technologies that bring together visibility across cloud infrastructure, containers, hosts, and identities. However, these controls struggle to operate at the speed and scale of cloud-native applications and don't cater to the developer needs.

Enter **cloud detection and response (CDR)**, which refers to the set of practices and technologies aimed at identifying and mitigating security threats within cloud environments. These tools are designed to monitor cloud infrastructure, detect potential security incidents or threats, and respond effectively to mitigate risks.

To stay ahead of attackers and counter modern-day threats, security teams must automate many of their CDR activities such as data enrichment, alert correlation, and incident response. CDR tools should also automate manual tasks, integrate with application security and DevSecOps practices, offer Git-based remediation features, and provide context for alerts and threat prioritization. Gartner projects that SecOps will adopt preventative capabilities like these to secure development and deployment strategies and ensure runtime protection.

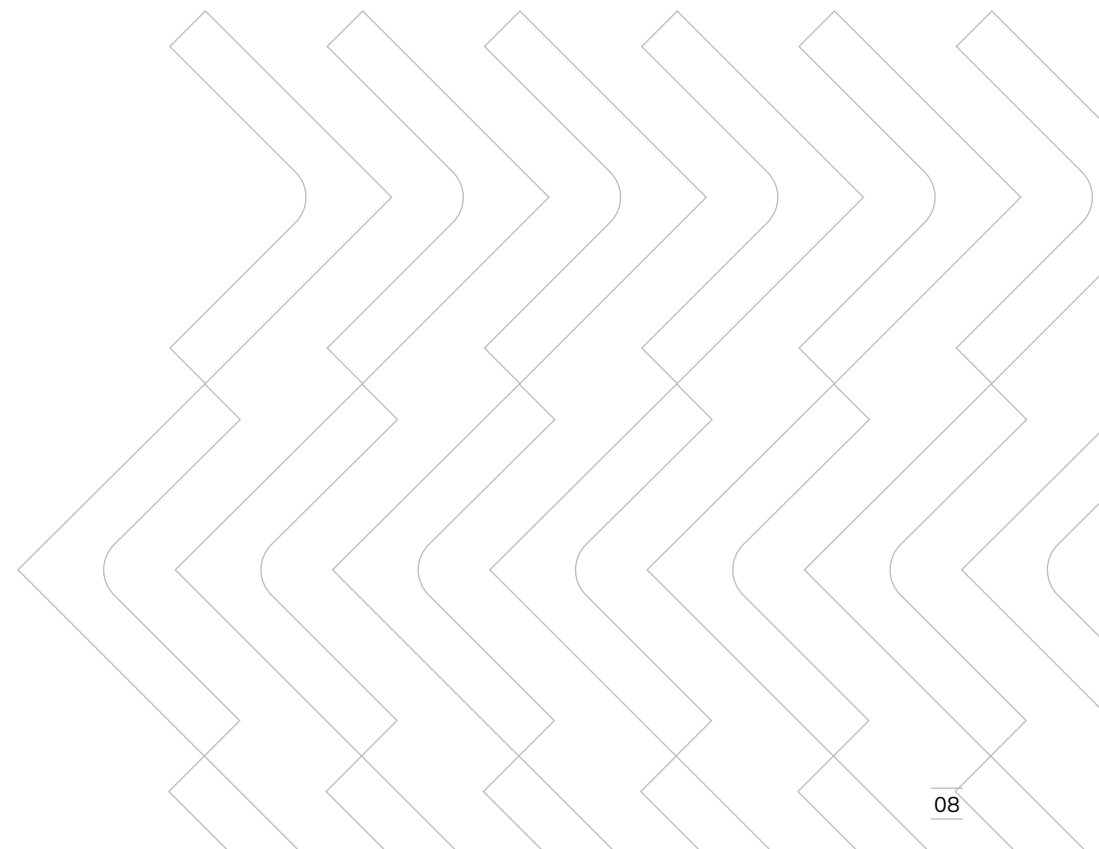
Key components of cloud detection and response may include:

- **Monitoring and visibility:** Cloud resources are ephemeral in nature and must be monitored throughout their lifetime. This involves analyzing logs, events, and other data generated by cloud services.
- **Threat detection:** CDR solutions should identify and detect potential security threats, such as unauthorized access, data breaches, malware, or suspicious activities within a cloud environment.
- **Incident response:** CDR tools must promptly contain an incident once detected, identify the root cause, and reduce attack surface to prevent further damage.
- **Automation:** Response actions must be streamlined to reduce the time to detect (TTD) and time to respond (TTR). Organizations should leverage automation to implement security policies and enforce compliance.
- **Forensics and analysis:** Security teams often need to conduct thorough analysis and forensic investigations to understand threat actor behavior. This helps to assess risk coverage and gather the information needed to prevent future security events.
- **Integration with security tools:** CDR solutions should seamlessly integrate with other security tools to ensure comprehensive visibility across a cloud ecosystem.
- **Compliance monitoring:** CDR tools should ensure that security policies and processes adhere to regulatory standards and industry requirements.

What is CWPP?

Cloud Workload Protection Platform (CWPP) tools protect workloads. Specifically, they focus on securing the whole application lifecycle, providing cloud-based security solutions that protect instances on AWS, Google Cloud Platform (GCP), Microsoft Azure, and other cloud vendors' platforms. CWPP solutions are built for specific use cases:

- **Runtime detection:** Detect suspicious behavior of applications at runtime. Automate response for threats.
- **System hardening:** Prevent security risk by eliminating potential attack vectors and condensing the system's attack surface.
- **Vulnerability management:** Detect OS and non-OS vulnerabilities of known exploitations and ensure it stays compliant with any regulatory requirements.
- **Network security:** Visualize network traffic inside containers and Kubernetes, and enforce Kubernetes-native network segmentation.
- **Compliance:** Ensure production workloads comply with regulatory standards.
- **Incident Response:** Respond to security incidents using valuable evidence from forensics to help you contain the breach.



CNAPP: Not Just Another Acronym

As the cloud-native application space evolves, more moving parts are inevitably introduced. Thankfully, the industry is using a modular approach with cloud-native technologies. As such, existing CI/CD pipelines and runtime platforms can be extended and updated as better methods are discovered.

The downside of all this modularity is complexity. It can be daunting to figure out what to introduce in the application lifecycle in order to get a reasonable level of security policy and enforcement in place. And that's where a **Cloud-Native Application Protection Platform (CNAPP)** comes into play. Leveraging a CNAPP gives you in-depth, multi-layered, agent-based, and agentless coverage across all aspects of your environment – everything from proactive validation of workloads to auditing policies on the public cloud platform you're running on.

What is CNAPP?

CNAPP is the umbrella security category that covers the use cases that would otherwise fall into the CSPM and CWPP categories. According to Gartner,

“Cloud-native application protection platform (CNAPP) provides more than CWPP-CSPM convergence: There are two important drivers for CNAPP. Firstly, CWPP vendors are looking to posture to provide workload context. Secondly, CSPMs are challenged to provide more and more visibility while “drilling down” into the workload. CNAPP integrates CSPM and CWPP to offer both, and potentially augments them with additional cloud security capabilities.”^[3]

One side benefit of a CNAPP is that it allows customers and vendors to readily see the value that cloud security suites can deliver, as opposed to a series of point solutions that need to be painstakingly integrated.

A CNAPP encapsulates four core capabilities from development to production and back to development. These are:

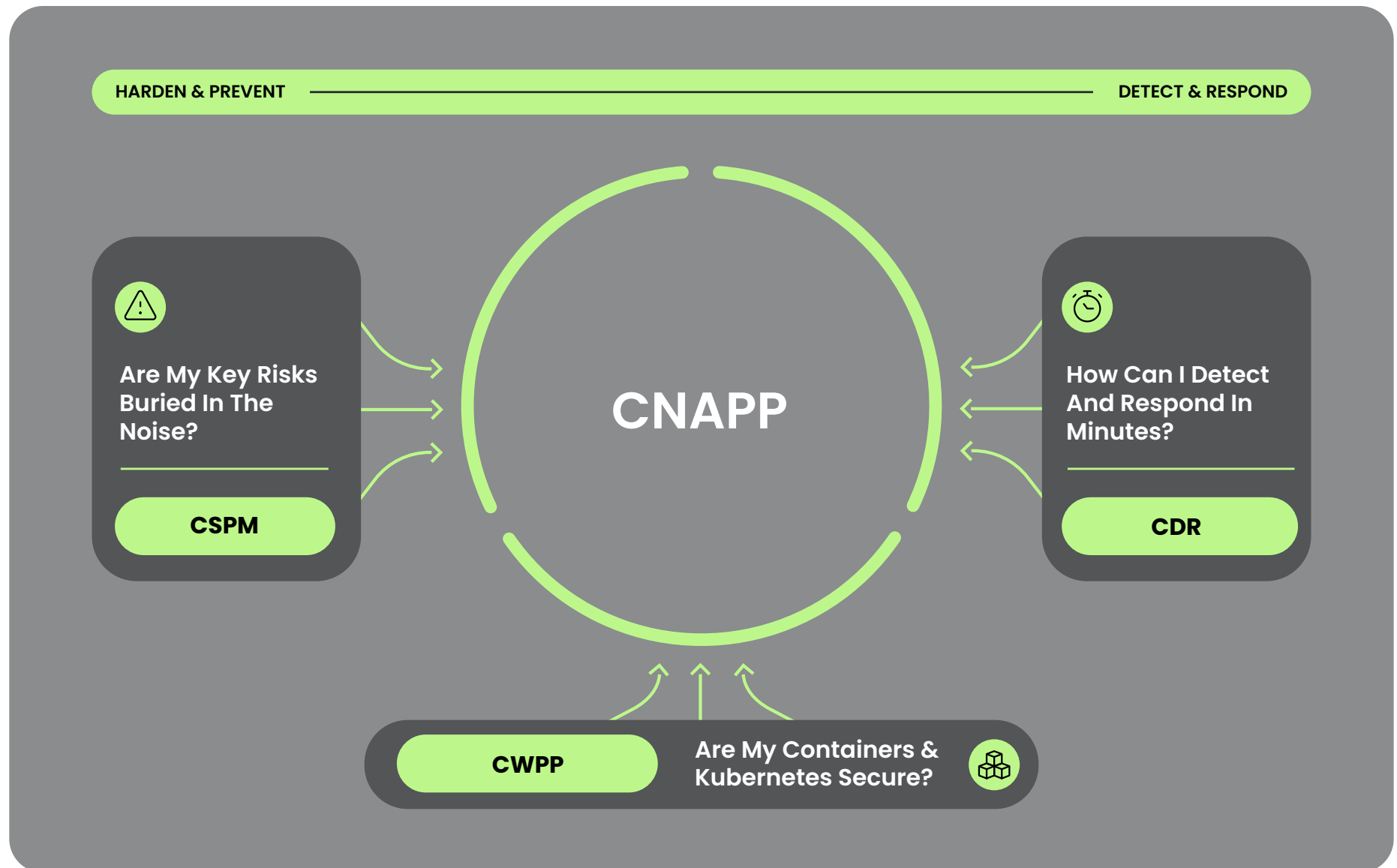
- Artifact scanning
- Cloud configuration
- Runtime protection
- Cloud detection and response

A CNAPP provides a feedback loop that enables true end-to-end coverage of a cloud-native application lifecycle.

3 Gartner, Inc., How to Protect Your Clouds with CSPM, CWPP, CNAPP, and CASB, 2021, Richard Bartley, 6 May 2021

Figure 2

The relationship between key cloud security solution product categories.



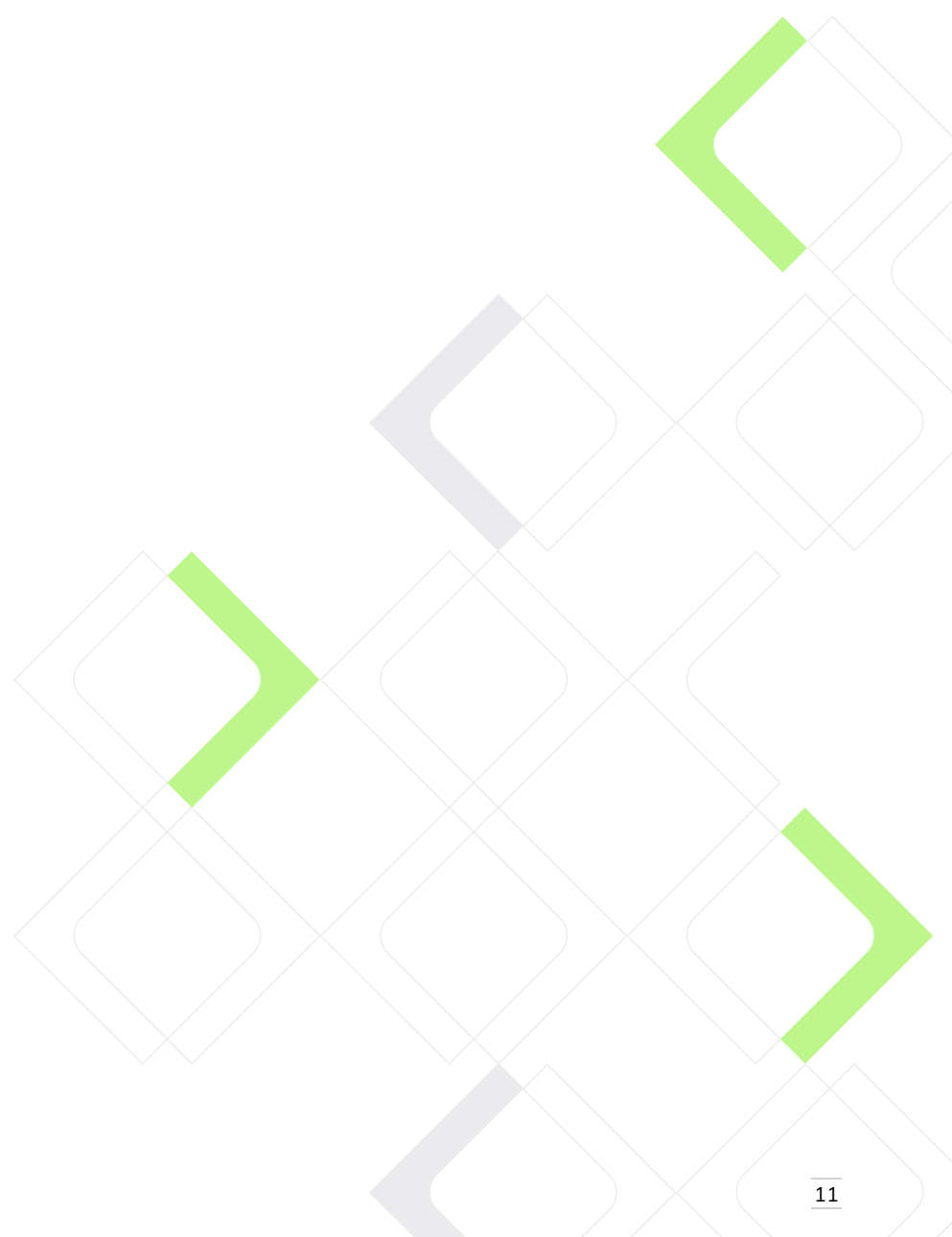
CNAPP has you covered

Implementing a CNAPP can give you dramatically better visibility and control of the entire cloud-native application stack. The alternative is a hodgepodge of point solutions that require inordinate amounts of time and effort trying to consolidate and correlate data across the organization's entire technology landscape, still not knowing conclusively that all areas are covered.

In the fast-moving environment of the cloud, this fragmented, time-consuming approach simply won't work. The Sysdig Threat Research Team has found that the average time from recon to attack completion is just 10 minutes. To outpace modern attacks, security teams have only five seconds to detect an attack, five minutes to triage, and five minutes to respond.

CNAPPs provide comprehensive coverage that moves at the speed of the cloud. In addition, a true CNAPP solution can reveal interrelationships between the insights of various use cases and promote collaboration between SecDevOps, DevOps, and cloud security operations teams. It can be the equalizer when it comes to providing real-time knowledge of the cloud environment and incorporating common workflows, data correlations, meaningful insights, and remediation.

By implementing a CNAPP, you can achieve a higher level of security across all major aspects of your cloud-native application stack. And by embedding CNAPP security from the earliest stages of the development process all the way into production, you can ensure that what is delivered will maintain the highest levels of security and integrity.



Five Key Considerations When Evaluating a Cloud Security Solution

Security tools provided by CSPs offer a wide array of functionalities. They can be plentiful, but most of these tools are geared toward their own cloud environments. To get everything integrated, especially if you're working with hybrid and multi-cloud architectures as many financial services organizations do, requires a lot of work on the part of cloud engineers and security engineers. At times like this, you'd want to consider a third-party solution, a CWPP or CNAPP tool rather than native CSP tooling.

Below are five key points to consider when evaluating a third-party solution:

01

Choose an agentless + agent-based approach for comprehensive protection

When evaluating security tools designed for the cloud – and depending on the service you consume from the cloud provider (IaaS, CaaS, PaaS, FaaS, etc.) – you will come across agentless, agent-based, and approaches that combine both.

Agentless deployments are easier, require minimal management overhead, impose little to no performance overhead, and can accommodate systems that can't handle agents. Because of this, most enterprises that are new to the cloud start with an agentless deployment. These deployments are a great way for security teams to gain breadth of coverage and visibility without slowing down other teams, and can help reduce overall cloud risk, identify areas of concern, and provide an inventory of assets in the cloud environment.

Agent-based approaches provide much deeper visibility that facilitates more comprehensive context and real-time detection, enabling faster incident response, containment, and investigation. But agents are more difficult and time-consuming to manage.

Despite their drawbacks, software agents are likely to play key roles in the cloud for years to come. While agentless security methods can easily access uniform, API-based cloud control planes to identify many types of problems, and they enable quick and easy onboarding, they should be part of a multi-layered defensive strategy that contains both agent-based and agentless technologies. Otherwise, there will be gaps in visibility and solution coverage.

Agentless approaches are effective for inventorying the cloud services your team is using and identifying known vulnerabilities in software. They can also allow your teams to detect threats based on logs. As for agent-based approaches, they deliver real-time detection of runtime threats, malware, and advanced persistent threats. This does not have to mean a point-in-time snapshot – with the use of monitoring logs like CloudTrail, GitHub, or Okta, agentless detections can be genuinely real-time.

Once you detect a threat, the detailed activity record and context an agent provides is critical for incident response, containment, and forensic investigation. To effectively manage security risk requires using both agentless and agent-based approaches.

02 Manage configuration and permission risk

The vast majority of cloud data breaches today occur because of misconfigurations. Unintuitive as this may sound, that's actually great news. With the right tools and controls in place, misconfigurations are almost entirely preventable.

When evaluating cloud security solutions, ensure you have full visibility into cloud assets, and can identify misconfigurations and drift across multi-cloud environments. Implement the least-privilege principle by detecting and removing excessive permissions on user roles, human and non-human. Look for tools that can not only automatically discover all identity and access management roles and their permission configurations, but also can detect roles with excess permissions and recommend the right permission settings.

03 Enable cloud security monitoring with audit logs

Cloud security monitoring is the first crucial step toward keeping track of potential security threats within a sprawling, multi-layered cloud environment. Audit logs systematically record actions within a cloud environment as the actions take place. They tell you who did what, when it happened, and what changed. If someone creates a user, changes permissions, or spins a new instance, it will be traced in those logs.

All of the major public cloud providers offer native services to enable audit logging and help you track the logs. Examples include [AWS CloudTrail](#), [Cloud Audit Logs in GCP](#), and [Azure audit logs](#). Almost anything happening in a cloud environment is tracked and logged in cloud audit logs. By analyzing these audit logs, you can detect unexpected behavior, configuration changes, intrusions, and data theft. However, these services typically work only with individual cloud accounts and individual clouds. If you're like [93% of organizations today](#) that use multiple clouds at the same time, a third-party tool is necessary. Third-party tools aggregate cloud audit logs from across various cloud environments so you can analyze them centrally and detect suspicious patterns within audit data from any public cloud environment.



Falco takes auditing further

Stream detection is a continuous process that collects, analyzes, and reports on data in motion. Based on that idea, the open source community offers a solution: Falco.

Connecting Falco to cloud audit logs allows you to identify unexpected changes to permissions and services access rights, as well as unusual activity that can indicate the presence of an intruder or data exfiltration. It doesn't require you to ship logs into an external repository for threat detection, so you don't incur reduced bandwidth and higher storage costs.

04 Implement runtime detection and response

Act fast on early indicators of compromise (IOC). Runtime threats are real and growing in sophistication. Adversaries are launching complex attacks to evade detection while infecting systems for maximum gain. Don't miss real-time signals. Get deep visibility into events to detect suspicious behavior and malicious activity in the cloud, container, and Kubernetes. Make sure you have the ability to collect detailed forensics evidence in case an incident occurs and the container is gone.

05 Map to the MITRE ATT&CK framework

All major cloud service providers offer native security tools to harden their compute services and environments; however, each of these services is slightly different from the other. Therefore, a common language is needed when talking about cloud security. Adopting a unified security framework will make it easier for security engineers to manage cloud breaches and provide a foundation for threat models and methodologies.

The MITRE ATT&CK framework is a comprehensive knowledge base that categorizes the major threats in a way that helps cybersecurity teams fortify their infrastructure. It provides analysis of all the tactics, techniques, and procedures (TTPs) that advanced threat actors use in their attacks. The MITRE ATT&CK framework serves as a foundation for threat models and methodologies. It can also give you a head start on any compliance standard, since it guides your cybersecurity and risk teams to follow established best practices.

MITRE ATT&CK for cloud maps the specific TTPs that advanced threat actors could possibly use in their attacks on cloud environments.

CHAPTER 05

Shared Responsibility Model for the Cloud

As you choose a cloud security solution, it's also important to understand what you do and don't need to secure – in other words, the shared responsibility model. All major public clouds (e.g., AWS, Azure, GCP) use a shared security concept to distinguish between security risks that the cloud provider manages and those that it expects customers to address.

Under this model, cloud providers are responsible for managing aspects of security on their end, such as securing physical servers that host VM instances and storage buckets. They also perform regular audits of their systems. However, the burden of securing resources that end users deploy in the cloud lies mostly with the end users themselves. At a minimum, cloud providers expect that the data you upload is protected by access controls as mandated by your compliance frameworks, and that you make sure to secure the OS running on a cloud VM instance.

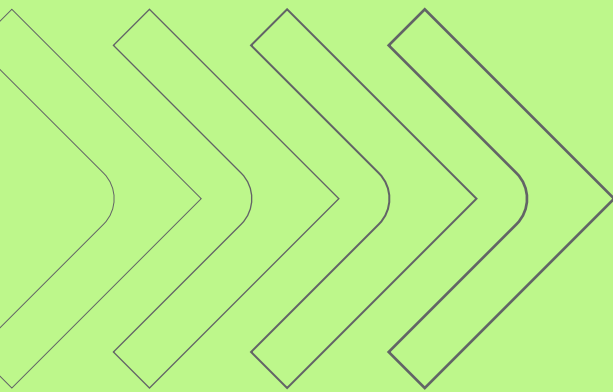
“The burden of securing resources that end users deploy in the cloud lies mostly with the end users themselves.”

Unified Container and Cloud Security With Sysdig

Security in the cloud is fundamentally different than it was on legacy and on-premises systems. But that doesn't mean it's impossible – just that it requires new tools and knowledge to navigate. With the right solution, your teams can spend less time deciphering and resolving security alerts, and more time building the financial products customers want. Look for a CNAPP solution that brings the functionality of cloud security tools (e.g., CSPM, CDR, and CWPP) into one platform, and make sure to evaluate your chosen solution against our key criteria for security and compliance in your industry. In the cloud, every second counts. Sysdig stops cloud attacks in real time by instantly detecting changes in risk with runtime insights, all built on an open source core. Sysdig correlates signals across workloads, identities, and services to uncover hidden attack paths and prioritize the risks that matter most.



Cloud empowers financial service providers to accelerate innovation, but also creates new security and compliance challenges that require new solutions to keep pace. A comprehensive CNAPP approach delivers security insights from development through production to correlate signals and spotlight true risk so you can respond at cloud speed. With the right security capabilities your teams can collaborate more effectively and free time to focus on delivering seamless digital experiences to banking customers.



See how Sysdig helps you secure every second.

Take the next step.

[REQUEST A DEMO →](#)

sysdig

E BOOK

COPYRIGHT © 2023-2024 SYSDIG, INC.
ALL RIGHTS RESERVED
EBK-004-F5 REV. B 03/24

About Sysdig

In the cloud, every second counts. Attacks move at warp speed, and security teams must protect the business without slowing it down. Sysdig stops cloud attacks in real time, instantly detecting changes in risk with runtime insights and open source Falco. Sysdig correlates signals across cloud workloads, identities, and services to uncover hidden attack paths and prioritize real risk. From prevention to defense, Sysdig helps enterprises focus on what matters: innovation.

Sysdig. Secure Every Second.