

# Cloud-Native Application Protection Platforms (CNAPP)

Mike Small, Alexei Balaganski

January 31, 2024



LEADERSHIP  
COMPASS  
2024

This report provides an overview of the Cloud-Native Application Protection Platforms (CNAPP) market and a compass to help you find a solution that best meets your needs. It examines solutions that provide an integrated set of security and compliance capabilities designed to protect cloud-native applications across the development and production lifecycle. It provides an assessment of the capabilities of these solutions to meet the needs of all organizations to monitor, assess, and manage these risks.

## Contents

Contents .....	2
Introduction / Executive Summary.....	4
Highlights .....	4
Market Segment .....	5
Cloud-Native Applications.....	6
Delivery Models .....	8
Required Capabilities.....	8
Leadership.....	11
Overall Leadership.....	11
Product Leadership.....	12
Innovation Leadership .....	14
Market Leadership .....	16
Correlated View.....	18
The Market/Product Matrix .....	18
The Product/Innovation Matrix.....	19
The Innovation/Market Matrix .....	21
Products and Vendors at a Glance .....	23
Product/Vendor evaluation .....	25
Spider graphs .....	25
Aqua Security – Aqua Platform.....	26
Check Point – CloudGuard CNAPP.....	29
Cisco – Panoptica.....	32
CloudDefense.AI – ACS Cloud Security .....	35
CrowdStrike – Falcon Cloud Security .....	38
IBM – Security and Compliance Center.....	41
Lacework – Cloud-Native Application Protection Platform .....	44

Microsoft – Defender for Cloud.....	47
Orca Security – Orca Cloud Security Platform .....	50
Palo Alto Networks – Prisma Cloud.....	53
Sysdig – Secure Platform .....	56
Uptycs – Hybrid Cloud Security Platform.....	59
Wiz – Cloud Security Platform .....	62
Vendors to Watch.....	65
AccuKnox.....	65
AlgoSec .....	65
Caveonix.....	65
Cyscale .....	65
Data Theorem.....	66
Fortinet.....	66
Oracle .....	66
Qualys.....	66
SentinelOne .....	67
Sophos.....	67
Tigera.....	67
VMware.....	67

## Introduction / Executive Summary

This KuppingerCole Leadership Compass provides an overview of the Cloud-Native Application Protection Platform (CNAPP) market segment and the vendors in that segment. It covers the trends that are influencing the market, how it is further divided, and the essential capabilities required of solutions designed to protect cloud-native applications across the development and production lifecycle. It also provides ratings of how well these solutions meet our expectations. To better understand the fundamental principles this report is based on, please refer to [KuppingerCole's Research Methodology](#).

The distinctive feature of CNAPP solutions currently offered by vendors is the integration of several capabilities that were previously offered as standalone products. These most often include Cloud Security Posture Management (CSPM) for identifying vulnerabilities and misconfigurations in cloud infrastructures, Cloud Workload Protection Platforms (CWPP) that deal with runtime protection of workloads deployed in the cloud (such as virtual machines, containers, and Kubernetes, as well as databases and APIs), and Cloud Infrastructure Entitlement Management (CIEM) for centralized management of rights and permissions across (multi-)cloud environments. Cloud Service Network Security (CSNS) is sometimes included as well, combining such capabilities as web application firewalls, secure web gateways, and DDoS protection.

Cloud IaaS is now extensively used to develop and deliver new applications and reengineer existing ones. This is often because cloud services provide an environment for accelerated development without the need for capital expenditure and avoids lengthy procurement delays to obtain hardware. However, security is a shared responsibility for cloud services, and this increases complexity.

While the Cloud Service Providers (CSPs) must take steps to secure the service they provide, it is up to the customer to secure the way they use the service. CNAPP tools are intended to reduce complexity by helping organizations using multiple cloud services to identify and manage the risks for which they have responsibility.

## Highlights

The highlights from this report are:

- The customer is responsible for the security and compliance of how they use cloud services, and there are several factors which increase risks when using the cloud.
- Cloud services are dynamic, thus a traditional static approach to security is not effective. In addition, many organizations fail to adapt and apply their normal internal security and compliance controls.
- The distinctive feature of CNAPP solutions is the integration of multiple capabilities that were previously offered as standalone products to address various risks and challenges.

- This report describes the major capabilities that CNAPP should provide to help customers secure their use of cloud services, and then evaluates solutions from several vendors.
- These solutions should cover the major IaaS cloud services and provide visibility of the risks from the way that these are configured and used.
- The capabilities should automate the detection, reporting and remediation of vulnerabilities and threats across cloud entitlements, compute services, cloud network and storage elements as well as Kubernetes orchestration platforms and CI/CD pipelines.
- The capabilities should support DevOps teams as well as security teams.
- They should also help to manage and report on compliance with laws and regulations, as well as to implement security best practices.
- This is still an evolving market and in the near term we expect products to mature by expanding the depth of their coverage and increasing the use of AI/ML to enhance effectiveness.
- In the longer term, the increasing use of AI and Large Language Models (LLM) creates an entirely new kind of cloud workload with new risks and challenges. Tools will be needed to help to manage these.

## Market Segment

The ready availability of cloud services has changed the way in which organizations do business. Retailers have moved online, manufacturers have reorganized their supply chains, and many employees now work from home. These changes have been made possible by the way in which cloud services enable organizations to respond rapidly to changing business needs. However, while organizations understand how the IT services that they deliver themselves meet their security and compliance obligations, they are often less sure how to meet these when using a cloud service.

The major business risks from the use of IT services, however they are delivered, are the loss of business continuity due to downtime caused by IT service failures as well as cyber-attacks such as ransomware and denial of service; data breaches including data leakage as well as unauthorized access; and the failure to comply with the obligations imposed by laws or regulations. An organization must take appropriate steps to mitigate these risks when they use cloud services, just as they would when using other IT service delivery models.

These risks are not unique to the use of cloud services, but there are several factors which increase risks when using the cloud. Cloud services are frequently used for internet facing applications, and this increases their exposure to external cyber-attacks. In addition, cloud customers may fail to manage their responsibilities for security and compliance effectively.

Also, cloud services are dynamic and a traditional static approach to security is not appropriate. Finally, many organizations fail to adapt and apply their normal internal security and compliance controls, such as identity and access governance and vulnerability management, to their use of cloud services.

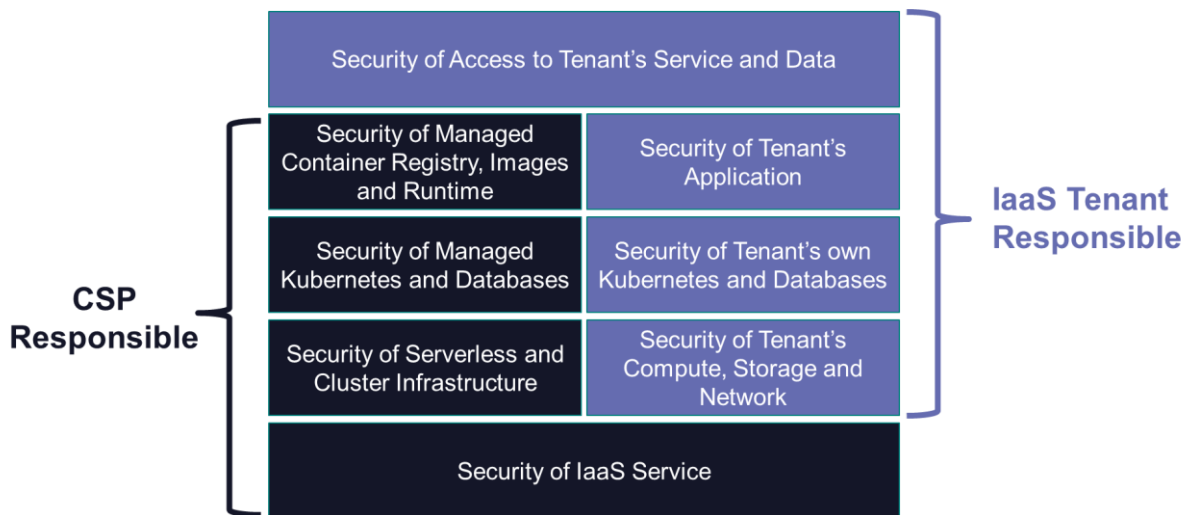


Figure 1: How responsibilities for security and compliance are shared

While major Cloud Service Providers (CSPs) go to great lengths to secure the services that they provide, it is up to the cloud service customers to secure their use of these services. The responsibility for security and compliance is shared between the cloud customer and the CSP. The customer does not manage or control the underlying cloud infrastructure but is responsible for managing everything above the service provided. The customer also remains responsible for compliance with laws and regulations governing the processing of their data. How these responsibilities for IaaS are shared is illustrated in Figure 1.

## Cloud-Native Applications

Cloud-Native Applications are generally built using a microservices architecture based on containers. Microservices, containers, and Kubernetes have become synonymous with modern DevOps methodologies, continuous delivery, and deployment automation and are generally seen as a breakthrough in the way to develop and manage cloud-native applications and services.

Containers are standardized units of software that package application code and all required dependencies into portable images that can be seamlessly deployed in various environments. A container image includes everything an application needs to run – a runtime environment, system libraries and tools, and settings. A single container image can be easily shared between multiple execution environments, as well as instantiated multiple times to support scalability, high availability, and support for hybrid and multi-cloud deployments.

However, this approach brings new security challenges and attempts to repurpose existing security tools to protect containerized and microservice-based applications have proven to be inadequate due to their inability to adapt to the scale and ephemeral nature of containers. Static security products that focus on identifying vulnerabilities and malware in container images, while serving a useful purpose, do not address the full range of potential risks.

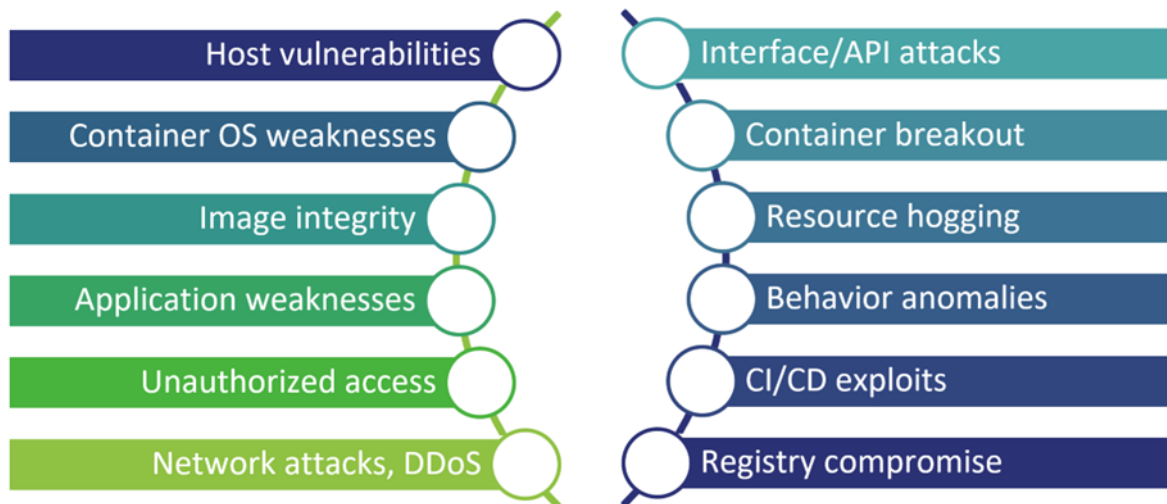


Figure 2: Examples of some risks related to containers.

What further differentiates cloud-native security as a discipline within the larger scope of cybersecurity is that it spans multiple organizational units and teams, which often have conflicting goals and requirements. Application developers, infrastructure operations teams, cloud engineers, security analysts and incident response units, even auditors and legal experts – at different stages of the container lifecycle, all have a say in how exactly this container should be created, inspected, run, monitored, and protected from various risks.

Thus, the primary challenge for vendors creating cloud-native security solutions is making sure that all these various technologies can operate together, fully automated and at the cloud scale, considering the ephemeral and stateless nature of containers that differentiates them from traditional endpoints.

There is a wide range of solutions on the market that help to secure the way in which cloud services are used. These tools provide additional controls that are relevant to the security threats and risks that are relevant to the cloud. These tools include:

- **CASB (Cloud Access Security Brokers)** provides control over which SaaS services organizational users can access. CASB discovers shadow IT usage and prevents access to unsanctioned services that the organization considers to be too risky. They often integrate with the major SaaS services to implement fine-grained controls over how these sanctioned services can be used. They also include or integrate with DLP (Data Leakage Prevention) solutions to control which data can be moved to cloud services.
- **SASE (Secure Access Service Edge)** provides network-based access controls to cloud services. They commonly provide capabilities that are a convergence of SD-WAN (Software Defined Wide Area Networking), SWG (Secure Web Gateways), VPN (Virtual Private Network) and Remote Browser Isolation (RBI) to implement Zero Trust access controls based on the combination of user and device identities.
- **CIEM (Cloud Infrastructure Entitlement Management)** provides controls over the entitlements possessed by virtual resources. In a software defined infrastructure,

such as that provided by a cloud service, the software defined elements need entitlements to operate and threat actors can exploit excessive entitlements.

- **CSNS (Cloud Service Network Security)** provides capabilities to help to secure the in-cloud network, combining tools such as web application firewalls, secure web gateways, and DDoS protection.
- **CSPM (Cloud Security Posture Management)** provides a way to continuously identify, visualize, and manage an overview of the risks associated with the use of IaaS cloud services.
- **CWPP (Cloud Workload Protection Platform)** provides controls at the microservices instance/container level. They typically include threat detection, intrusion prevention, anti-malware, application control, and vulnerability monitoring.
- **DSPM (Data Security Posture Management)** provides a way to discover, catalog and ensure protection and compliance of data held across multiple clouds, from databases to unstructured object storage services.

CNAPP solutions currently offered by vendors provide a platform for IaaS that integrates several of the above capabilities that were previously offered as standalone products. A key success factor for them is the ability to work in unison across multiple environments, architectural layers, and, ideally, third-party integrations providing the additional context needed to achieve robust cloud security.

## Delivery Models

Since the aim of these solutions is to manage risk in how cloud IaaS services are used, it is likely that most will be delivered through the cloud to provide tight integration with the services that they are securing. However, it is possible that some solutions could be delivered and deployed on-premises or at the edge.

Deployment models for CNAPP include:

- a physical appliance – that can be deployed on-premises or in a data center.
- a virtual appliance that can be deployed on-premises or in a cloud service.
- a service from multi-tenant public cloud services where updates and patches are deployed by the service provider across all tenants with full automation. This is a growing market because of ease of adoption combined with the scalability offered by public clouds.
- single-tenant services that can operate in various deployment models, i.e., in private or public clouds or even on-premises, where they are operated in a full as-a-service model, i.e., services where updates, patches, etc. are deployed by the service provider across all tenants with full automation.

## Required Capabilities

This Leadership Compass analyses the main attributes and functions of Cloud-Native Application Protection Platforms. These capabilities should include:



**Basic capabilities** – include analyzing and managing the risks related to the way in which the customer’s cloud IaaS services are configured and being used. These risks include those related to identities and access, the data held, and the security controls implemented to secure network access, compute service elements, container-based DevOps, and applications.

**Deployment** – how quickly, easily, and repeatably can the solution be deployed. This category considers deployment options that the solution offers and whether the solution requires agents installed on the protected systems.

**Administration** – how easy it is to administer the solution. An example would be wizards provided for ease of use and CLI/APIs for automation. It covers the capabilities the solutions provide to securely delegate administration to lines of business managers and application owners.

**Multi-Cloud Coverage** – there are now many public and private cloud services available, and most organizations use more than one of these. Furthermore, these services are based on a wide range of different technologies, many of which are proprietary. Therefore, it is important that the solution covers the risks for this range of cloud services and technologies. These should include the major hyperscale cloud services such as Amazon AWS, Microsoft Azure, IBM, Google Cloud, and Oracle OCI as well as others.

**Service Inventory** – the range of cloud services provided and the dynamic nature of how services are acquired and deployed makes it possible for organizations to be unaware of the services that are in use. This adds to the risks since these services and service elements may not be configured correctly. The solution should be able to dynamically discover and record the services and service elements owned or in use by the customer. In addition, the solution should be able to interoperate with existing CMDB (Configuration Management Data Base) solutions.

**Cloud Entitlements Risks** – the solution should dynamically discover and analyze the user accounts (people and services) with access to the cloud services and their entitlements. It should identify, report, and remediate user accounts with excessive / abnormal privileges and other risks such as orphan accounts (those without owners), as well as accounts with weak authentication policies.

**Data Storage Security** – the solution should discover and analyze the cloud data storage services to identify, report, and remediate excessive risk. This includes data storage services without appropriate controls (e.g., not encrypted), data storage with public access, and data storage directly exposed to the Internet for a wide range of cloud storage types (File Systems, Object Stores, Databases, etc.).

**Cloud Network Security** – the solution should discover and analyze cloud network security controls to support a Zero Trust approach to network management. It should discover and map cloud networks, as well as identify, report, and remediate risky firewall configurations, risky permitted network protocols, and poor TLS certificate management and rotation.

**Cloud Compute Service Security** – the solution should discover and analyze cloud compute services owned to identify, report, and remediate risky configurations. It should cover VMs with risky patch levels, VMs with unmanaged vulnerabilities, and risky configurations for a wide range of VM and OS types. It should also support these capabilities for serverless computing elements.

**Cloud Container Security** – the solution should be able to discover and report on cloud container services owned. Identify / report / remediate insecure container images, container registries, and deployments for common container environments such as Kubernetes.

**Cloud Application Security** – the solution should be able to discover, and report on cloud apps deployed and identify / report / remediate apps exposed to the internet, apps with exposed vulnerabilities (e.g., SQL Injection), apps without appropriate traffic controls (e.g., WAF), and apps with other risky deployments.

**Application Programming Interface (API) Security** – the solution should be able to discover and identify / report / remediate APIs exposed to the internet and APIs without appropriate access controls, including those developed by the organization, as well as management interfaces provided by cloud services themselves.

**Risk Reporting** – the solution should provide capabilities to report on the risks that have been discovered. The reports should provide information on the likelihood of the risk and its impact. It should provide a report of the aggregated overall risk / security posture based on its analysis, suitable for presentation to board level management. The reporting capabilities should be interactive, allowing the user to expand the overall risks to identify the underlying causes. The solution should also support integration with workflow / ticketing systems to recommend, initiate, and track remediation.

**Compliance and Best Practices** – the solution should support the comparison and reporting of security posture against a range of common security frameworks and best practices such as NIST, ISO/IEC 2700x, CIS as well as major regulatory obligations.

## Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identify vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept or pilot phase, based on the specific criteria of the customer.

Based on our evaluation, we created various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

## Overall Leadership

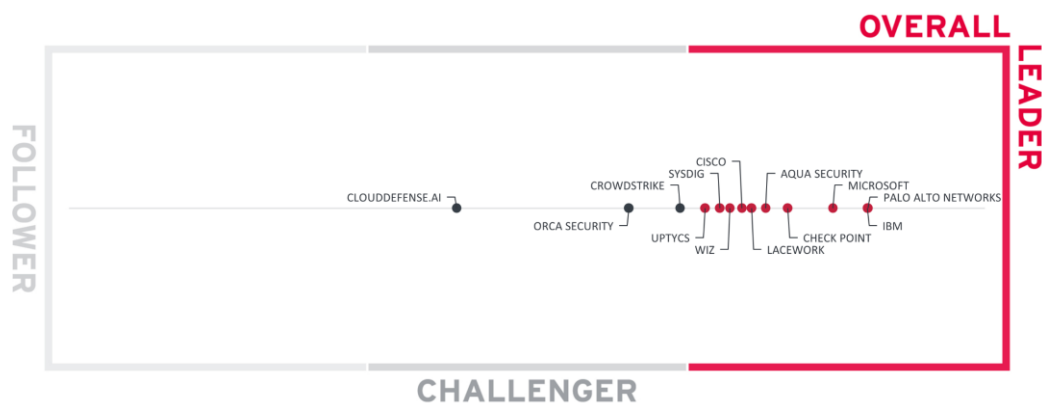


Figure 3: Overall Leadership in the Cloud-Native Application Protection (CNAPP) market

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right. The rating provides a consolidated view of all-around functionality, market presence, and financial security.

However, these vendors may differ significantly from each other in terms of product features, innovation, and market leadership. Therefore, we recommend considering our other leadership categories in the sections covering each vendor and their products to get a comprehensive understanding of the players in this market and which of your use cases they support best.

Among the Overall Leaders we can find a group of large, established security vendors like Microsoft, Palo Alto Networks, Check Point, and Cisco – all of which are equally strongly represented in other KuppingerCole’s Leadership Compasses. However, they are joined by somewhat smaller and more specialized cloud security providers like Wiz, Aqua Security, Sysdig, Uptycs, and Lacework. This clearly demonstrates the continued growth and the

turbulent evolution of the CNAPP market that creates equal opportunities for industry veterans and successful cloud-native startups.

Among the Challengers, we observe CrowdStrike, a well-established endpoint security vendor that has only recently expanded into the field of cloud security, as well as Orca Security and CloudDefense.AI – both pure-play CNAPP solution providers, which are yet to gain a strong foothold in the global market.

There are no Followers in this overall leadership rating.

Overall Leaders are (in alphabetical order):

- Aqua Security
- Cisco
- Check Point
- IBM
- Lacework
- Microsoft
- Palo Alto Networks
- Sysdig
- Uptycs
- Wiz

## Product Leadership

Product leadership is the first specific category examined below. This view is mainly based on the presence and completeness of required features as defined in the required capabilities section above. The vertical axis shows the product strength plotted against the combined/overall strength on the horizontal axis. The Product Leadership chart is rectangular and divided into thirds. Product Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

All vendors found among the Product Leaders deliver leading-edge capabilities across the depth and breadth of the Cloud-Native Application Protection Platforms (CNAPP) capability spectrum evaluated for the vendors in this Leadership Compass. However, we can also observe some much smaller vendors among the leaders, which nevertheless are able to offer their solutions with comprehensive capabilities, flexible deployment options and lower operational complexity than the market giants.

CloudDefense.AI is the only Challenger in this rating. It has a good offering but lacks certain advanced capabilities that we expect to see, either in the depth or breadth of functionalities seen in the Leadership segment offerings.

There are no Followers in the Product Leadership rating.



Figure 4: Product Leadership in the Cloud-Native Application Protection (CNAPP) market

Product Leaders are (in alphabetical order):

- Aqua Security
- Check Point
- Cisco
- CrowdStrike
- IBM
- Lacework
- Microsoft
- Orca Security
- Palo Alto Networks
- Sysdig

- Uptycs
- Wiz

## Innovation Leadership

Next, we examine innovation in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

This view is mainly based on the evaluation of innovative features, services, and/or technical approaches as defined in the Required Capabilities section. The vertical axis shows the degree of innovation plotted against the combined/overall strength on the horizontal axis. The Innovation Leadership Chart is rectangular and divided into thirds. Innovation Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

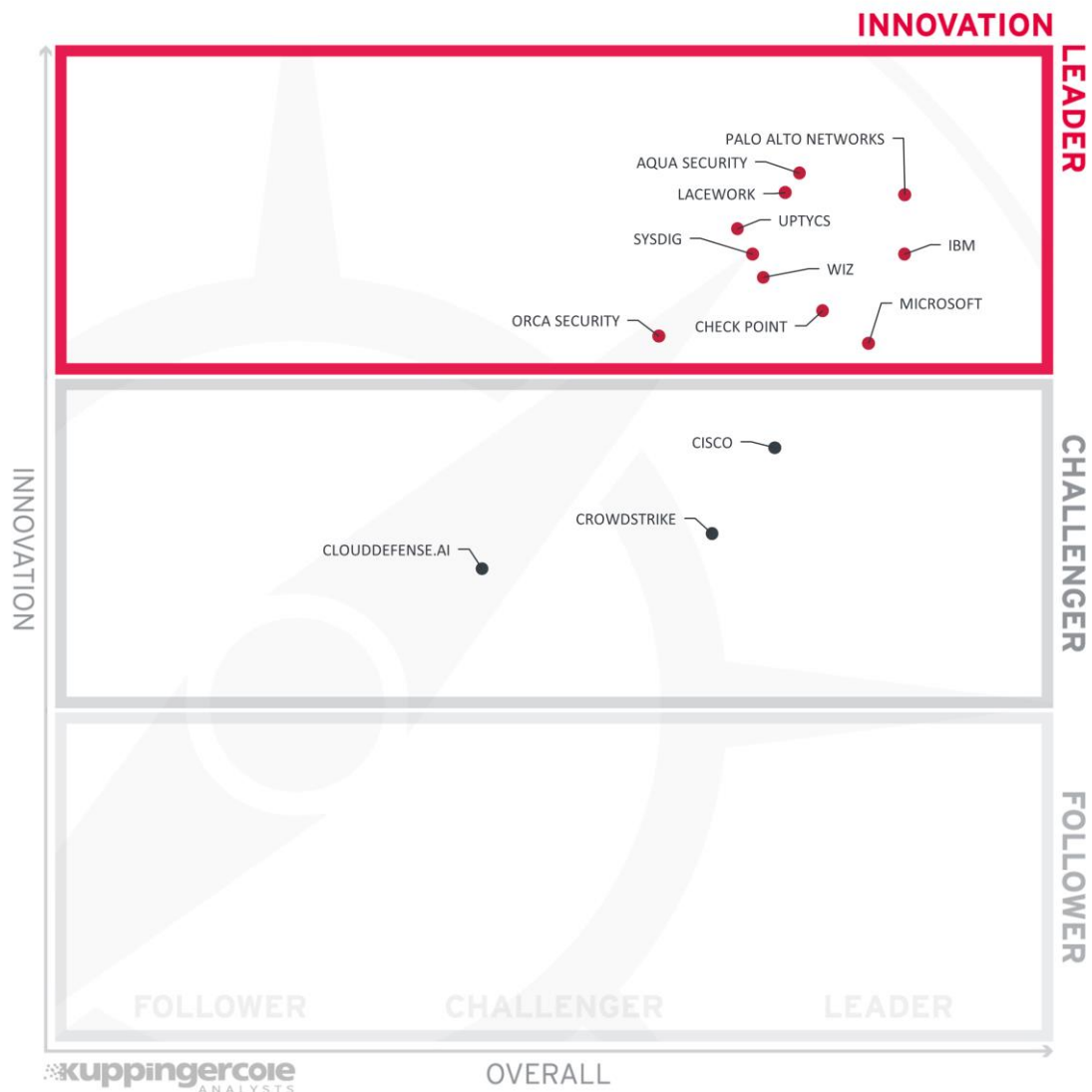


Figure 5: Innovation Leadership in the Cloud-Native Application Protection (CNAPP) market

Innovation Leaders are those vendors that are delivering cutting-edge products, not only in response to customers’ requests, but also because they are driving the technical changes in the market by anticipating what will be needed in the months and years ahead. There is a correlation between the Overall, Product, and Innovation Leaders, which demonstrates that leadership requires feature-rich products that are looking over the horizon to bring advancements to help their customers.

There are also some newer vendors that we have identified in the leadership category because of their vision and how this is implemented in their solutions.

The Challengers also have some specific innovations that make their offerings attractive to their customers but lack the breadth of innovation that other vendors demonstrate; among the Innovation Challengers we can observe CloudDefense.AI, CrowdStrike, and Cisco.

Again, there are no Followers in the Innovation rating.

Innovation Leaders (in alphabetical order):

- Aqua Security
- Check Point
- IBM
- Lacework
- Microsoft
- Orca Security
- Palo Alto Networks
- Sysdig
- Uptycs
- Wiz

## Market Leadership

Lastly, we analyze Market Leadership. This is an amalgamation of the number of customers, the number of transactions evaluated, the ratio between customers and managed identities/devices, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and the financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

In this chart, the vertical axis shows the market strength plotted against the combined/overall strength on the horizontal axis. The Market Leadership Chart is rectangular and divided into thirds. Market Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

It is entirely unsurprising that only the large, established vendors with global market presence have made it into the Leaders segment. These include Microsoft, Cisco, Palo Alto Networks, Check Point, and CrowdStrike (the latter being a relative newcomer to cloud security).

The rest of the vendors are found among Market Challengers. Some of them are relatively young, lack a comprehensive global presence, focus mainly on their home markets, or are still in their growth phase.

There are no Followers in this market segment as well.





Figure 6: Market Leaders in the Cloud-Native Application Protection (CNAPP) market

Market Leaders (in alphabetical order):

- Check Point
- Cisco
- CrowdStrike
- IBM
- Microsoft
- Palo Alto Networks

## Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a product leader, but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

### The Market/Product Matrix

The first of these correlated views contrasts Product Leadership and Market Leadership.



Figure 7: Market/Product Matrix for the Leadership Compass CNAPP

The vertical axis represents the market position plotted against product strength rating on the horizontal axis.

This comparison shows which vendors are better positioned in our Product Leadership analysis than their position in the Market Leadership analysis. Vendors above the line are somewhat "overperforming" in the market. It comes as no surprise that these are often very large vendors, while vendors below the line may more often be innovative but focused on specific regions, as an example.

In the upper right segment, we find "**Market Champions**". Here we see the major vendors in the cloud security market: Aqua Security, Check Point, Cisco, CrowdStrike, IBM, Microsoft, and Palo Alto Networks as market champions positioned in the top right-hand box.

In the top center box, we see no vendors that have a strong market presence but with products that are less feature-rich in this market.

**Market Disruptors** – In the middle right-hand box, as this is an emerging market, we see vendors that deliver strong product capabilities for this market segment but are not yet considered Market Champions. These vendors are Lacework, Orca Security, Sysdig, Uptycs, and Wiz. These all have a strong potential to disrupt the market and improve their market position due to the strong product capabilities they are already delivering.

In the middle of the chart, we see the vendors that provide good but not leading-edge capabilities and therefore are not market leaders. The vendor in this position is CloudDefense.AI.

## The Product/Innovation Matrix

This view shows the correlation between Product Leadership and Innovation. It is not surprising that there is a fairly good correlation between these two views, with a few exceptions. The distribution and correlation are tightly constrained to the line, with a considerable number of established vendors plus some smaller vendors.

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

The vendors positioned closest to the line are those showing a good balance of product features and innovation. While all the vendors take different approaches to delivering CNAPP, all perform well in both the current product offering and the level of innovation they demonstrate.

The box at the top right contains the technology leaders. These vendors all show strong innovation and offer strong products in this market. These vendors are (in alphabetical order): Aqua Security, Check Point, IBM, Lacework, Microsoft, Palo Alto Networks, Orca Security, Sysdig, Uptycs, and Wiz.

Cisco, and CrowdStrike appear in the top middle top box with excellent products but less innovation in this market segment than those in the top right-hand box.

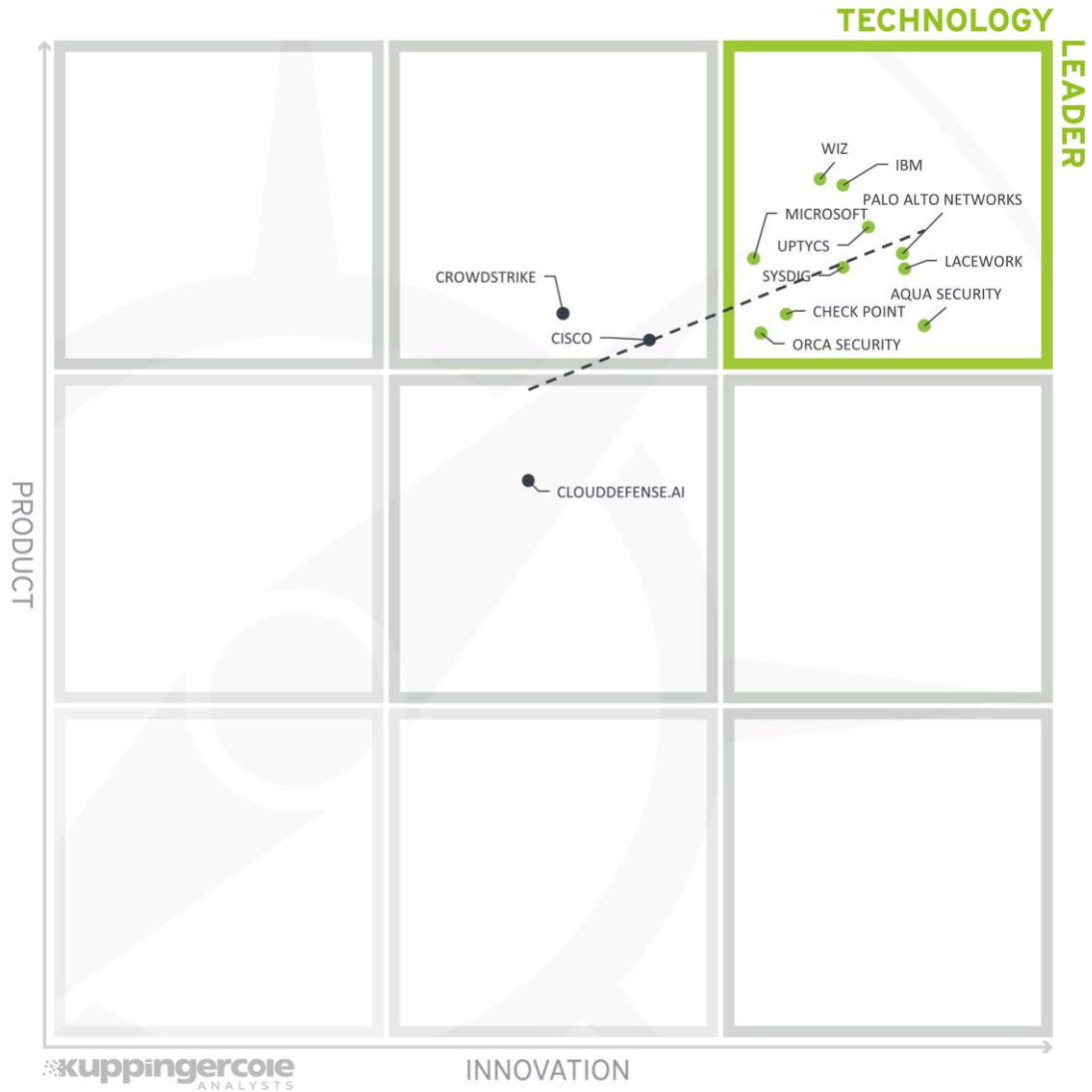


Figure 8 Product/Innovation Matrix for the Leadership Compass CNAPP

One vendor appears in the center box, showing both good innovation and product capabilities. However, it remains at a Challenger level in both product and innovation ratings. This vendor is CloudDefense.AI and has the potential to further increase its position in the CNAPP market.

## The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

The vertical axis represents the market position rating plotted against innovation in this market on the horizontal axis. Note that some vendors may have a different rating for innovation in different markets.

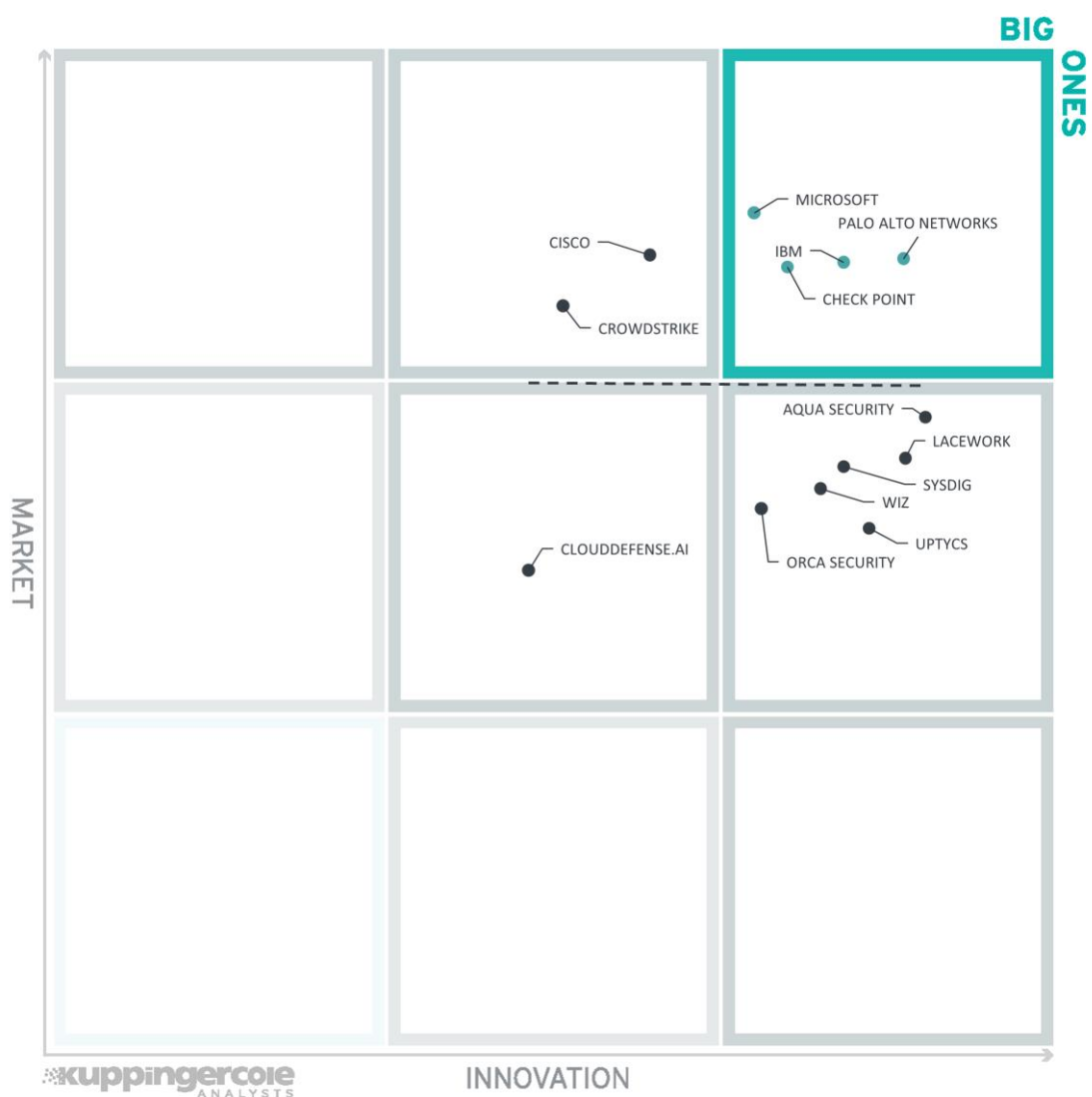


Figure 9 Market/Innovation Matrix for the Leadership Compass CNAPP

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate though having less market share, and thus the biggest potential for improving their market position.

In the upper right-hand corner box, we find the "**Big Ones**" in the CNAPP market. We see (in alphabetical order) Check Point, IBM, Microsoft, and Palo Alto Networks. These companies are being rewarded by the market for the level of innovation they provide in their products and services.

In the top middle box, there are two vendors with a strong market presence and good innovation. These are (in alphabetical order) Cisco and CrowdStrike.

**Market Disruptors** - Several vendors appear in the middle right box, showing a proficient level of innovation but with less market presence than the vendors in the "Big Ones" category. These include (in alphabetical order) Aqua Security, Lacework, Orca Security, Sysdig, Uptycs, and Wiz. These innovators are setting new standards for solutions in this market by providing easy to use, lightweight and highly scalable SaaS-based solutions that have the potential to change the market landscape.

One vendor appears in the center box, it remains at a Challenger level in both market and innovation ratings. This vendor is CloudDefense.AI and has the potential to further increase its position in the CNAPP market.

## Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Cloud-Native Application Protection Platforms. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other.

These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1.

Vendor	Security	Functionality	Deployment	Interoperability	Usability
<b>AQUA SECURITY</b>	strong positive	strong positive	strong positive	strong positive	positive
<b>CHECK POINT</b>	strong positive	strong positive	strong positive	strong positive	strong positive
<b>CISCO</b>	strong positive	positive	strong positive	positive	strong positive
<b>CLOUDEFENSE.AI</b>	strong positive	positive	strong positive	neutral	positive
<b>CROWDSTRIKE</b>	strong positive	positive	strong positive	positive	strong positive
<b>IBM</b>	strong positive	strong positive	strong positive	strong positive	strong positive
<b>LACEWORK</b>	strong positive	strong positive	strong positive	strong positive	strong positive
<b>MICROSOFT</b>	strong positive	positive	strong positive	strong positive	strong positive
<b>ORCA SECURITY</b>	positive	strong positive	strong positive	positive	positive
<b>PALO ALTO NETWORKS</b>	strong positive	strong positive	strong positive	strong positive	strong positive
<b>SYSDIG</b>	strong positive	strong positive	strong positive	strong positive	positive
<b>UPTYCS</b>	positive	strong positive	strong positive	strong positive	positive
<b>WIZ</b>	strong positive	strong positive	strong positive	strong positive	strong positive

Table 1: Comparative overview of the ratings for the product capabilities

In addition, we provide in Table 2 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
<b>AQUA SECURITY</b>	strong positive	strong positive	positive	positive
<b>CHECK POINT</b>	strong positive	strong positive	strong positive	strong positive
<b>CISCO</b>	positive	strong positive	strong positive	strong positive
<b>CLOUDEFENSE.AI</b>	positive	neutral	neutral	neutral
<b>CROWDSTRIKE</b>	positive	strong positive	strong positive	strong positive
<b>IBM</b>	strong positive	strong positive	strong positive	strong positive
<b>LACEWORK</b>	strong positive	positive	strong positive	positive
<b>MICROSOFT</b>	strong positive	strong positive	strong positive	strong positive
<b>ORCA SECURITY</b>	strong positive	positive	positive	positive
<b>PALO ALTO NETWORKS</b>	strong positive	strong positive	strong positive	strong positive
<b>SYSDIG</b>	strong positive	positive	positive	positive
<b>UPTYCS</b>	strong positive	positive	positive	neutral
<b>WIZ</b>	strong positive	positive	positive	positive

Table 2: Comparative overview of the ratings for vendors



## Product/Vendor evaluation

This section contains a quick rating for every product/service we have included in this KuppingerCole Leadership Compass document. For many of the products, there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

### Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For the Cloud-Native Application Protection Platforms, we look at the following eight categories:

**Multi-Environment** – the extent to which the capabilities provided cover a wide range of cloud services, as well as integrate with a wide range of DevOps and security tools and standards.

**Cloud Entitlements** – dynamically discover and analyze the user accounts (people and services) with access to the cloud services and their entitlements. It should identify, report, and remediate user accounts with excessive / abnormal privileges and other risks such as orphan accounts, as well as accounts with weak authentication policies.

**Cloud Storage Security** – discover and analyze cloud data storage services to identify, report, and remediate excessive risk. This includes data storage services without appropriate controls, data storage with public access, and data storage directly exposed to the Internet for a wide range of cloud storage types.

**Cloud Network Security** – discover and analyze cloud network security controls to support a Zero Trust approach to network management, map cloud networks owned, and identify, report, and remediate risky firewall configurations, risky permitted network protocols, etc.

**Cloud Compute Security** – discover and analyze cloud compute services owned to identify, report, and remediate risky configurations of virtual machines and serverless computing elements.

**Cloud Container Security** – discover and report on cloud container services owned. Identify / report / remediate insecure container images, container registries and deployments for common container environments such as Kubernetes.

**Cloud Application Security** – discover, and report on cloud apps deployed and identify / report / remediate apps exposed to the internet, apps with exposed vulnerabilities, apps without appropriate traffic controls, and apps with other risky deployments.

**Cloud Posture Management** – continuously identify, visualize, and manage an overview of the risks associated with the use of the IaaS cloud services and how well this use complies with a range of regulations, standards, and best practices.

## Aqua Security – Aqua Platform

Aqua Security is a cloud-native security company headquartered in Ramat Gan, Israel. It was founded in 2015 with the mission to protect cloud native assets. It is one of the pioneers among the dedicated cloud-native security solution providers. As well as providing security solutions, it also maintains a large open-source ecosystem with projects like Trivy, a container vulnerability scanner.

Aqua Platform is a complete cloud-native security platform that provides security across the application lifecycle (from development to production), for the whole stack (workloads, infrastructure, hosts, orchestration, and cloud layers), and across containers, virtual machines, and serverless functions.

It supports a wide range of cloud services and DevOps environments. It also features AI-based recommendations for remediating issues across container images and other artifacts, multiple clouds, and multiple workload types.

The platform is designed from the ground up to ensure consistent visibility into and protection for cloud workloads from the early development stage, beginning with identifying software supply chain risks in application source code. Vulnerability management and dynamic threat analysis help to identify, classify, and analyze both known and unknown vulnerabilities.

Vulnerability scanning is inbuilt and uses Trivy. The solution does not support third-party scanners for containers, but it does support third-party scoring of vulnerabilities. It features automated Static Application Security Testing (SAST) that helps to uncover issues in code and to use open-source components safely with Software Composition Analysis (SCA) that integrates directly into the Integrated Development Environment (IDE), as well as dynamic threat analysis to detect malware in container images using a secure sandbox.

It can scan Kubernetes clusters for misconfigurations that could be exploited and use pre-defined assurance policies to automate the secure deployment of Kubernetes applications at the Kubernetes admission controllers. Furthermore, it can also block the usage of misconfigured or risky Infrastructure as Code (IaC) files.

It can help to identify and remove risks in proprietary and third-party code, generate Software Bills of Materials (SBOMs), ensure integrity of images through build pipelines, and secure the tools and processes used to build applications.

Aqua includes Cloud Detection and Response (CDR) that can help to identify previously unknown attack patterns in real time using extended Berkeley Packet Filter (eBPF) and behavioral indicators curated by the Aqua Nautilus threat research team. This in addition to deterministic runtime controls such as drift prevention, fileless execution, and reverse shell execution. It supports compliance reporting with out-of-the-box reports policies and reports covering a wide range of security and risk frameworks including ISO/IEC 27001, NIST Cybersecurity Framework, and MITRE ATT&CK as well as CIS Benchmarks.

All these capabilities are integrated into a single control plane with unified policy management across different workload types, as well as common User interface, access management, reporting, etc. The Aqua platform is designed for SaaS delivery, but can be run in isolated environments as well, both on-premises and in edge deployments.

Organizations looking for a container focused CNAPP should consider the Aqua Security Platform.

<b>Security</b>	strong positive	
<b>Functionality</b>	strong positive	
<b>Deployment</b>	strong positive	
<b>Interoperability</b>	strong positive	
<b>Usability</b>	positive	

Table 3: Aqua Security's rating

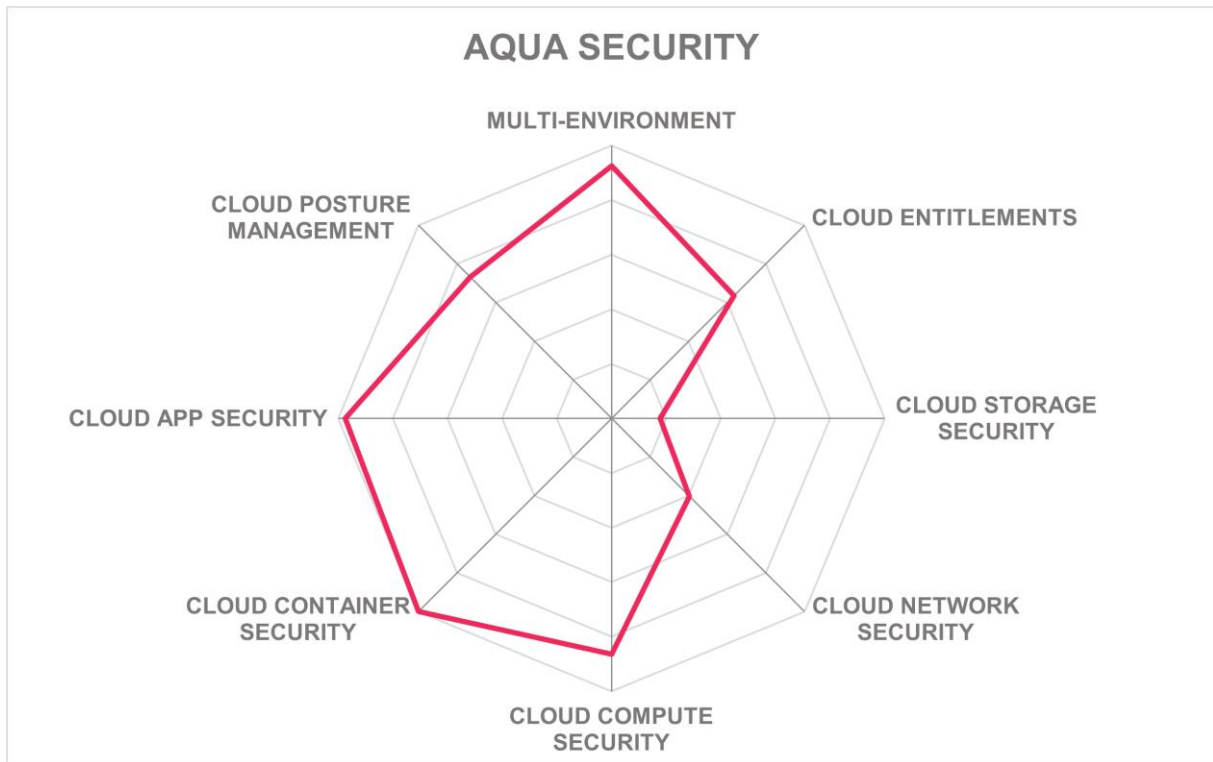
### Strengths

- Fully integrated, unified platform specifically designed for cloud-native workload security.
- Supports a wide range of cloud services including Alibaba, Azure, AWS, Google Cloud, IBM Cloud, Oracle OCI as well as VMWare.
- Agents are not required, but are needed for certain types of detections, for example real-time detection and blocking, or detecting in-memory attacks.
- Detects security risks related to service elements with excessive account permissions or entitlements.
- Network discovery is used to create zero-trust (allow listing) of inbound and outbound connections between microservices.
- Detects known vulnerabilities and exposures (CVEs) within compute service elements as well as risky OS configurations.
- Includes own anti-malware embedded as part of the default policy.
- Supports a wide range of Kubernetes orchestration platforms including Amazon EKS, Microsoft Azure AKS, Google GKE, Oracle OKE, Red Hat OpenShift, Rancher, and VMWare Tanzu.
- Fully covers each phase of the workload lifecycle, at every layer of infrastructure.
- Supports integration with a wide range of developer CI/CD pipelines.
- Inbuilt SBOM capabilities include analysis of dependencies, and support for export/import of SPDX and CycloneDX.
- Provides out of the box policies and reports covering a wide range of security and risk frameworks including ISO/IEC 27001, NIST Cybersecurity Framework, and MITRE ATT&CK as well as CIS Benchmarks.
- Interoperates with a wide range of SIEM platforms and other security operations solutions out of the box.

### Challenges

- Does not cover risks related to user accounts for cloud service administrators.
- Does not cover risks related to cloud data storage systems.
- Limited coverage of cloud network security risks.
- Does not offer security controls for service meshes.
- As a pure-play cloud-native security vendor, additional coverage would require third-party integrations.

Leader in



## Check Point – CloudGuard CNAPP

Check Point Software Technologies Ltd. was founded in 1993 and provides cybersecurity solutions to corporate enterprises and governments around the world. Check Point Infinity's portfolio of solutions comprises three core pillars: Check Point Harmony, for remote users; Check Point CloudGuard, to automatically secure clouds; and Check Point Quantum, to protect network perimeters and datacenters. This report focuses on Check Point Cloud Guard.

CloudGuard CNAPP provides protection for every layer of cloud application workloads, including identities and data from CI/CD to runtime. It replaces legacy application security solutions like Web Application Firewalls with a unified AI-powered protection engine that helps eliminate false positives with continuous dynamic behavior profiling of each user and resource.

It helps security and DevOps teams to deploy applications with a Zero Trust approach to security. CloudGuard Posture Management provides both agent and agentless visibility and assesses security posture, detects misconfigurations, automates, and actively enforces standard policies, and protects against attacks and insider threats.

CloudGuard's Effective Risk Management (ERM) engine prioritizes risks and provides remediation guidance using AI and risk scoring to reduce the attack surface. It covers applications running in multiple cloud services including Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure as well as Alibaba Cloud, and Kubernetes.

Delivered a SaaS, it does not require agents, making it easy and fast to deploy. It provides a single common graphical interface to specify, monitor, and enforce security policies across multiple service environments. It uses the underlying cloud controls to implement the policy on each cloud.

CloudGuard pulls information from the Cloud Providers to create and maintain a frequently updated inventory of cloud accounts and entitlements. It detects security risks related to account entitlements and CIEM (as a part of the CNAPP platform) provides automatic recommendations of the least privilege policies based on actual permission usage.

CloudGuard supports DevSecOps by seamlessly integrating into the CI/CD pipeline to scan code, automate protection, detect malware, and eliminate blind spots. In addition, it automates open-source governance and SBOM creation to ensure software supply chain security. CloudGuard Spectral automated tools integrate with developers' tools to prevent exposing API keys, tokens, and credentials, as well as remediating security misconfigurations.

Check Point CloudGuard provides automated cloud-native security, unified across applications, workloads, and network to manage risk, maintain posture, and prevent threats at cloud speed and scale.

<b>Security</b>	strong positive
<b>Functionality</b>	strong positive
<b>Deployment</b>	strong positive
<b>Interoperability</b>	strong positive
<b>Usability</b>	strong positive



Table 4: Check Points's rating

### Strengths

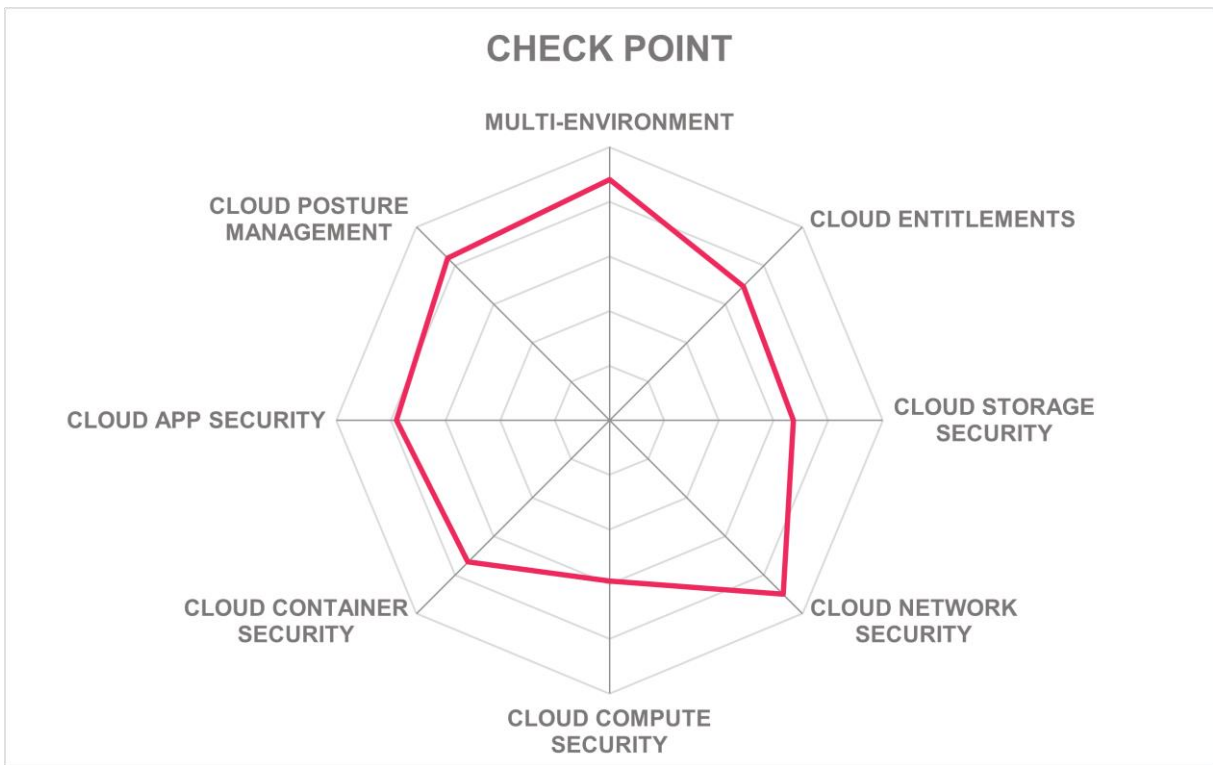
- Effective Risk Management (ERM) engine prioritizes risks and provides remediation guidance using AI and risk scoring to reduce the attack surface.
- Delivered as SaaS for ease of deployment.
- Covers a wide range of services and development environments.
- Helps to secure both “Lift and Shift” and “Cloud-Native” cloud deployments.
- It can be either agent-powered or agentless, depending upon customer requirements.
- Agentless Workload Posture scans and identifies risks across all cloud workloads, including Serverless and Virtual Machines.
- Cloud native workload protection covers APIs and microservices from development to runtime.
- Detects and blocks malicious behaviors with guardrails for Kubernetes cluster operations.
- Patent-pending AI engine provides context-based web application and API protection.
- Integrates into the CI/CD pipeline to prevent vulnerabilities and exposures such as hard-coded secrets from reaching production.
- Context Graph helps to highlight potential attack paths.
- Out-of-the-box integration with a wide range of SIEM, incident management, and workflow tools.

### Challenges

- Documentation is only available in English and Chinese. However, support services are available in many languages from offices across the world.
- Limited coverage of cloud storage vulnerabilities, such as data exposed directly to the internet.
- Does not detect missing / misconfigured anti-malware protection.
- Only covers risks in Linux variants.

Leader in





## Cisco – Panoptica

Cisco Systems, Inc. is a well-established digital communications technology conglomerate with its headquarters in San Jose, California. The company offers a wide range of cybersecurity products including firewalls, intrusion prevention systems, secure access systems, security analytics and malware defense.

Panoptica is Cisco's cloud-native application security solution, and it provides contextualized security that can help to identify, prioritize, and remediate security risks and misconfigurations in complex cloud environments. It includes capabilities that cover cloud security including Cloud Workload Protection, CI/CD security, Kubernetes Security Posture Management, API security, Cloud Security Posture Management, and Attack Path Analysis that includes a superset of functionality acquired from Lightspin.

The platform integrates with a wide range of existing tools and toolchains that DevOps teams are already using. It can help SecOps teams to observe and address security vulnerabilities and threats with real-time recommendations across the full stack of cloud assets based on business risk. It integrates with GitHub as a code repository, Jenkins and CircleCI for continuous integration (CI) pipelines, Helm for software deployments and Terraform for the infrastructure required by applications.

Furthermore, Panoptica scans all computing assets and images for CVEs, Malware and generates a software bill of materials (SBOM) for each image, identifies the vulnerabilities associated with each layer, and analyses deployment templates for configuration risk. It uses contextual mapping over graph database to identify the relationships between all cloud assets and services, and detect all potential attack path, to provide an accurate and up-to-date view of the cloud environment's security posture.

Panoptica provides visibility, risk analysis and remediation for any cloud service including Network, Identity, Data Stores and Compute services such as VMs, Serverless functions. It can inspect workloads for vulnerabilities and rank them by a risk score to identify the most urgent threats. It supports attack path analysis to accurately discover and remediate attack routes that could be exploited.

Panoptica helps to discover API endpoints and analyzes and scores OpenAPI/REST-based APIs from a security perspective. It monitors the APIs for security vulnerabilities at runtime. It supports declarative policies to govern which API calls the gateway will permit and disable risky APIs that do not adhere to specifications.

Panoptica should be considered by organizations looking for an integrated CNAPP solution covering the full cloud stack and with strong cross-platform capabilities.



<b>Security</b>	strong positive	
<b>Functionality</b>	positive	
<b>Deployment</b>	strong positive	
<b>Interoperability</b>	positive	
<b>Usability</b>	strong positive	

Table 5: Cisco's rating

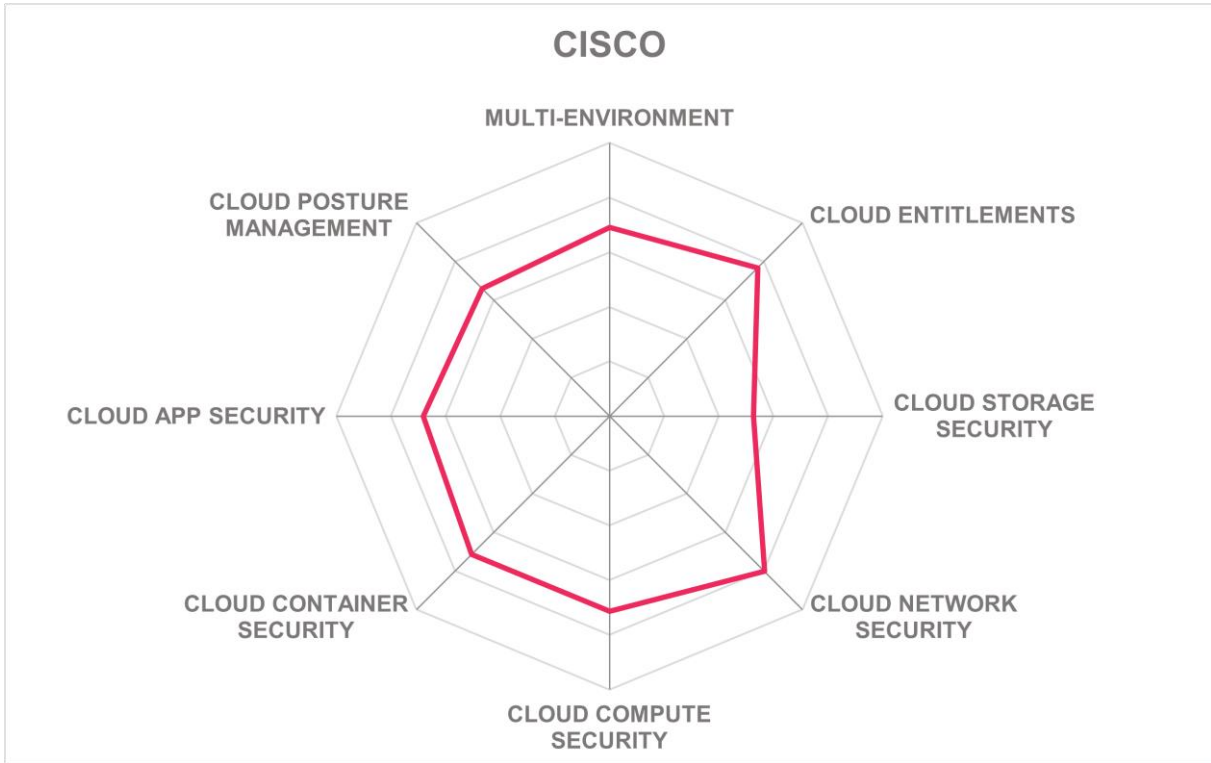
### Strengths

- Provides a complete, integrated CNAPP platform and tools.
- Capabilities include scanning, monitoring, and remediating risks, and compliance issues across public and hybrid multi-cloud environments.
- Integrated capabilities cover security risks across the full cloud stack.
- Provides a cohesive and prioritized view of threats, vulnerabilities, and compliance issues.
- Covers major public IaaS clouds including AWS, Azure, Google Cloud, and Oracle OCI.
- Identifies risks related to IaC tools such as Terraform.
- Discovers and analyzes the security of a wide range of cloud-native Kubernetes environments including AKS, EKS, GKS, OKS, OpenShift, Rancher, and Tanzu.
- Detects and prevents vulnerabilities in container images, functions, hosts as well as serverless implementations.
- Integrates with a wide range of CI/CD developer tools and pipelines.
- Supports drill down into common vulnerability exposures (CVEs) to identify the most urgent threats.
- The proprietary attack path analysis engine discovers exploitable attack vectors in the cloud stack.
- Analyzes and scores OpenAPI/REST-based APIs from a security risk perspective.
- Includes predefined policy security best practices such as CIS, ISO 27001:2013, and NIST CSF.
- Includes predefined templates to audit posture against a broad range of regulations such as HIPAA, and PCI-DSS.

### Challenges

- Cannot discover cloud accounts with weak credentials.
- Does not deal with cloud-based DBMS storage security vulnerabilities.
- Will not detect anti-malware missing or not running on servers. However, it does scan for and detect malware on computing assets.
- Depends upon XDR to cover the detection of many threats.
- Does not include capabilities to scan application code for vulnerabilities.

Leader in



## CloudDefense.AI – ACS Cloud Security

CloudDefense.AI was founded in 2020 and provides solutions to help enterprises protect their cloud applications and infrastructure from cyber-attacks. It has its headquarters in Palo Alto, California with development centers in India, UK, and USA. It provides products that cover cloud security and application security.

Cloud Defense.AI offers two major products, these are CloudDefense ACS Cloud Security and CloudDefense DevSecOps. Both are delivered as SaaS (Software as a Service).

Cloud Defense ACS Cloud Security capabilities cover Cloud Security Posture Management (CSPM), Cloud Infrastructure Entitlement Management (CIEM), Cloud Workload Protection (CWP), Kubernetes Security Posture Management (KSPM), and threat detection with automated remediation. It is based on an identity-first approach to cloud security and provides automated risk assessment, prioritization, and recommended remediation.

Cloud Defense ACS Cloud Security can detect and manage cloud vulnerabilities and misconfigurations with real-time anomaly detection. To provide context around security incidents, it supports a contextual security graph that helps to highlight the misconfiguration and vulnerabilities that require immediate action. The platform assigns tags and risk scores to all vulnerabilities identified. These help organizations prioritize which security issues to address first. It includes AI-driven remediation techniques to help to accelerate corrective actions.

Its CIEM capabilities provide insight into net-effective permissions across multiple clouds to help to detect and correct excessive permissions. It offers insights into dependencies between users, resources, and policies and gives automated suggestions to achieve the least privilege permissions.

Its CWP and KSPM capabilities provide continuous scanning for critical risks across various components like Virtual Machines, Containers, Serverless workloads, and Kubernetes clusters. These risks include vulnerabilities, exposure of sensitive data, presence of malware or secrets, and potential compliance misconfigurations.

CloudDefense DevSecOps provides unified threat intelligence across all attack surfaces for applications. This includes Software Composition Analysis (SCA), Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) as well as for APIs and containers. It can identify security vulnerabilities categorized by their risk calculated using multiple factors. This platform is extensible with webhooks to integrate with any workflow. CloudDefense.AI claims that its scanner is up to three times faster than competitive tools.

CloudDefense.AI provides cloud security solutions with a strong focus on secure cloud-based DevOps.

---

<b>Security</b>	strong positive
-----------------	-----------------

---

<b>Functionality</b>	positive	
<b>Deployment</b>	strong positive	
<b>Interoperability</b>	neutral	
<b>Usability</b>	positive	

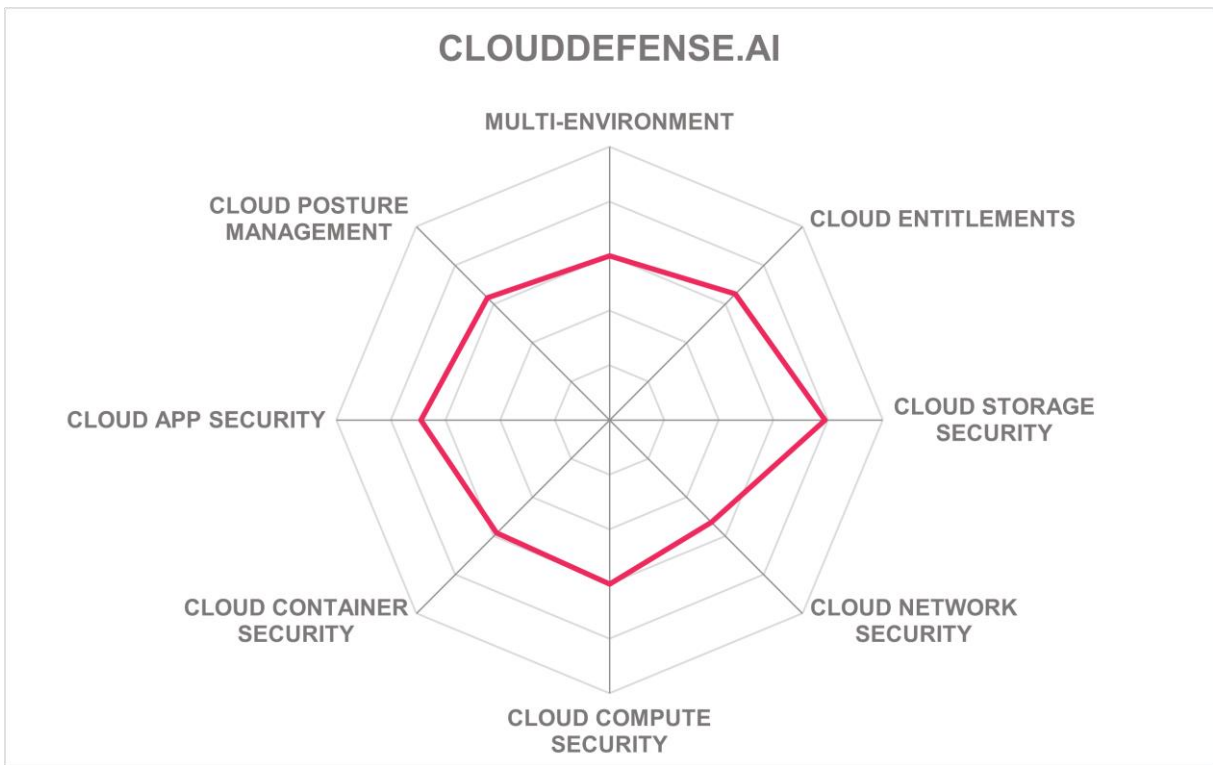
Table 6: CloudDefense.AI's rating

### Strengths

- Provides capabilities to detect and identify excessive privileges and other entitlement-based risks.
- Detects storage related vulnerabilities such as internet exposed storage for a wide range of cloud storage services.
- Capabilities cover a wide range of risks impacting compute service elements.
- Detection of risky configurations within compute OS environments.
- Supports securing Kubernetes environments AWS EKS and Microsoft Azure AKS.
- Provide visibility into the full container and orchestration asset inventory.
- Can identify known vulnerabilities in third-party tools and open-source libraries.
- Provides capabilities to analyze the security of the container registry for security risks.
- Integrates with a wide range of developer CI/CD pipelines.
- Provides capabilities to analyze a wide range of image package types for security vulnerabilities and risks.
- Includes incident management and response capabilities.
- Competitive pricing.

### Challenges

- Customers are mainly in the US, UK, and India.
- Extending the range of cloud services covered.
- Extending integration with a wider range of SIEM platforms.
- No support for modern secure communications protocols such as TLS 1.3.
- Lack of in-depth analysis of risks within the customers' cloud service network.
- No support for compute environments beyond Linux.
- No integrations with third-party incident response tools.



## CrowdStrike – Falcon Cloud Security

CrowdStrike Holdings, Inc. is a global cybersecurity company, providing modern security with advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity, and data. This report focuses on the Falcon Cloud Security modules covering CSPM, CIEM, and CWPP. These are offered as SaaS and offer both agentless deployment with extended agent-based capabilities and feature a graphical user interface.

Falcon Cloud Security discovers and provides threat intelligence, detection and response, workload runtime protection and cloud security posture management as well as container and Kubernetes protection across AWS, Azure, and Google clouds. These services are automatically configured when the services are deployed and compared against industry benchmarks and best practices. It can identify risks such as misconfigurations, public workloads, and unauthorized modifications. It includes guided remediation and provides guardrails against future mistakes.

Furthermore, it uses the capabilities provided by the CrowdStrike Falcon Platform operating in concert with the cloud-native security services to provide protection and detection that covers everything from the cloud control plane to cloud run-time. Together, these functions provide visibility, detect misconfigurations and anomalous behavior, and offer appropriate guidance to reduce attack surfaces in response to threats.

Falcon Cloud Security also provides complete visibility into the container images hosted in the cloud, helping to find hidden malware, embedded secrets, and vulnerabilities from libraries. It integrates with the CI/CD pipeline to help prevent misconfigured containers from deploying without the need for complex Rego rules. It features Kubernetes Operator and Helm Charts to provide ease-of-use based on familiar tools. Likewise, it integrates with native cloud tools as well as GitHub, Jenkins, and other build tools to support secure DevOps.

In addition, it will monitor storage to detect risks from public access permissions and data exposed to the internet. It can also monitor database instances to verify that high availability, backups, and encryption are enabled.

Falcon Cloud Security gives visibility into cloud resources, and the relationships between resources, access, and permissions through the CrowdStrike Asset Graph. It covers risks related to the security of identities associated with the resources and is analyzed through the integrated Cloud Infrastructure Entitlement Management (CIEM) capability. It can help to identify and remediate excessive account permissions and integrates with Microsoft Azure Active Directory as the identity provider. Entitlement modeling is supported to uncover and help to minimize risks from excessive entitlement combinations.

Falcon Cloud Security delivers streamlined, automated compliance and governance across multi-cloud environments to pinpoint their weak spots. It helps organizations assess their cloud environments against industry standards across built-in frameworks such as CIS, PCI, NIST, and HIPAA to understand their compliance posture. Along with the individual findings,

CrowdStrike Falcon Cloud Security provides the remediation steps, alert logic and MITRE ATT&CK information for each policy to enable rapid response to issues.

Organizations looking for CSPM, CWPP, and CIEM as well as EASM and ASPM capabilities as part of a comprehensive security portfolio with strong XDR capabilities should consider CrowdStrike Falcon Cloud Security.

<b>Security</b>	strong positive
<b>Functionality</b>	positive
<b>Deployment</b>	strong positive
<b>Interoperability</b>	positive
<b>Usability</b>	strong positive



Table 7: CrowdStrike's rating

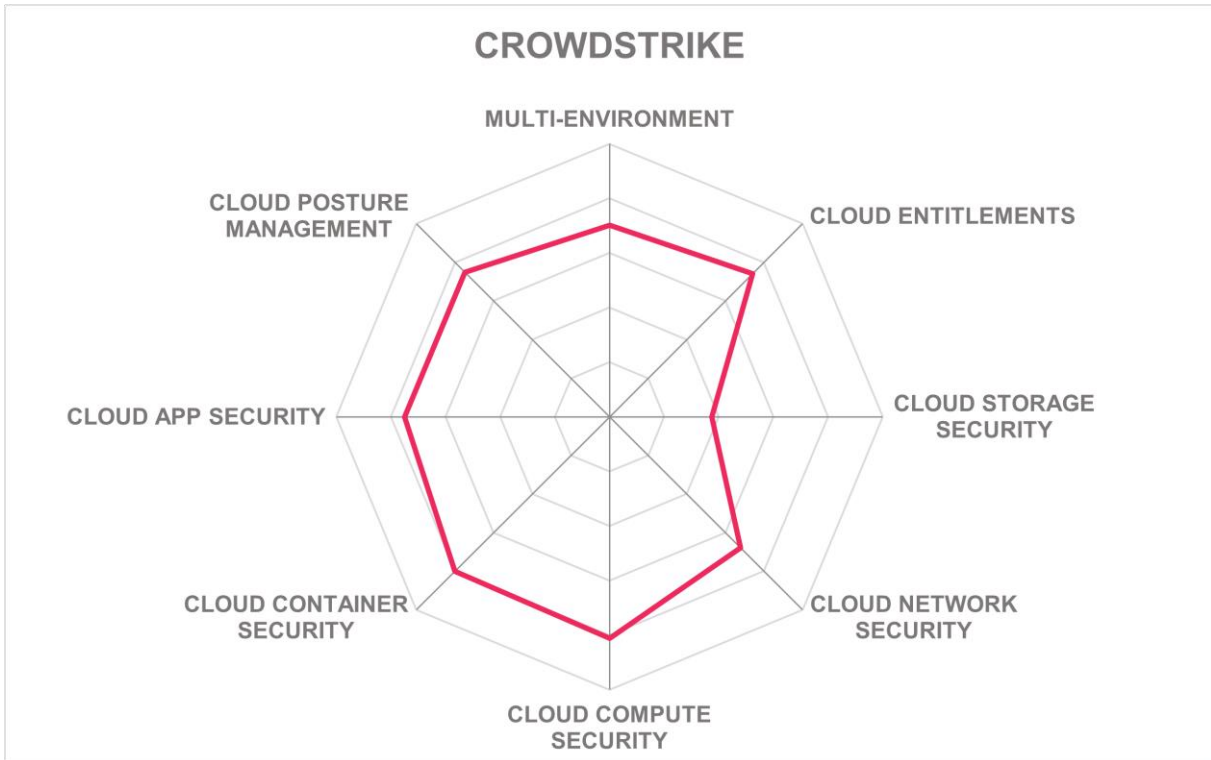
### Strengths

- Provides an integrated graphical representation of cloud service elements, topology, and risks in context.
- Detects risks related to users and excessive entitlements.
- Visualizes entitlement paths to show potential attack paths.
- Detects misconfigurations in cloud service elements including compute, network, and storage.
- Detects risks related to CVEs and misconfigurations in hosts and containers.
- Support integrations with a wide range of developer CI/CD pipelines.
- Built-in SBOM enumerates the software and creates a list of related vulnerabilities.
- Identifies misconfigurations, embedded secrets, and other violations of security policies in images.
- Detects Container drift (modifications to executables in production).
- Includes incident management and response capabilities.
- Detects risks related to storage elements including public access, lack of encryption and backup.
- Integrated XDR capabilities provide threat detection and response.
- Out-of-the-box audit reports covering a wide range of security best practices and compliance frameworks.
- Open APIs for ease of integration.

### Challenges

- Support and documentation only available in English and Japanese.
- Integration with Identity Providers limited to Microsoft Active Directory and AWS IAM
- Does not cover the risks related to the management of TLS certificates.
- Agents are required for some environments.
- Cannot detect storage such as S3 that is not encrypted or is exposed to the internet.

Leader in





## IBM – Security and Compliance Center

IBM Corporation is a multinational technology and consulting company headquartered in Armonk, New York. With over one hundred years of history, IBM has evolved from a computing hardware manufacturer toward offering a broad range of software solutions and infrastructure, hosting, and consulting services in such high-value markets as business intelligence, data analytics, cloud computing, virtualization, and information security.

Recently, IBM has expanded IBM Security and Compliance Center (SCC) to a solution suite that combines security, risk management, and compliance capabilities to serve the needs of multiple stakeholders within an enterprise. This approach not only improves coverage and efficiency but establishes a central cross-team collaboration place for all security and compliance monitoring and management across hybrid multi-cloud environments.

The platform comprises a range of Cloud-Native Application Protection Platform (CNAPP) capabilities. These include Cloud Security Posture Management (CSPM) to provide visibility into cloud resources, discover vulnerabilities and misconfigurations, and apply compliance controls across multi-cloud and hybrid environments. Cloud Infrastructure Entitlement Management (CIEM) is included to govern and audit cloud identities and manage permissions, optimize access policies, and enforce regulatory requirements.

Cloud Workload Protection (CWPP) provides runtime monitoring and protection for servers, containers, and Kubernetes clusters along with forensics and incident response for detected threats. Cloud Detection and Response (CDR) extends security controls to native cloud services, providing visibility and detection of suspicious activities across clouds. Automation and integration capabilities are present at every stage of the lifecycle: from initial deployment to CI/CD development pipelines to runtime prevention and blocking of risky activities.

IBM positions SCC's capabilities as going beyond a pure-play CNAPP platform to offer an open, flexible solution suite that can perform the above capabilities across hybrid, multi-cloud environments in an organic, integrated manner. Based on a technology-agnostic declarative framework, comprising a range of IBM's own and third-party technologies (for example, the container security stack is based on the open-source Falco project by Sysdig) and open for further third-party integrations, the platform can address the requirements of a wide range of different customer groups.

Running natively on the IBM Cloud, SCC is built directly into the cloud's management console and can be enabled with just a few clicks, providing a fully managed turn-key solution for all enterprises. To enable multi-cloud coverage, an instance of SCC Workload Protection service must be deployed and can be leveraged across cloud providers (AWS, Azure, etc.).

IBM says that additional types of integrations are planned for future releases, such as connectors to existing SIEM and XDR deployments, as well as support for watsonx.ai services. Customers are not forced to pay for capabilities they do not need or already have, which makes SCC more appealing to large enterprises with existing tools they do not need to rip and replace.

Organizations in regulated industries looking for a CNAPP solutions that covers a wide range of environments and needs should consider IBM Security and Compliance Center.

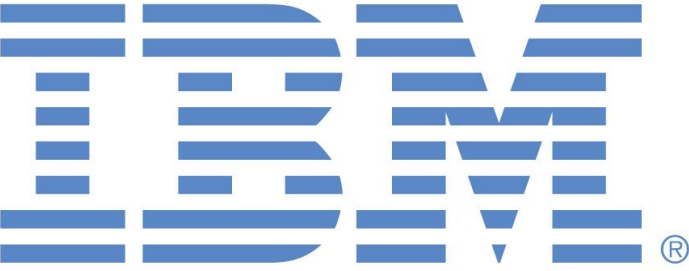
<b>Security</b>	strong positive	
<b>Functionality</b>	strong positive	
<b>Deployment</b>	strong positive	
<b>Interoperability</b>	strong positive	
<b>Usability</b>	strong positive	

Table 8: IBM's rating

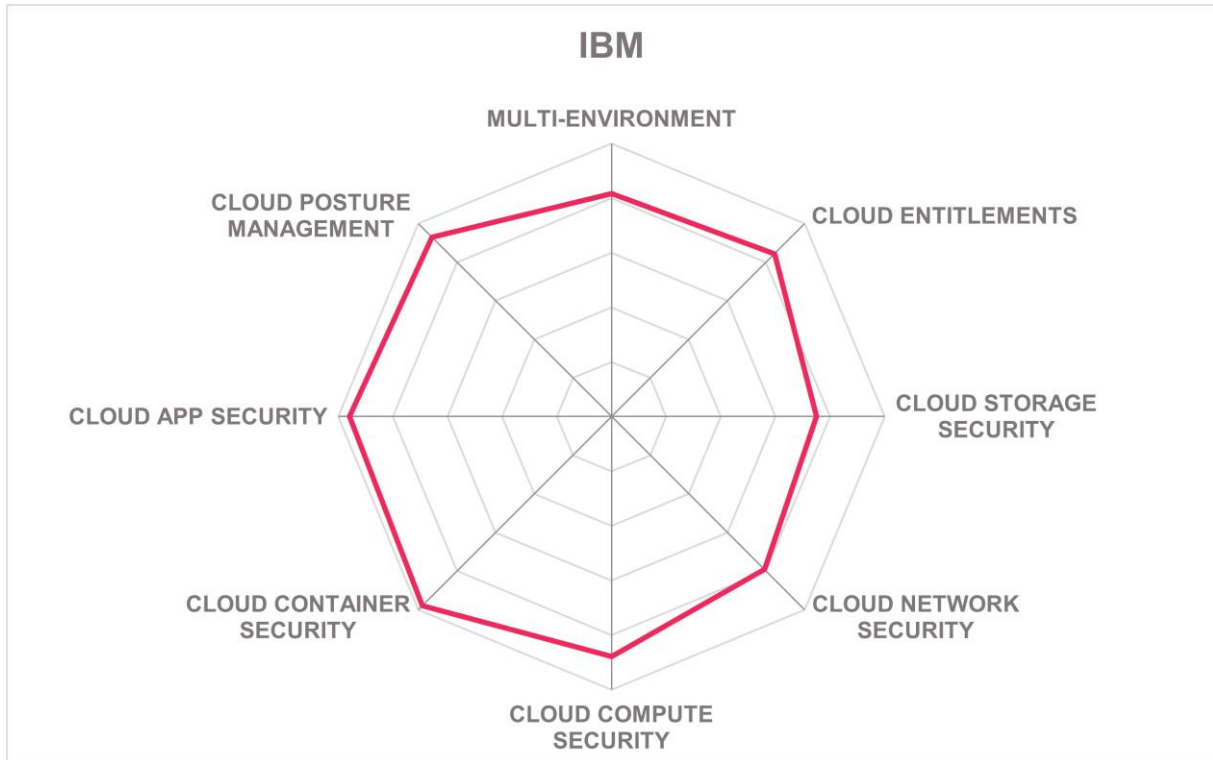
### Strengths

- A single unified platform designed for managing security and compliance controls across hybrid multi-cloud environments.
- Based upon a technology-agnostic compliance framework designed by IBM together with regulated industry professionals.
- Supports the IBM Cloud Framework for Financial Services, a set of control requirements designed to address the security and regulatory compliance obligations of financial institutions.
- AI ICT guardrails providing a pre-defined profile of infrastructure and related data controls, required to manage AI and Generative AI workloads.
- Instant deployment on IBM Cloud; can be quickly extended to other cloud providers.
- Large library of prepackaged compliance profiles: with controls, guidelines, documentation.
- Open architecture supporting third-party integrations and flexible pricing: turn-key or build-your-own deployments are possible.
- Automation and orchestration capabilities across systems and environments.
- Protection of critical hybrid multi-cloud workloads with prioritization of vulnerabilities in use and real-time threat detection.
- Provides deployable reference architectures and support for Policy-as-Code to accelerate secure cloud-native application development and deployment.
- Helps to automate CI/CD pipeline, block vulnerabilities in before production and investigate suspicious activity with real-time visibility by detecting and prevent drift across applications.
- Can help to protect data in cloud data stores and shield sensitive data with centralized encryption policies and auditing of data access across different data sources.
- Provides integration with GRC solutions for risk assessment and management including visibility into third- and fourth-party risk posture.

### Challenges

- Yet to deliver the full feature set to enable the strategic vision of the framework.
- Fully managed SaaS experience only available on IBM Cloud.
- Expanding data protection capabilities across multiple DB engines is still in progress.

Leader in



## Lacework – Cloud-Native Application Protection Platform

Lacework is a cloud security solution provider based in Mountain View, California, which was founded in 2015. The Lacework Cloud-Native Application Protection Platform helps organizations secure their use of cloud services by continuously monitoring and protecting cloud-native applications. It is designed to correlate data from across the customer's entire cloud life cycle to secure the apps and the cloud infrastructure they use from build time through runtime.

It features the Polygraph Data Security Platform, a data-driven cloud security architecture designed to ingest massive amounts of cloud telemetry across public cloud and container environments, uncover threats, anomalies, vulnerabilities, and misconfigurations by applying patented machine learning and behavioral analytics.

Lacework CNAPP includes Code Security, Cloud Workload Protection, Cloud Security Posture Management, Cloud Infrastructure Entitlement Management, Attack Path Analysis, Kubernetes Security, Container Security, Compliance, Host intrusion Detection, and Behavioral Analytics Visibility across multi-cloud environments.

In October 2023, Lacework announced expanded multi-cloud support to now include Oracle Cloud Infrastructure (OCI), two new ServiceNow container and infrastructure vulnerability response applications, and attack path visualization and analysis for Azure environments. Lacework agentless workload scanning now checks workloads every five minutes for a more continuous view of resources and their associated risks. New Lacework Windows vulnerability management capabilities can detect vulnerabilities in Windows operating systems to help secure "lift and shift" applications moved to the cloud. While new custom framework capabilities make it easier to operationalize and manage custom security requirements.

For containerized workloads, the platform provides full visibility and tracking from container image to container instances across a wide variety of infrastructures. This includes build-time software vulnerability risks, continuous runtime vulnerability risks, infrastructure and network visibility, and runtime behavior tracking.

Lacework supports a wide range of developer environments and package types for both container images and host-based applications. In addition, the Lacework agent reports which packages are in use by the application at runtime to minimize wasted effort for vulnerable application dependencies that are included, but unused, by developers.

The Lacework Polygraph machine learning engine automatically learns the activities and behaviors that are unique to container and cloud environments and surfaces unexpected changes, along with full context to make investigations quick and easy. Lacework states that through the consolidation of multiple tools into a single platform and a 95% reduction in false positives, the platform promises to achieve up to 80% reduction in root cause and investigation times for security analysts.

Dynamically calculated risk scores for each event and artifact related to it provide a consistent method of quantifying container risks and then defining thresholds that would prevent vulnerable or compromised images from deployment to production.

Organizations looking for a unified CNAPP that is based on machine learning and data correlation should consider Lacework CNAPP.

<b>Security</b>	strong positive	
<b>Functionality</b>	strong positive	
<b>Deployment</b>	strong positive	
<b>Interoperability</b>	strong positive	
<b>Usability</b>	strong positive	

Table 9: Lacework's rating

### Strengths

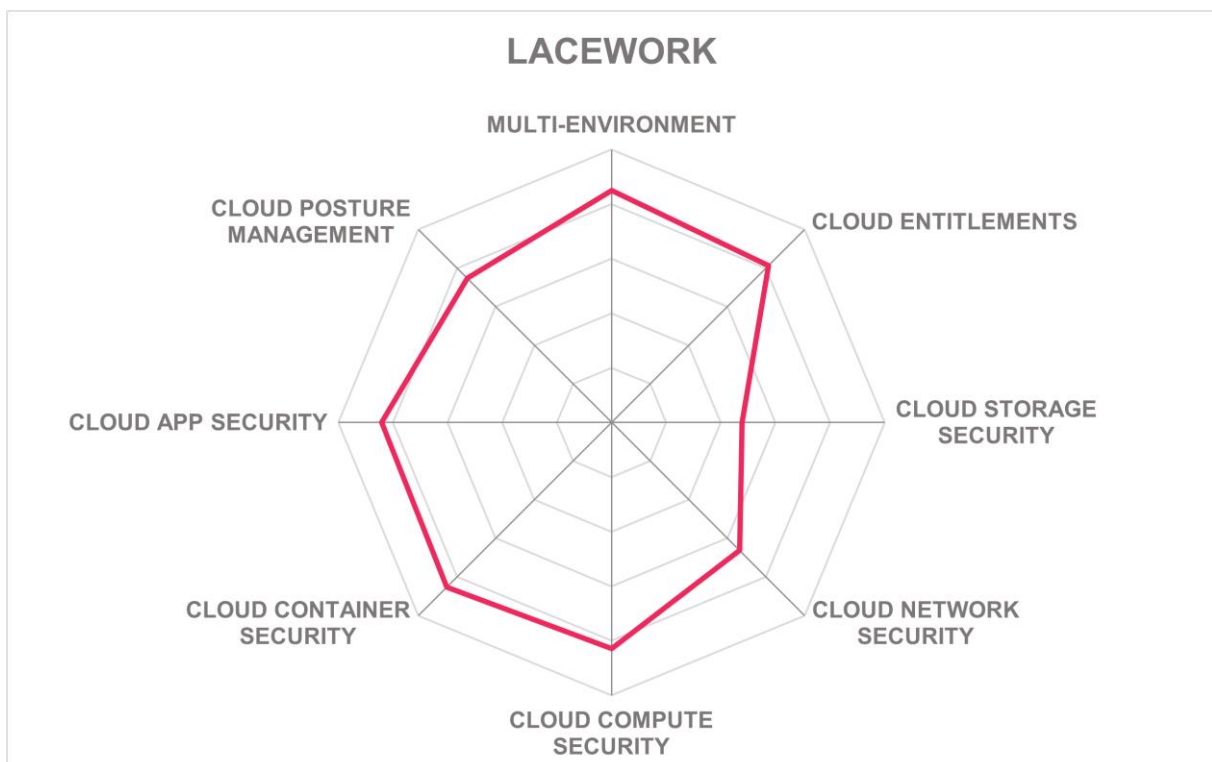
- Provides a comprehensive CNAPP platform.
- Easy to deploy as an agentless SaaS. Optional agents provide in-depth insight into running hosts and containers.
- Unifies code and cloud security with native software composition analysis (SCA), software bill of material (SBOM), Static Application Security Testing (SAST) and Infrastructure as Code (IaC) scanning.
- Provides a central management console for visibility and posture management across Amazon Web Services (AWS), Google Cloud, Azure, and OCI deployments.
- Polygraph provides rapid detection of potentially risky activities based on behavioral baseline of normal operations for cloud workloads.
- Prioritizes risks by correlating multiple factors and events from disparate sources to create highly contextualized alerts.
- Features behavioral-based threat detection that does not require rules and claims to be effective at detecting zero-day vulnerabilities.
- Analyzes a wide range of package types for security vulnerabilities and risks.
- Integrates with a wide range of CI/CD developer tools and pipelines.
- Measures the security posture of Kubernetes environments and detects anomalies via Kubernetes Audit Logs, in both EKS and GKE.
- Covers DevOps Risks through container and registry scanning, and the Kubernetes admission controller.
- Continuously monitors security risks related to user and service identities and entitlements, including excessive entitlements and orphan accounts.
- Assesses risk of stored secrets and data exposed to the internet via agentless workload scanning.
- Takes a “private by design” approach to agentless workload scanning that ensures customer data never leaves their account.
- Attack path analysis capabilities assess risks based on internet path exposure, vulnerabilities, misconfigurations, exposed secrets, and privileged access.

- Detects known vulnerabilities and exposures in compute service elements.
- Continuously monitors runtime package activity to identify active vs inactive packages and assess vulnerabilities in terms of risk within a specific customer environment.
- Integrates with a wide range of common SIEM and workflow / incident management platforms.

### Challenges

- No risk detection for the configuration of virtual network routing control points such as firewalls.
- Does not detect missing / inoperative anti-malware on servers.
- Cannot identify risks related to poor certificate management.

Leader in



## Microsoft – Defender for Cloud

Microsoft Corporation is a multinational technology company with headquarters in Redmond, Washington. It is best known for its software products, such as the Windows operating systems and the Microsoft Office suite. It also offers Microsoft Azure, which is a cloud computing platform, as well as multi-cloud cybersecurity tools. This report focuses on Microsoft Defender for Cloud.

Microsoft Defender for Cloud is a Cloud-Native Application Protection Platform (CNAPP) that helps protect cloud-based applications from various cyber threats and vulnerabilities. It includes many subcomponents including Defender CSPM including DevOps Security, Defender for Containers, Defender for Servers, Defender for DevOps, Defender for Storage, Defender for Azure SQL, and Defender for SQL servers and machines. This solution is part of Microsoft's vision to provide vulnerability, risk, and posture management capabilities across the whole enterprise IT estate, building on top of the cloud security graph and expanding to other organizational signals.

Microsoft Defender for Cloud provides multi-cloud posture management capabilities including agentless vulnerability scanning, container image scanning, attack path analysis, integrated data-aware security posture, and an intelligent cloud security graph with code to cloud remediation workflows. These capabilities cover AWS and Google Cloud, as well as Microsoft Azure. The solution features the Microsoft cloud security benchmark as a built-in standard, providing detailed technical guidance for Azure as well as other cloud providers.

Microsoft Entra Permissions Management helps to expose cloud infrastructure entitlements, prevent permissions creep, and enforce the principle of least privilege across the multi-cloud environment. Defender for Cloud integrates with Entra Permissions Management, providing unified visibility and recommendations in a central cloud security dashboard.

The CWPP capabilities of Microsoft Defender for Cloud cover file integrity monitoring, vulnerability assessment for servers and adaptive controls for network and application hardening. Defender for Cloud also protects managed and unmanaged database engines, containerized environments, and additional workload types according to their attack surface and security risks. It also offers near real-time malware scanning across file types to detect polymorphic and metamorphic malware upon content upload.

It supports securing code by providing capabilities to protect applications and resources from code to cloud across multi-pipeline environments, including GitHub, Git Lab, and Azure DevOps. These findings, such as IaC (Infrastructure as Code) misconfigurations and exposed secrets, can then be correlated with other contextual cloud security insights to prioritize remediation in code.

It provides a visual map of the cloud environment that can be queried to find security risks. This also provides attack path modelling capabilities for the network to help to identify potential risks and ensure that changes do not increase exposure.

Organizations looking for a CNAPP with a Microsoft focus which also provides multi-cloud capabilities including data aware security posture should consider Microsoft Defender for Cloud.

<b>Security</b>	strong positive	
<b>Functionality</b>	positive	
<b>Deployment</b>	strong positive	
<b>Interoperability</b>	strong positive	
<b>Usability</b>	strong positive	

Table 10: Microsoft's rating

### Strengths

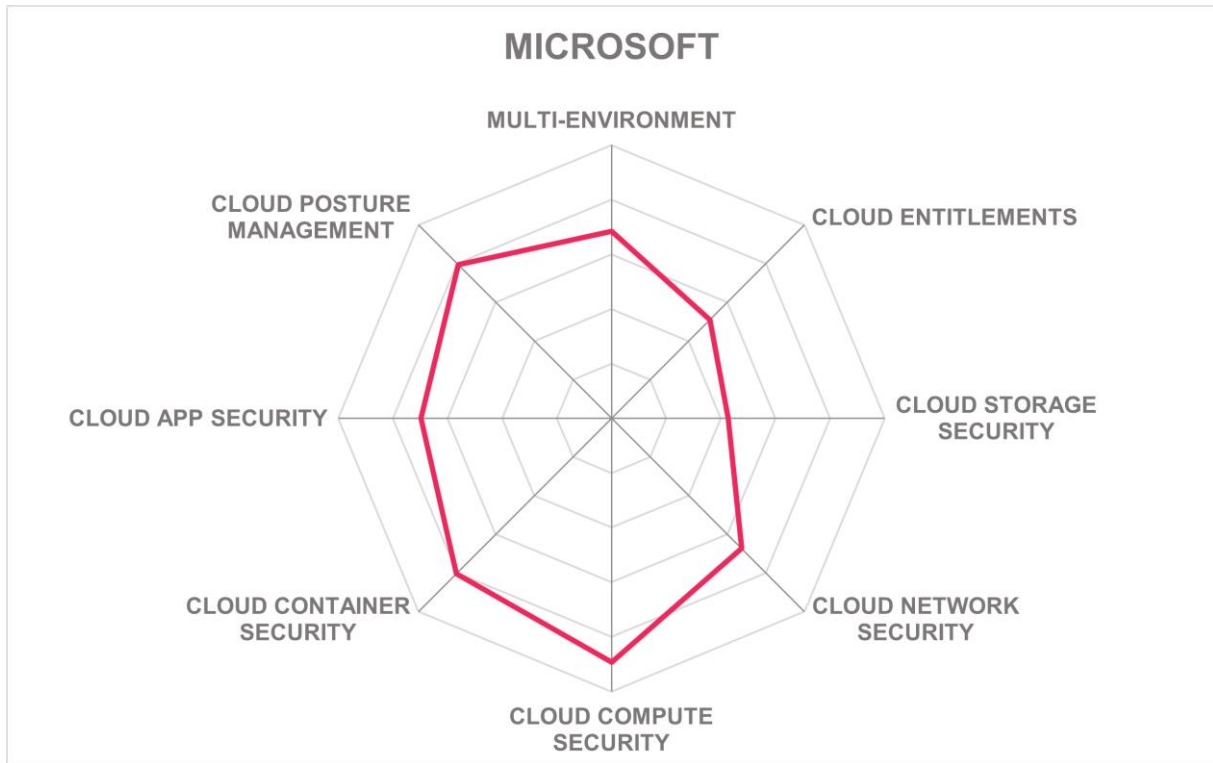
- Provides a complete CNAPP platform that covers Azure, AWS, and Google Cloud, with support for additional cloud providers planned.
- Supports automatic and agentless discovery of the cloud data estate, including managed and shadow data resources.
- Built-in integration with Defender External Attack Surface Management, Microsoft Entra Permissions Management and Microsoft Defender Vulnerability Management.
- Integrated into CI/CD tools to assess cloud workloads, containers, and IaC artifacts.
- Defender for Containers includes host-level threat detection with over 60 Kubernetes-aware analytics, AI, & anomaly detections based on the runtime workload.
- Risk evaluation and attack path analysis is based on a cloud security graph built from a wide variety of cloud feeds.
- AI-based automatic attack path algorithms identify potential attack paths and blast radius to identify and assess risk.
- Prioritizes misconfigurations, vulnerabilities, and assets based on their business criticality and risk.
- Built-in policies and controls based around the Microsoft cloud security benchmark.
- Out-of-the-box assessment of posture against a broad range of security best practices and regulatory compliance frameworks such as ISO/IEC 27001, MITRE ATT&CK, and PCI DSS as well as support for custom frameworks.

### Challenges

- Requires integration of multiple products (e.g., Microsoft Entra Permissions Management) for full functionality.
- Does not currently detect excessive cloud entitlements relative to policy and usage – but this is on the roadmap.
- No integrations with third-party identity solutions – the focus is on Microsoft Entra Permissions Management.
- Cannot identify misconfigurations, embedded secrets, and other violations of security policies in container Images.
- No SBOM (Software Bill of Materials) capabilities.



Leader in



## Orca Security – Orca Cloud Security Platform

Orca Security was founded in 2019 and has its headquarters in Portland, Oregon, with R&D in Israel. Orca Security offers a Cloud Security Platform that provides a zero-touch approach to cloud security.

This approach is made possible by Orca Security's patented SideScanning™ technology that provides visibility across an organization's cloud environment without the need for agents. Its context engine combines workload and cloud configuration details to build a unified data model and a visual map of all the organization's cloud assets across AWS, Azure, Google Cloud, Oracle Cloud Infrastructure (OCI), and Alibaba.

Orca Cloud Security Platform context engine combines the intelligence gathered from inside workloads, including the workload's host configurations (e.g., running services, and firewall configurations) together with cloud configuration details (e.g., IAM roles, VPCs, and security groups) to build a unified data model. This is used to build a graph-based map of the organization's cloud estate, providing visibility into the cloud assets and their relationships, as well as providing clear insight into which risks should be regarded as top priority.

Orca Cloud Security Platform performs a complete inventory of the customer's public cloud assets, including software inventories of cloud workloads. It also inventories assets on the customer's cloud infrastructure platform(s), including data and network assets such as storage buckets, security groups, cloud accounts, images, cloud services, and more.

To support DevOps security, Cloud Security Platform can scan both containers and Kubernetes for security risks, misconfigurations, and vulnerabilities. This includes (but is not limited to) a wide range of container related cloud orchestration platforms such as AKS, EKS, GKE, and Rancher. It integrates with a wide range of DevOps and DevSecOps CI/CD pipelines and processes to embed security into the application code as early as possible. It also provides threat intelligence, risk scoring, and mitigation recommendations based on data sensitivity, exposure, and quality.

Orca Cloud Security Platform detects, prioritizes, and continuously monitors common and obscure Identity and Access Management (IAM) misconfigurations across the organization's public cloud to meet IAM compliance obligations and to improve cloud security posture. In addition to poor password hygiene, Orca scans the organization's cloud for exposed keys, passwords in shell histories, vulnerabilities, and other information attackers can use to achieve unauthorized access.

Orca Cloud Security Platform enables organizations to detect and prioritize cloud security risks, such as misconfigurations, vulnerabilities, malware, compromised credentials, data leakage, and compliance violations. In addition, Orca also helps organizations to fulfill data subject rights, manage consent, conduct DPIAs, and notify data breaches under GDPR and other regulations.

Orca Cloud Security Platform should be considered by organizations looking for a comprehensive and innovative approach to CNAPP solution that includes strong entitlement management and data sensitivity considerations.

<b>Security</b>	positive	
<b>Functionality</b>	strong positive	
<b>Deployment</b>	strong positive	
<b>Interoperability</b>	positive	
<b>Usability</b>	positive	

Table 11: Orca Security's rating

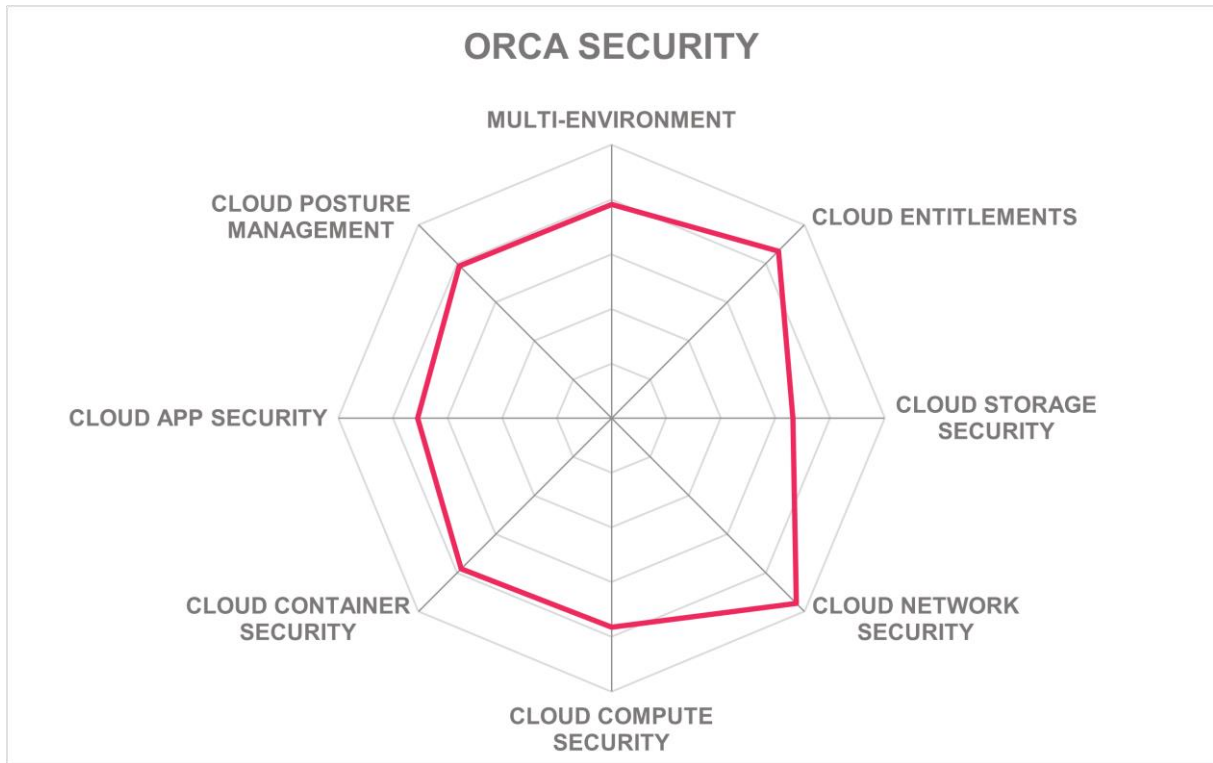
### Strengths

- Orca Security's patented SideScanning™ approach does not require agents and does not impact running workloads.
- Integrates with the Alibaba, AWS, Azure, Google, and Oracle OCI Cloud IaaS services.
- Monitors cloud infrastructure resources including storage buckets, security groups, VPCs, IAM roles and permissions, KMS keys, and more.
- Prioritizes risks based on the severity of the underlying security issue, its accessibility, and business impact to highlight the most critical issues.
- Remediation guidance is powered by multiple forms of GenAI. Integrates with Amazon Bedrock, Google Cloud Vertex AI, and Microsoft Azure ChatGPT.
- Monitors for risky Identity and Access Management (IAM) misconfigurations and provides capabilities to identify and remediate risky cloud entitlements.
- Leverages context-aware intelligence to detect vulnerabilities that could enable lateral movement.
- Discovers and analyzes the risks related to a wide range of cloud compute services owned by the customer.
- Detects malware across the cloud estate, including paused / idle workloads and orphaned VMs.
- Covers security risks in the major cloud Kubernetes orchestration platforms.
- Integrates with a wide range of developer CI/CD pipelines.
- Provides a complete inventory of all customer's cloud assets.
- Automatic scanning of cloud databases for PII exposure and compliance.
- Provides an automated API inventory, API exposure telemetry, and external exposure activity as part of the solution.
- Monitors over 1000 unique controls across 100+ compliance frameworks.
- Out-of-the-box third-party integrations, including a wide range of SIEM and workflow/incident management platforms.

### Challenges

- Support for SBOM (Software Bill of Materials) capabilities is still a roadmap item.
- No support for Red Hat OpenShift.
- Does not identify packages that are not known to CVE databases.

Leader in



## Palo Alto Networks – Prisma Cloud

Palo Alto Networks, founded in 2005 in Santa Clara, CA, is the pioneer in Next-Generation Firewall (NGFW) technology. Palo Alto Networks also offers an advanced Cloud-Native Application Protection Platform (CNAPP), automated SOC technology, and other network security products. This report focuses on the CNAPP capabilities offered by Prisma Cloud.

Prisma Cloud by Palo Alto Networks is a comprehensive CNAPP and in October 2023, Palo Alto announced the Prisma Cloud Darwin release. This release provides what Palo Alto Networks describes as “Code to Cloud Intelligence” and “AppDNA”: These features trace security issues back to their source in code, to help remediate risk at its origin.

Prisma Cloud provides a comprehensive inventory of cloud assets that includes detailed information about each asset, such as its configuration and security posture. It normalizes the data from each of the different cloud data sources to provide a consistent view of assets and their risks across clouds.

According to Palo Alto, AppDNA structures the inventory into an application-centric view that displays the cloud apps in their entirety covering the cloud services, infrastructure assets, compute workloads, API endpoints, data and code that make them up, together with business context, in one place.

Prisma Cloud supports multiple cloud platforms including Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure (OCI) IBM Cloud, and Alibaba Cloud. Its CSPM helps the customer to monitor their multi-cloud compliance posture and supports reporting from a single console. It covers over ninety compliance frameworks out-of-the-box, and the customer can add custom frameworks.

It provides context-based prioritization of risks. The platform analyzes misconfigurations, network exposures, excessive permissions, and vulnerabilities for combinations that create potential attack paths. This risk-based analysis uses the Prisma Cloud context engine to identify multiple vulnerabilities across a cloud that can be exploited in an attack.

Prisma Cloud Infinity Graph helps users to understand risks with context. It correlates the risks across the technology stack including misconfigurations, vulnerabilities, pipeline risks, exposure, identity and secrets, sensitive data, showing potential attack paths. The graph also overlays active attack attempts to show what is occurring and whether there is protection in place.

Prisma Cloud analyzes audit events using ML to detect anomalous activities that could indicate account compromises, insider threats, stolen access keys, and other potentially malicious user activities. It also uses ML to detect network anomalies and threats. It can detect port scan and port sweep activities that probe a server or host for open ports as well as threats hiding in DNS traffic, such as domain generation algorithm (DGA) and crypto mining activity.

Organizations looking for CNAPP capabilities delivered as part of a much wider integrated security platform and with excellent compliance monitoring capabilities should consider Palo Alto Networks Prisma Cloud.

<b>Security</b>	strong positive	
<b>Functionality</b>	strong positive	
<b>Deployment</b>	strong positive	
<b>Interoperability</b>	strong positive	
<b>Usability</b>	strong positive	

Table 12: Palo Alto Networks' rating

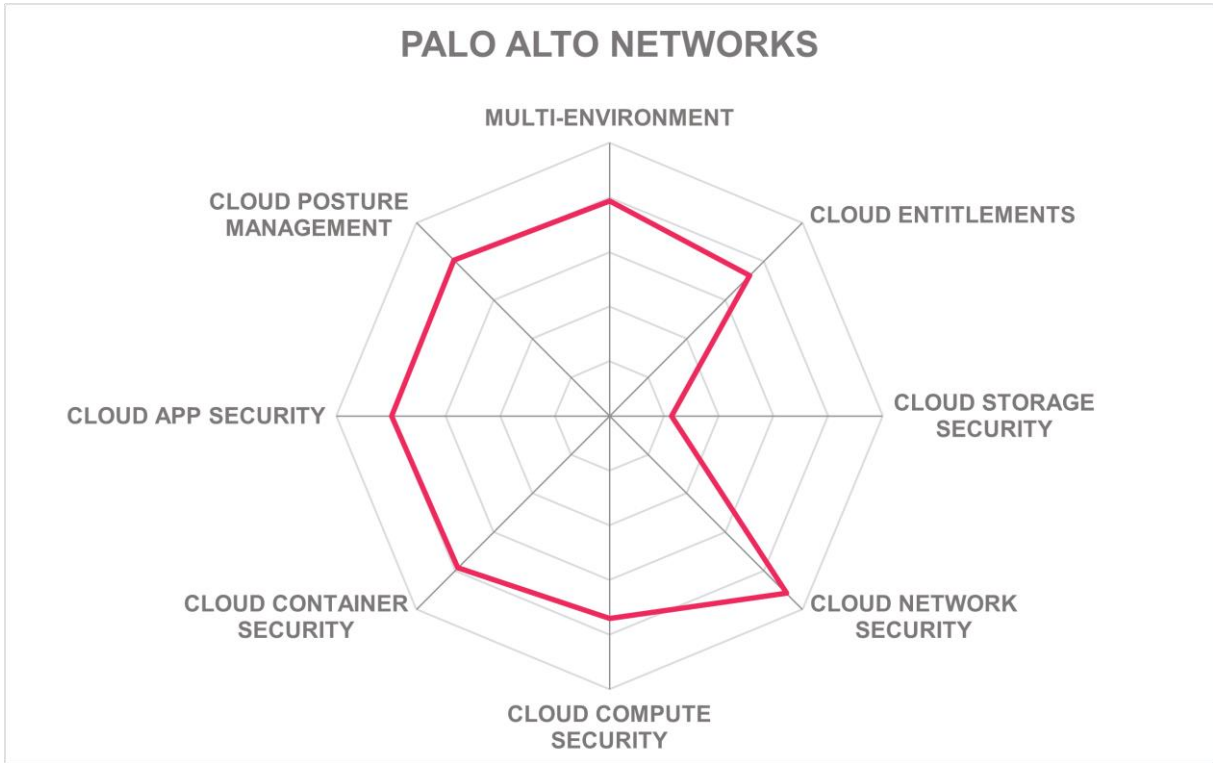
### Strengths

- Provides a complete, integrated CNAPP platform and tools that cover security risks in all cloud app elements from code to cloud.
- Covers all the major public IaaS clouds including Alibaba, AWS, Azure, Google Cloud, IBM Cloud, and Oracle OCI.
- Identifies risks related to IaC tools such as Terraform, CloudFormation, as well as Kubernetes YAMLS.
- Discovers and analyzes the security of a wide range of cloud-native Kubernetes environments including AKS, EKS, GKS, OKS, OpenShift, Rancher and Tanzu.
- Detects and prevents vulnerabilities in container images, functions, hosts as well as IaC templates.
- Analyzes a wide range of package types for security vulnerabilities and risks.
- Provides and integrates with a wide range of CI/CD developer tools and pipelines.
- Out-of-the-box policies that help to govern IAM best practices. These compute the net effective permissions a user has based on context.
- Helps to implement the least privilege micro-segmentation and cloud-native application and network firewalling in hybrid and multi-cloud environments.
- The inbuilt cloud network analyzer engine automatically calculates net effective reachability of cloud resources to detect exposed assets.
- Includes predefined policy security best practices such as CIS, ISO 27001:2013, MITRE ATT&CK, and NIST CSF.
- Includes predefined templates to audit posture against a broad range of regulations such as GDPR, HIPAA, HITRUST, PCI-DSS, and SOX.

### Challenges

- Requires subscription to multiple options to get the full benefits.
- Full data security capabilities depend upon Palo Alto Networks Enterprise DLP and Wildfire.
- Coverage of storage security risks is limited to AWS S3 and Azure Blob storage. Note that Palo Alto Networks recently acquired Dig Security that provides a DSPM solution.

Leader in



## Sysdig – Secure Platform

Sysdig was founded in 2013 and has its corporate HQ in San Francisco, CA in the USA, but nearly 45% of employees are outside the United States. It offers the Sysdig Secure CNAPP Platform which enables teams to secure builds, detect and respond to runtime threats, and continuously manage cloud configurations, permissions, and compliance.

Sysdig can be deployed as an agent based and agentless solution and uses API-based queries to access the managed environments. It supports AWS, Azure, Google Cloud, IBM Cloud, Oracle Cloud, Docker, Mirantis, Red Hat, SUSE Rancher, VMware Tanzu, and Kubernetes. Sysdig continuously manages cloud infrastructure and identity risks by identifying and enabling the remediation of misconfigurations in the cloud control plane, cloud resources, and cloud-deployed workloads. Sysdig also leverages runtime visibility from open-source Falco to detect threats across the entire cloud infrastructure and provides rich context for investigations and response by correlating relevant information across assets, users, and activity. Sysdig supports common frameworks, regulatory requirements, and internal company policies to assess target environments against security standards.

The platform can check cloud and Kubernetes environments against major compliance standards out-of-the-box, including PCI-DSS, NIST 800-53, CIS, SOC2, GDPR, and many more. It maps out of the box policies onto the relevant compliance frameworks, which are weighted as high, medium, or low. The overall compliance score is based on the weighted average, rather than the pass/fail result. This recognizes that not all compliance requirements represent equal risks and allows users to take risk-based decisions.

Enabling Policy as Code, it provides a wizard to create CSPM policies and controls, which generates Policy as Code in OPA (Open Policy Agent) based format. It maps cloud assets and resources to their IaC manifest files in various formats and compares these with the policies to detect and remediate any deviations.

Sysdig supports DevOps security by continuously evaluating IaC artifacts throughout the CI/CD pipeline and workload life cycle. It also analyzes the configuration of Kubernetes resources and exploits the Kubernetes Admission Controller to evaluate the risks associated with containerized workloads before deploying them to the cluster. With inventory, it allows customers to gain visibility and prioritize which resources require an immediate fix across cloud (Azure, AWS, and GCP) and Kubernetes. Inventory displays a searchable list of all resources from cloud accounts, Kubernetes data sources, and IaC Git resources connected to Sysdig, along with their compliance policy passing score.

It also offers CIEM capabilities to help customers get a comprehensive view into access permissions across AWS accounts, including ephemeral services such as Lambda functions; eliminate excessive permissions by applying least-privilege policies; and regularly perform access reviews to evaluate active and inactive user permissions and activity.

The Sysdig Platform should be considered by organizations looking for preventive and detective CNAPP capabilities, which also supports the investigative actions required when a security incident occurs.



<b>Security</b>	strong positive
<b>Functionality</b>	strong positive
<b>Deployment</b>	strong positive
<b>Interoperability</b>	strong positive
<b>Usability</b>	positive



Table 13: Sysdig's rating

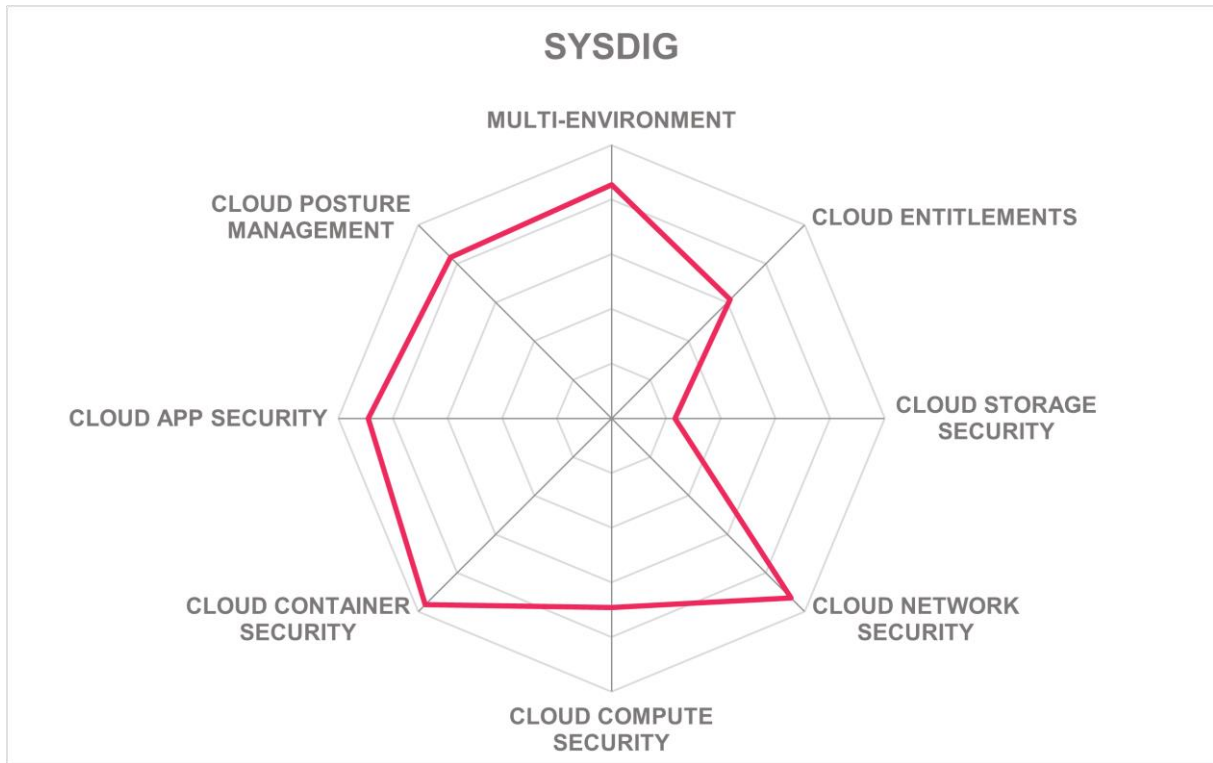
### Strengths

- Built on an open-source security stack, such as Falco and Open Policy Agent, which accelerates and drives standardization.
- It leverages the Cloud Attack Graph to correlate, contextualize, and prioritize data context from multiple domains to help to identify the real risks.
- End-to-end detection across containers, cloud services, Linux/Windows servers, identities, and third-party apps, including the ability to detect and rapidly alert to an attack.
- Multi-layered detection approach leveraging Falco rules, ML, and drift detection, curated by the Sysdig Threat Research team.
- Captures detailed user and system activity including commands, network connections, file activity, and process lineage for forensic investigation.
- Provides a single view of vulnerability risk across the container lifecycle, from build through detection and response.
- Provides rich vulnerability details - such as the CVSS vector from multiple sources including the fix version, and link to publicly available exploits.
- Runtime intelligence, known as runtime insights, helps to identify vulnerabilities that are tied to packages used at runtime to help prioritize the vulnerabilities that matter, as well as to recognize posture drift in real-time as it occurs, rather than at the next scan.
- Shared policy model, which allows teams to consistently enforce policies across multiple cloud and Kubernetes environments.
- The shared policy model is agnostic to the state, to where in the pipeline it is being checked, and to the language being used.
- Remediation Guru, which provides remediation fixes at the source to allow security and DevOps teams to solve issues more quickly.

### Challenges

- No support for Azure Active Directory or other major identity providers, although Azure and Okta IdP support is on the roadmap.
- Does not currently support Oracle OCI and OpenStack compute service risks.
- Cannot detect risks related to users / service accounts without a physical owner (orphan accounts).

Leader in



## Uptycs – Hybrid Cloud Security Platform

Uptycs is a venture funded technology company that was founded in 2016 and has its headquarters in Waltham, Massachusetts. Their CNAPP provides unified security for hybrid multi-cloud, Kubernetes, and connected development environments, including developer workstations.

The Uptycs platform incorporates cloud workload protection, cloud security posture management, cloud infrastructure entitlements management, Kubernetes and container security, and cloud detection, investigation, and remediation. It is intended to help organizations make better risk decisions about vulnerabilities and threats derived from signals emanating from a large volume and variety of security and IT data. It enables customers to better protect their digital assets spread across their hybrid IT infrastructure, and to reduce mean time to detection and mean time to mitigation against attacks by eliminating tool, team, and infrastructure silos.

The solution offers a continuously updated cloud inventory that includes the configuration details for resources from AWS, Azure, and Google Cloud with real-time detection of changes. It provides a consistent graphical interface to view and query resources and their security status across the multiple cloud provider accounts and services. This includes visualization of the relationships between resources and events to provide a context in which to judge risks, including visualizing the potential blast radius of a breached developer laptop.

Uptycs provides permission gap analysis and identity mapping to see which assets an identity has access to, which permissions are granted to them, and which of those are being used. This helps to establish the least-privilege Zero Trust approach.

It provides visibility and control across all workloads, covering hosts, VMs, containers, micro VMs, and serverless functions to support secure DevOps and enable Kubernetes security posture management (KSPM). This provides visibility into the vulnerabilities and compliance of images, containers, pods, and hosts across Google GKE, AWS EKS, Azure AKS, Kubernetes, OpenShift, VMware Tanzu, and Google Anthos. It integrates with the CI pipeline and includes an embedded Open Policy Agent (OPA) gatekeeper supporting enforcement as well as auditing.

Uptycs features out-of-the-box rules to help organizations audit their cloud resource configurations against a wide range of security benchmarks and regulatory frameworks. These include CIS Benchmarks, PCI-DSS, AWS Well-Architected Framework, HIPAA, HITRUST, NSA Hardening, ISO 2700, FedRAMP, SOC 2 and more. It provides overview dashboards that provide a visual summary of compliance with the capability to drill down to root causes and to track how compliance has changed over time.

The platform also offers capabilities to detect and investigate threats. This includes in-depth analysis of cloud identity activity, providing insights into access patterns as well as suspicious behavior. It can also detect, and map attack techniques and sub-techniques described by MITRE ATT&CK to provide security analysts with a better context during triage and investigations. It provides the ability to remediate security issues at the workload level. Remediation spans manual steps to fully automated options. The depth of workload

remediation includes process level blocking within containers, killing specific workloads, shutting down network activity, and more.

Organizations looking for a complete CNAPP to cover hybrid multi-cloud environments, Kubernetes infrastructure, and software supply chain security should consider Uptycs Hybrid Cloud Security Platform.

<b>Security</b>	positive
<b>Functionality</b>	strong positive
<b>Deployment</b>	strong positive
<b>Interoperability</b>	strong positive
<b>Usability</b>	positive



Table 14: Uptycs' rating

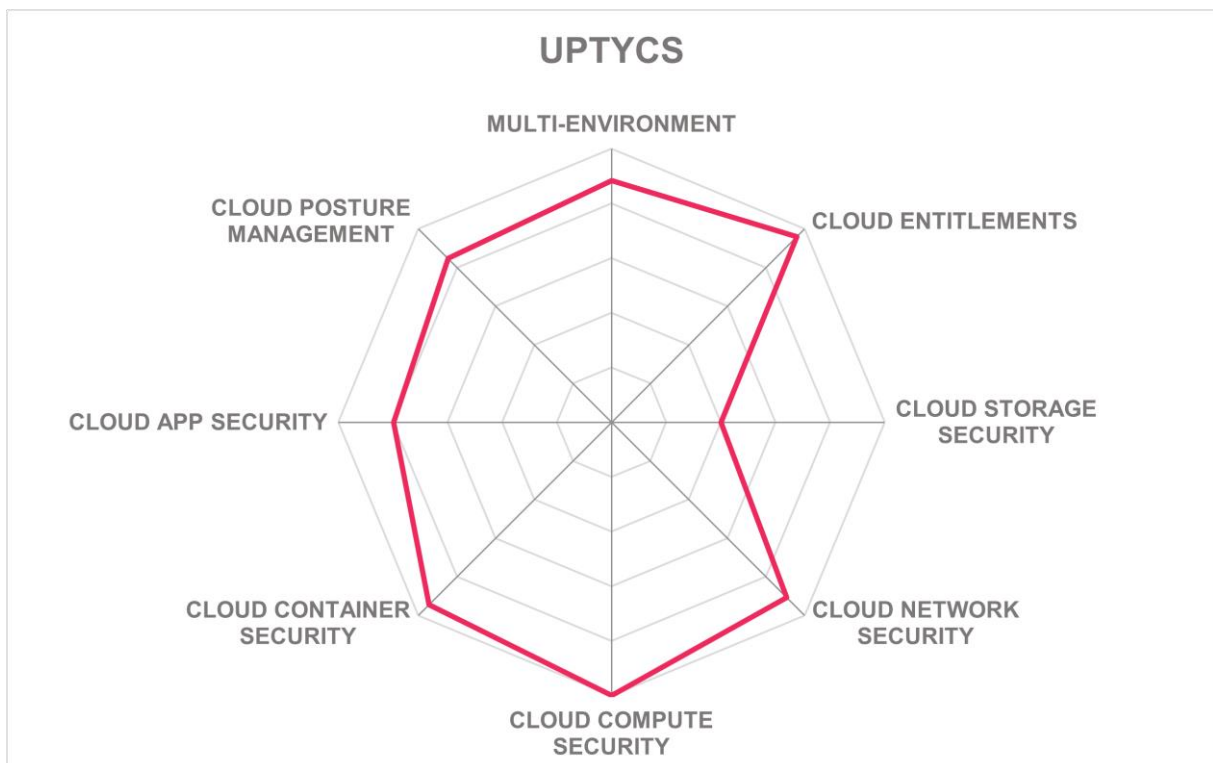
### Strengths

- Provides a complete inventory snapshot across all cloud accounts and services.
- Exposes relationships across resources – including alterations and non-conformance.
- Supports a wide range of public cloud services and virtualized infrastructures.
- Supports both agentless and agent-based deployment, depending on the depth of telemetry required.
- Provides auto-remediation working with native cloud functions (1-click remediation).
- Supports semi-automatic remediation via CLIs to invoke customer's tools.
- Integrates with a wide range of SIEM platforms and workflow / incident management systems.
- Detects and analyzes security risks related to user accounts for people, devices, and service elements with access to cloud services.
- Identifies resources like EC2, S3, EFS, Lambda, and RDS that are exposed to inbound internet traffic.
- Certificate Discovery capability provides visibility into certificates that are self-signed, use wildcards, have weak key lengths, and are expired.
- Discovers risks, vulnerabilities, and exposures across a wide range of cloud compute service environments.
- Scans compute instances for over one thousand types of stored secrets.
- Provides visibility into all 58 Kubernetes resource types, files, processes, and socket level visibility into containers.
- Supports image layer scanning for multiple layers deployed on a container image.
- Supports compliance reporting against a wide range of frameworks and standards including NSA, HIPAA, US FedRAMP, PCI-DSS, ISO 27001, DISA, and VDA.
- Detects threats in workloads through MITRE-based behavioral detection and anomaly-based detection techniques.
- Native integration into CI/CD tooling for development teams to apply security policies consistently across the container image lifecycle (build, store, and deploy).

### Challenges

- Growing the customer base to achieve profitability.
- Expanding the partner ecosystem.
- Does not detect application code vulnerabilities such as SQL Injection.
- Does not cover storage risks related to cloud DBMS or cloud Data lakes.

Leader in



## Wiz – Cloud Security Platform

Wiz is a cloud security startup with its headquarters in New York City. The company was founded in January 2020. Wiz provides a solution that allows organizations to detect and remediate security issues in their use of public cloud infrastructure. Wiz Cloud Security Platform is a CNAPP that includes CSPM, KSPM, CWPP, CDR, vulnerability management, IaC scanning, CIEM, DSPM, and container and Kubernetes security.

Wiz Cloud Security Platform is delivered as Software as a Service and uses the APIs provided by the managed environments and does not require agents to be installed. It covers Alibaba Cloud, AWS, Azure, Google Cloud, Oracle Cloud, Kubernetes, VMware. It provides visibility at the cloud layer, as well as the workload layer across virtual machines, containers, and serverless.

Wiz can identify misconfigurations in both the cloud service and the virtual resource layers. These are identified by comparing the detected configuration of resources with over 2,000 configuration rules relating to frameworks such as CIS, NIST CSF, PCI-DSS, and others. In addition, there are over 10,000 host configuration rules based on benchmarks such as CIS Benchmark for Red Hat Enterprise Linux, Ubuntu Linux, NGINX, and Microsoft Windows Server. The findings generated for both cloud and host configuration rules are assigned severity to help prioritize findings based on their criticality.

It provides visibility into the security of Kubernetes clusters including OpenShift, Kubernetes, Google Kubernetes Engine (GKE), Amazon Elastic Kubernetes Service (EKS), Azure Kubernetes Service (AKS) as well as standalone containers.

For remediation, it can integrate with existing ticketing systems such as ServiceNow or Jira. It provides built-in playbooks for remediating some misconfigurations, and the user can create their own custom playbooks. It determines how critical risks are by correlating findings across misconfigurations, vulnerabilities, networks, identities, secrets, malware, and data to identify toxic combinations. For cloud-native resources, Wiz traces the workload back to the code repository and individual that last committed code for remediation at the root cause.

Wiz scans code and integrates into the CI/CD pipeline to detect and prevent security misconfigurations and vulnerabilities early in the development cycle. These include Jenkins, Travis CI, GitHub, GitLab, CircleCI, as well as AWS DevOps and Azure DevOps. It provides CI/CD guardrails supporting a single set of policies covering container and VM image scanning, IaC template scanning, code scanning, Kubernetes Admission Control, and container image integrity checks.

It calculates the effective network and identity exposures and uses attack path analysis to discover which misconfigurations could lead to lateral movement that could compromise high-value assets. These are visualized on the Wiz Security Graph dashboard which integrates security signals across the cloud environment into a unified view that shows the full context around risks.

Organizations looking for a comprehensive CNAPP platform should consider Wiz.

<b>Security</b>	strong positive	
<b>Functionality</b>	strong positive	
<b>Deployment</b>	strong positive	
<b>Interoperability</b>	strong positive	
<b>Usability</b>	strong positive	

Table 15: Wiz's rating

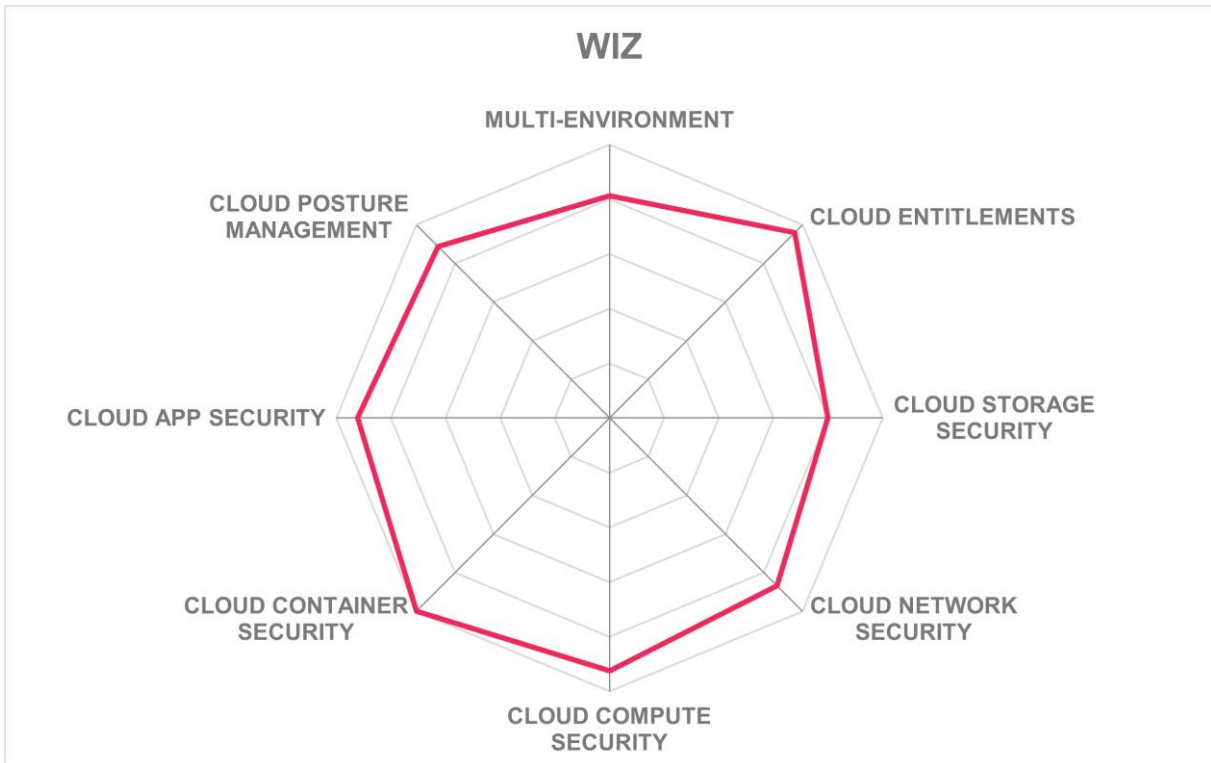
### Strengths

- Also supports VMware vSphere, Red Hat OpenShift, Akamai Linode.
- Comprehensive CNAPP functionality that includes CSPM, KSPM, CWPP, Vulnerability Management, IaC scanning, CIEM, DSPM, and Kubernetes.
- Wiz Security Graph models all the resources and technologies running in the cloud.
- Provides a single prioritized view of risks covering misconfigurations, network exposure, secrets, vulnerabilities, malware, identities, sensitive data, and AI security risks.
- Identifies the toxic combinations of issues that in combination represent the major risks. This provides Contextual-aware risk identification that includes data storage.
- Discovers and identifies security risks in a wide range of security orchestration platforms.
- Integrates into a wide range of CI/CD pipelines and code to detect and prevent security misconfigurations and vulnerabilities early in the development cycle.
- It can provide detailed information about packages, open-source libraries, nested dependencies in Java, Node.js, Python, Go.
- Provides an analysis of chains of exposures and attack paths to high-value assets.
- Supports custom policies using Rego, the language used by OPA (Open Policy Agent).
- Provides out-of-the-box compliance status reports against over one hundred frameworks such as CIS, PCI-DSS, NIST CSF, HIPAA.
- RBAC based controls allow multiple teams to monitor and remediate their own areas within the overall cloud usage.
- Integrates with a wide range of workflow / incident management and SIEM solutions.

### Challenges

- Relatively young but fast-growing organization.
- Some limitations around the detection of risks related to TLS certificates.
- Support and documentation are only available in the English language.

Leader in





## Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other companies in the market that readers should be aware of. These vendors did not participate in the rating for various reasons, but nevertheless offer a significant contribution to the market space.

### AccuKnox

AccuKnox is a cloud-native security vendor founded in 2020 and based in Cupertino, California. The company maintains KubeArmor, an open-source cloud-native policy-based security enforcement system for Kubernetes and other cloud workloads to restrict unwanted behavior of containers, pods, and virtual machines at the system level.

**Why worth watching:** on top of its open-source foundation, the company offers a comprehensive Zero Trust CNAPP solution. Combining agentless cloud security posture management with eBPF and Linux Security Modules for runtime enforcement, AccuKnox delivers instant inline threat remediation across multi-cloud and hybrid deployments.

### AlgoSec

AlgoSec was founded in 2004 and has its headquarters in Ridgefield Park, New Jersey in the USA. The AlgoSec patented platform enables organizations to gain visibility, reduce risk and manage changes across their hybrid network.

**Why worth watching:** In 2022 AlgoSec acquired Prevasio and obtained Prevasio's agentless cloud-native application protection platform (CNAPP). This will be strengthened by the cloud service network security (CSNS) capabilities from AlgoSec.

### Caveonix

Caveonix was founded in 2017 and has its headquarters in Falls Church, Virginia. Caveonix CNAPP provides visibility, analysis, and automated remediation to secure cloud workloads across VMs, containers, and serverless functions. It features exposure scanning and Zero Trust policies to help to protect cloud-native applications during runtime.

**Why worth watching:** Caveonix claims that automated testing and in-depth analysis powered by their Neural-Insight engine allow developers to prioritize and remediate security and compliance issues before they are deployed into runtime environments.

### Cyscale

Cyscale Ltd. is a cloud security company founded in 2019 and headquartered in London, England. The company offers an agentless platform for automating the contextual analysis of cloud misconfigurations, vulnerabilities, access issues, and data risks.

**Why worth watching:** the Security Knowledge Graph that powers the Cyscale platform provides context information about complex relationships between multi-cloud assets to support identifying and prioritizing threats that have real impact on data security.

## Data Theorem

Data Theorem is a company specializing in application security solutions. Founded in 2013 and based in Palo Alto, CA, the company offers a range of automated managed services for application, API, and cloud security. Cloud Secure is the company's solution combining AppSec and CNAPP capabilities across hybrid multi-cloud environments.

**Why worth watching:** Cloud Secure combines cloud infrastructure and workload monitoring capabilities with source code analysis and vulnerability management. Together with Data Theorem's other products, it offers comprehensive protection against data breaches and exploits across APIs, cloud services, and software supply chains.

## Fortinet

Fortinet is a cybersecurity company that was founded in 2000 with its headquarters in Sunnyvale, California. Fortinet provides the Fortinet Security Fabric which consolidates and connects their range of security products. The Fortinet Cloud Security portfolio includes FortiCNP, which is Fortinet's CNAPP solution.

**Why worth watching:** FortiCNP features risk-based prioritization with context-based insights to help security teams to take the actions which will have the most impact to reduce risk.

## Oracle

Oracle Corporation is a multinational information technology company founded in 1977 and headquartered in Austin, Texas. Over the years, the company has grown into one of the largest players in the software industry, as well as a prominent cloud service provider.

**Why worth watching:** Oracle Cloud Guard is an OCI service that helps tenants to monitor, identify, achieve, and maintain a strong security posture on Oracle Cloud. Recently, Oracle introduced new workload protection capabilities to the service, essentially turning it into a full-featured CNAPP platform within OCI.

## Qualys

Qualys, Inc. is an American company that was founded in 1999 and is based in Foster City, California, specializing in cloud security, compliance, and related services. Qualys provides cloud-based security and compliance solutions. Qualys TotalCloud™ is a complete CNAPP solution covering CSPM, IaC, CWPP, Cloud Detection & Response (CDR), and Kubernetes container security.

**Why worth watching:** Qualys features multiple scanning methods that can be used on the same workload, include no-touch, agentless, API-based scanning that can provide results in under 5 minutes and snapshot-based scanning.

## SentinelOne

SentinelOne is a cybersecurity company established in 2013 and based in Mountain View, California. One of the pioneers of AI-based endpoint security technology, it later expanded into cloud workload and data protection as well. In January 2024, SentinelOne announced the acquisition of PingSafe, a cloud security platform that incorporates attackers' intelligence into security coverage, focusing on vulnerabilities that traditional tools often overlook.

**Why worth watching:** in addition to “traditional” CNAPP capabilities, the PingSafe platform incorporates an offensive security engine with a visual hacker graph, as well as leak detection for cloud credentials and other application secrets. Combined with SentinelOne's existing tools, the unified solution will provide better coverage and automation for the entire cloud landscape.

## Sophos

Sophos is a cybersecurity company that was founded in 1985 with its headquarters in Abingdon, England. Sophos offers a wide range of cyber security solutions including Sophos Cloud Native Security. This provides complete cloud security coverage across multiple environments, workloads, and identities.

**Why worth watching:** Sophos Cloud Native Security provides a centralized and integrated cloud-native security solution that monitors, manages, and detects cloud risk.

## Tigera

Tigera is a cloud-native application security vendor headquartered in San Francisco, California. Founded in 2016, the company is the creator and maintainer of Calico Open Source, a widely used container networking and security solution with a strong global user base.

**Why worth watching:** Building on this open-source foundation, Tigera offers an enterprise-grade commercial Cloud-Native Application Protection Platform that prevents, detects, troubleshoots, and automatically mitigates risks of security issues for containers and Kubernetes during build, deploy, and runtime. The platform is available both as Calico Enterprise for on-prem and hybrid deployments and as Calico Cloud, a managed SaaS solution.

## VMware

VMware is a technology company founded in 1998 and headquartered in Palo Alto, California. In November 2023, the company's acquisition by Broadcom was finalized, and

now it operates as a business unit within Broadcom. It offers VMware Aria, which was previously known as vRealize - a cloud solution that unifies applications, infrastructure, and services across private, hybrid, and public clouds into a single cloud management platform with a common data model.

**Why worth watching:** VMware Aria Guardrails is a multi-cloud governance service to help to automate end-to-end policy enforcement across heterogeneous cloud and Kubernetes environments.

## Related Research

[Leadership Compass: Cloud Security Posture Management](#)  
[Leadership Compass: Container Security](#)  
[Leadership Compass: SASE Integration Suites](#)  
[Leadership Compass: Software Supply Chain Security](#)  
[Leadership Compass: Cloud Backup for Ransomware Protection](#)  
[Leadership Compass: CIEM & Dynamic Resource Entitlement & Access Management \(DREAM\) platforms](#)  
[Market Compass: Cloud-delivered Security](#)  
[Whitepaper: Assuring Cloud Security and Compliance](#)  
[Advisory Note: Security Organization Governance and the Cloud](#)  
[Advisory Note: Cloud Services and Security](#)  
[Blog: Cloud Security Alphabet Soup](#)

## Copyright

©2024 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole deny all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators, and software manufacturers in meeting both tactical and strategic challenges and making better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact [clients@kuppingercole.com](mailto:clients@kuppingercole.com).