**A Practical Guide to Gartner’s Cloud Security Archetypes**

**Introduction**

The cloud security solutions market is growing rapidly and there are many types of solutions to support your specific business needs. But figuring out the right tool, let alone the right type of tool, can be difficult. This guidedistills the main concepts of five archetypes that fall under the broader cloud security management platform umbrella:

* Cloud Access Security Broker (CASB),
* Cloud Workload Protection Platform (CWPP),
* Cloud Security Posture Management (CSPM),
* Cloud Infrastructure Entitlement Management (CIEM), and
* Cloud-Native Application Protection Platform (CNAPP).

Gartner developed and defined these archetypes, which often overlap in terms of capabilities, to provide businesses with analysis that better informs their decision making. The last two, CIEM and CNAPP, are recent additions.

**For each category, we will describe:**

* what each tool category is,
* where it is best used, and
* benefits and limitations.

***What Is It?***

We will look at what each tool category does and highlight some notable features.

***In What Context Is It Best Used?***

In these sections, we will look at the best deployment patterns and implementation scenarios for each tool.

Per Gartner, deployment patterns for cloud fall into three general groupings:

1. Infrastructure as a Service (IaaS). This includes the collective group of IaaS-only patterns, including just IaaS and IaaS with containers.
2. Software as a Service (SaaS) and application. This covers all SaaS, and application-level focused patterns, including Platform as a Service (PaaS).
3. Mixed. This covers IaaS plus mixed are more complex combinations of IaaS with other cloud services, including SaaS and PaaS.

Gartner assessed CASB, CWPP, and CSPM tools across these three deployment patterns for single, multi, and hybrid cloud implementations. We will take a look at how they ranked and in what scenarios the tool category could be most useful. Please note that Gartner has not yet formally assessed the CIEM and CNAPP archetypes.

***Benefits and Limitations***

Why use a particular tool category? What are the potential drawbacks to be aware of? We’ll break down the positives and negatives for each one.

**Cloud Access Security Broker**

***What Is It?***

CASBs are on-premises or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers (CSPs) to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention, etc.

***In What Context Is It Best Used?***

According to Gartner, CASBs are most effective on SaaS deployments for single and multi-cloud implementations. CASBs are also somewhat effective in mixed deployments.

***Benefits and Limitations***

***Benefits***

* Good visibility.
* Good detection. Capable of detecting unsanctioned cloud applications (“shadow IT”) and as well as sensitive data in transit.
* Rich data. By its nature of controlling users’ access to cloud SaaS applications, CASBs can produce rich audit logs with events related to the users’ behavior using the applications.

***Limitations***

* Lack automated action. While CASBs can provide great data and information, they do not have the capacity to take automated action to remediate potential threats. This could be a concern for companies who do not have enough security employees to address the high volume of issues that will need manual intervention.
* Struggle to provide consistent information because of incompatible services across CSPs.
* Struggle to keep up with the pace of adoption of services across CSPs
* CASBs require users to go through a central gateway; therefore, if users access cloud resources outside of this avenue (shadow IT), security teams might be blind to it.

**Cloud Workload Protection Platform**

***What Is It?***

According to Gartner, CWPPs are workload-centric security offerings that target the unique protection requirements of workloads in modern hybrid, multi-cloud data center architectures. In plain english, CWPPs help organizations protect their capabilities or workloads (applications, resources, etc.) running in a cloud instance.

CWPP capabilities vary across vendor platforms, but typically include functions like system hardening, vulnerability management, host-based segmentation, system integrity monitoring, and application allow lists. CWPPs enable visibility and security control management across multiple public cloud environments from a single console.

**Gartner divides CWPP vendors into eight categories:**

1. Broad, Multi-OS Capabilities
2. Vulnerability Scanning, Configuration, and Compliance Capabilities
3. Identity-Based Segmentation, Visibility, and Control Capabilities
4. Application Control/Desired State Enforcement Capabilities
5. Memory and Process Integrity/Protection Capabilities
6. Server EDR, Workload Behavioral Monitoring, and Threat Detection/Response Capabilities
7. Container and Kubernetes Protection Capabilities
8. Serverless Protection Capabilities

In its 2020 Market Guide for Cloud Workload Protection Platforms, Gartner states that workloads are becoming more granular — with shorter life spans — as organizations continue to adopt DevOps-style development patterns, with multiple iterations deployed per week or even per day. The best way to secure these rapidly changing and short-lived workloads is to take a proactive approach. By incorporating security via DevSecOps through the use of Infrastructure as Code templates, pre-deployment vulnerability management and code scanning, workloads are protected from the very beginning.

***In What Context Is It Best Used?***

Gartner states that the best possible context for a CWPP is a single provider IaaS, particularly where there are requirements for additional security capabilities to protect workloads.

***Benefits and Limitations***

***Benefits***

* Provide visibility into and control over workloads.
* Provide comprehensive protection against workload risks deployed in IaaS. This is significant because workloads are difficult to protect, and as more organizations adopt container-based service deployments, the difficulty of protecting workloads will persist.
* Can alert and escalate issues; local policy scripting at the workload level permits posture changes, such as firewall changes and application whitelist changes.

***Limitations***

* Lack identity and access management functions.
* Cannot provide overall risk management services across all cloud deployments.
* Cannot perform event monitoring outside of workloads.

**Cloud Security Posture Management**

***What Is It?***

CSPM solutions continuously manage cloud security risk. They detect, log, report, and provide automation to address issues. These issues can range from cloud service configurations to security settings and are typically related to governance, compliance, and security for cloud resources.

CSPM tools focuses on four key areas:

* Identity, security, and compliance
* Monitoring and analytics
* Inventory and classification of assets
* Cost management and resource organization

***In What Context Is It Best Used?***

CSPM tools are most effective when used in multi-cloud IaaS environments. They can also protect IaaS elements of mixed deployments.

***Benefits and Limitations***

***Benefits***

* Provide unparalleled visibility into an organization’s cloud assets and their respective configurations.
* Provide valuable context by mapping interdependencies between cloud infrastructure, services, and abstraction layers to fully understand the source and scope of risk.
* Enforce the protection of data by assuring that native and other data security controls are in place.
* Identify workload issues and potential attack surfaces/exposures by detecting configuration issues/deviation from best practices. They interoperate with native monitoring and alerting to provide effective incident identification and escalation.
* By integrating with identity platforms or native cloud identity, CPSMs help provide privileged access control to IaaS cloud administration.

***Limitations***

Most CSPM limitations are connected to their interconnections with native CSP security controls. For example, CSPMs:

* Do not apply security at the data, operating system or application layers or provide additional data security controls. However, they will enforce native data and application controls.
* Do not typically perform vulnerability scanning directly; rather, they rely on native tools and other third-party product outputs.

**Cloud Infrastructure Entitlement Management**

***What Is It?***

In its 2020 Cloud Security Hype Cycle, Gartner included a new category and corresponding “C” acronym, CIEM. This new archetype describes solutions focused on cloud Identity and Access Management (IAM), which is often too complex and dynamic to be managed effectively by native CSP tools alone. The emerging CIEM category is designated for technologies that provide identity and access governance controls with the goal of reducing excessive cloud infrastructure entitlements and streamlining least-privileged access controls across dynamic, distributed cloud environments.

***In What Context Is It Best Used?***

IaaS and PaaS environments.

***Benefits and Limitations***

***Benefits***

* Provides visibility into who and what can access your cloud resources.
* Replaces time-consuming intervention to remediate overly permissive access and entitlements.
* Protects sensitive data.
* Prevents overly permissive or unintended access.
* Enables and empowers audit and compliance functions.

***Limitations***

* Many CIEM solutions are not constructed holistically; rather, many vendors that deal with IAM outside the cloud are creating piecemeal solutions based on separate products that deal with identity governance and administration, access management, and multi-factor authentication. Managing identity and access in the cloud requires a much broader contextual understanding of an organization’s cloud environments and the various  complex policy layers that determine access and permissions.

**Cloud-Native Application Protection Platform**

***What Is It?***

Gartner recently designated CNAPP as a new category to reflect emerging trends in cloud security. CNAPPs bring application and data context in the convergence of the CSPM and CWPP archetypes to protect hosts and workloads, including VMs, containers, and serverless functions.

***In What Context Is It Best Used?***

IaaS and PaaS environments.

***Benefits and Limitations***

***Benefits***

* Strong automation and orchestration.
* Better security by enabling standardization and deeper layered defenses.
* Allows workloads to be accessed more frequently.

**Divvycloud by Rapid7**

***Where Does DivvyCloud by Rapid7 Fit In?***

The combination of capabilities and broad positioning across the CSPM, CWPP, and CIEM categories supports DivvyCloud by Rapid7’s placement into Gartner’s newest archetype, CNAPP. DivvyCloud by Rapid7 fits nicely in the CSPM category and has become recognized as an industry leader in this capacity. DivvyCloud by Rapid7 also checks off boxes in the CWPP category, and our position is made even stronger when working in conjunction with Rapid7’s InsightVM tool. Furthermore, DivvyCloud by Rapid7’s recently released Cloud IAM Governance module fits into the CIEM category as well.

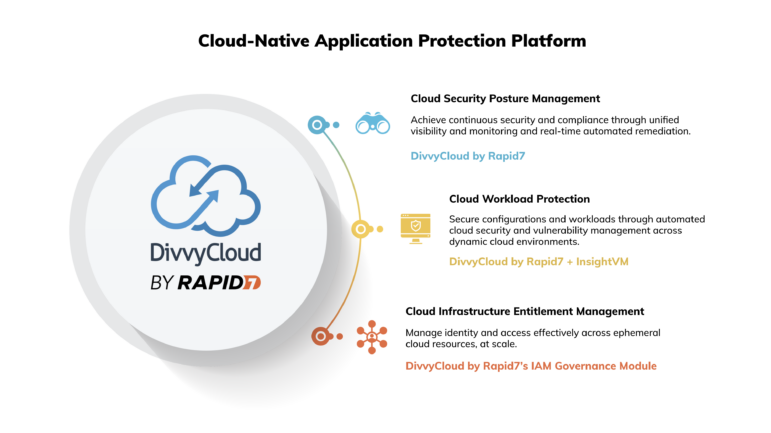
***What Makes DivvyCloud by Rapid7 Stand Out?***

We’ve approached cloud security in a unique way. Here’s how we’re different.

1. **Multi-cloud from the start**. This is important because a majority of organizations don’t rely solely on a single CSP; rather, they use a combination of CSPs and containers. In a multi-cloud environment, you can’t just audit AWS, you have to audit AWS, Azure, GCP, Kubernetes, etc. Those that don’t currently use more than one CSP will likely be multi-cloud in the future — either through mergers and acquisitions or through the natural course of innovation among product development teams.
2. **Unified visibility and monitoring**. Unified visibility allows you to monitor and understand security and compliance across all of your clouds and containers. DivvyCloud by Rapid7 standardizes multi-cloud data as an asset inventory to make cloud security more accessible, even as new services are released by CSPs. For example, with standard terminology across cloud environments DivvyCloud by Rapid7 clarifies provider-specific resource names like S3 Bucket (AWS), Blob Storage Container (Azure), or Cloud Storage (Azure). Instead, DivvyCloud by Rapid7 uses the normalized terminology “Storage Container” for all these.  
     
   With DivvyCloud by Rapid7’s standardized asset inventory, you can apply a unified policy and automated real-time remediation across all of your environments for an approach that is sustainable, comprehensive, and forward-looking.
3. **Real-time automation and remediation**. DivvyCloud by Rapid7 automates the protective and reactive controls necessary for an enterprise to innovate at the speed of cloud. Automation is the key to being able to achieve both security and speed at scale. With an API polling and event-driven approach to identify risk and trigger remediation, DivvyCloud by Rapid7 provides fast detection of changes that enables automated remediation to occur in real time.  
     
   With a highly customizable automation engine, users can quickly and easily define workflows (“Bots”) that deliver automation. A single Bot can be configured to apply a unified approach to remediation across all clouds creating a consistent, scalable, and sustainable approach to cloud security.
4. **Extensible platform**. From custom policies to a robust API, DivvyCloud by Rapid7 can adapt to your unique business needs. We provide a flexible data model with multiple levels of adaptability, including: configuration through the user interface, customization through our plugin-based architecture, and automation through our RESTful API.
5. **Risk Assessment and Auditing**. Our Compliance Scorecard delivers a visual representation of risk aligned with regulatory standards, industry standards, or your own corporate standards. Through our interactive heat map, we provide a unified view across all cloud environments that can be filtered by facets like cloud environment, account, business unit, application, risk profile, compliance standard, etc.
6. **Threat Protection**. We leverage native CSP services and security controls (e.g., Amazon GuardDuty) for best-in-class intelligent threat detection that continuously monitors for malicious activity and unauthorized behavior like:

* crypto-currency mining,
* credential compromise behavior,
* communication with known command-and-control servers, and
* API calls from known malicious IPs.

When a threat is identified, DivvyCloud can perform automated remediation actions, including reconfiguring cloud services, making changes to cloud infrastructure, driving human-centered workflows with integration into systems like ServiceNow and Jira, and orchestrating workflow actions in other security and management systems.

[](https://divvycloud.com/wp-content/uploads/2020/12/Screen-Shot-2020-12-11-at-12.35.16-PM.png)

**DivvyCloud by Rapid7’s Cloud IAM Governance Module**

DivvyCloud by Rapid7’s Cloud IAM Governance module, launched in October 2020, fits into the CIEM category. This new IAM Governance Module helps you:

* Identify and reduce cloud identity risk.
* Gain visibility to assess, prioritize and remediate improper permission combinations that grant unintended or overly permissive access.
* Explore effective access by principal, resource, or application.
* Understand true access of complex IAM combinations.
* Establish and maintain least privilege.
* Limit and understand cloud security blast radius.

**Cloud-Native Security: DivvyCloud and InsightVM**

Balancing cloud security and compliance to support DevOps is critical, as the fundamental role of traditional security teams is changing substantially. As we look to integrate security into the DevOps culture, it is important to rethink our approach and minimize real or perceived friction. A key part of this evolution is adoption of modern tools that support the developer-driven, API-centric, and infrastructure-agnostic patterns of cloud-native security. Rapid7 offers exactly that with a DivvyCloud and InsightVM integration that brings best-in-class capabilities together to solve problems holistically.

When used in combination with Rapid7’s InsightVM tool and its CWPP capabilities, DivvyCloud’s position as a CSPM solution is strengthened even more, giving customers the ability to scan for vulnerabilities and baseline compliance. The combination of InsightVM and DivvyCloud exemplifies the convergence of CWPPs and CSPMs into the new CNAPP category. By using both InsightVM and DivvyCloud concurrently, organizations get the best of both worlds.

**Conclusion**

CSPM and CIEM tools, like DivvyCloud by Rapid7, are important investments for organizations seeking to innovate while staying secure in the cloud. CSPMs provide incredible visibility, monitoring, and detection while taking security a step further — automating responses to mitigate potential risks. CSPMs are uniquely positioned to handle the current and future challenges that make it difficult for organizations to stay secure in the cloud. And with the challenges of identity and access posing significant challenges to cloud security in the near term, the CIEM archetype cannot be overlooked. Fortunately, DivvyCloud by Rapid7’s IAM Governance module fits into this category.

Going beyond CASBs, CWPPs, and CSPMs and into the realm of CNAPPs, the combination of InsightVM and DivvyCloud by Rapid7 offers the best of both worlds as we move toward the next generation of cloud-native security solutions.

Interested in how DivvyCloud by Rapid7 and/or InsightVM can help fuel innovation without sacrificing security? [Schedule a personalized demo](https://divvycloud.com/request-demo/) with one of our cloud security experts.