KuppingerCole ANALYSTS

Cloud Security Posture Management

Mike Small

July 27, 2023

This report provides an overview of the CSPM (Cloud Security Posture Management) market and a compass to help you find a solution that best meets your needs. It examines solutions that provide a way to continuously identify and control certain risks associated with the use of cloud services. It provides an assessment of the capabilities of these solutions to meet the CSPM needs of all organizations to monitor, assess, and manage these risks.

Contents

Figures

Introduction / Executive Summary

The KuppingerCole Leadership Compass provides an overview of a market segment and the vendors in that segment. It covers the trends that are influencing that market segment, how it is further divided, and the essential capabilities required of solutions. It also provides ratings of how well these solutions meet our expectations.

This Leadership Compass covers solutions that ….

> provide a way to continuously identify and control certain risks associated with the use of cloud services. They provide visibility into vulnerabilities in the way these services are configured, secured, and used and assess the risks against common regulatory obligations, security frameworks, and organizational policies. They automate the discovery and reporting of these risks and automate appropriate corrective action.

Most organizations now have a hybrid IT environment where services are delivered in multiple ways, some on premises or at the edge while others are delivered as cloud services. 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 CSPs (Cloud Service Providers) must take steps to secure the service they provide it is up to the customer to secure the way they use the service. CSPM tools are intended to reduce this complexity by helping organizations using cloud services to identify and manage the risks under their control.

There are many acronyms for tools that help to secure cloud services, and these are described in the report. CASB (Cloud Access Security Brokers) together with SASE (Secure Access Service Edge) implement controls which largely focus on SaaS (Software as a Service); however, the risks extend to all cloud service delivery models. CNAPP (Cloud Native Application Protection) focuses on helping to secure the cloud infrastructure elements and the tools used in the DevOps lifecycle. CWPP (Cloud Workload Protection) helps to identify vulnerabilities and misconfigurations within the cloud Virtual Machines and Container hosts. CIEM (Cloud Infrastructure Entitlement Management) provides controls over the entitlements related to virtual resources. CDR (Cloud Detection and Response) helps to detect and respond to threats and active attacks on the customer’s cloud service elements.

CSPM does not replace the controls provided by these tools. Rather, it provides visibility into IaaS and PaaS and helps organizations to ensure that the controls over their multi-cloud environment are deployed in a way that meets the organization's risk appetite. It helps to enable agile governance through the management of guardrails.

Highlights

The highlights from this report are:

- The responsibility for security and compliance is shared between the cloud customer and the CSP.
- The security and compliance 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 dynamic and 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.
- Good governance, with a consistent approach to the security of IT services regardless of how they are delivered, is the best approach. Guardrails provide an agile approach to good governance.
- There is an emerging market in tools to help manage the cloud customers' security responsibilities for various details of cloud services.
- CSPM solutions provide overall visibility into cloud customers' risks to help them to manage their security responsibilities and compliance obligations.
- This report describes the major capabilities that CSPM solutions should provide to achieve these aims and then evaluates how well solutions from several vendors provide these capabilities.
- These capabilities include covering the major IaaS cloud services, providing an inventory of the cloud service elements used by the customer, and identifying the risks that stem from the way that these are configured and used.
- The solutions should cover risks associated with users and their entitlements, the types of data stored and how this is protected, how the in-cloud network is configured to support a Zero Trust approach, failure to mitigate CVEs (Common Vulnerabilities and Exposures) and failure to follow security best practices.
- Solutions should report security posture against a range of common security frameworks and best practices as well as major regulatory obligations.
- The report identifies vendors that, in our opinion, are leaders in four categories in this market segment. These are product leaders with leading edge products, market leaders with a large global customer base, innovation leaders that are driving change in the market and overall leaders.
- In addition, we identify those vendors that we believe have the potential to disrupt the market.

Market Segment

Good governance, with a consistent approach to the security of IT services regardless of how they are delivered, is the best approach to the hybrid IT environment that most organizations now have. This sets measurable business-related objectives for IT services and then monitors that these objectives are met. This approach allows the organization using the IT services to focus on their business and the service providers to focus on delivering the required service.

A governance-based approach to the use of a cloud service means that the cloud customer must clearly set out their business, security, and compliance objectives for the service. It also requires that the customer must be able to measure how well they are meeting these objectives. These are now sometimes referred to as Guardrails which emphasize the need to enable agility achieved through cooperation between teams. Cloud Security Posture Management solutions provide the capabilities needed to measure and enforce these Guardrails.

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 these are met when using a cloud service.

The major business risks from the use of IT services, however they are delivered, are 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 obligations imposed by laws or regulations. The organization must take appropriate steps to mitigate these risks when they use cloud services just as they would for other IT service models.

These risks are not unique to the use of cloud services but there are several factors which increase risks when using the cloud. Firstly, cloud services are frequently used for internet facing applications and this increases their exposure to external cyber-attacks. Secondly, cloud customers may fail to effectively manage their responsibilities for security and compliance. Thirdly, cloud services are dynamic and a traditional static approach to security is not effective. Finally, many 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.

While major CSPs (Cloud Service Providers) go to great lengths to secure the services that they provide, it is up to the cloud service customers to secure how they use 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

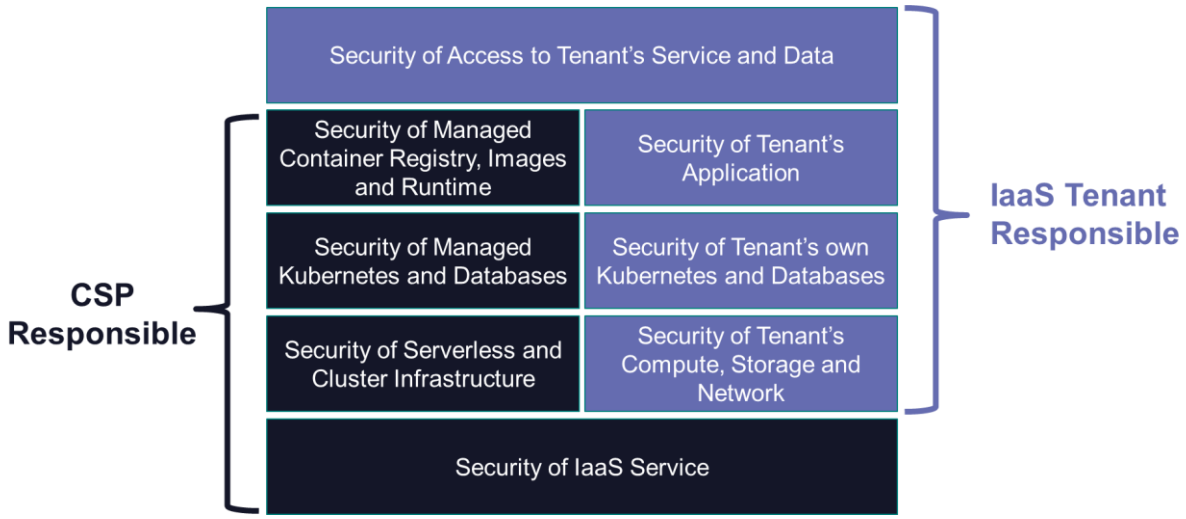


Figure 1: How responsibilities for security and compliance are shared

Figure 2 illustrates in more detail the major security processes a customer using an IaaS service must implement to fulfil their responsibilities. These processes are shown within the context of an overall security fabric. This covers all the elements that need to be secured in a consistent and cost-effective manner. It provides a common set of services that use appropriate tools to achieve the business defined security and compliance objectives.

There are several existing frameworks for the governance of and the best practices for IT security management. For example, the NIST Cybersecurity Framework (CSF) focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The ISO 27000 series of standards provides best practice recommendations for the management of information risks through security controls. There are also other industry-specific frameworks such as the PCI-DSS (Payment Card Industry Data Security Standard). Organizations should adopt the appropriate elements of these frameworks and apply them consistently across all the IT services that they use. CSPM solutions should provide capabilities to measure how well their use of cloud services meets their chosen standards.

Figure 2: A Fabric for Cloud Security

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) – these solutions provide 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) – these solutions provide 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. Threat actors can exploit excessive entitlements .

- CNAPP (Cloud Native Application Protection Platform) – these solutions provide capabilities to view and manage security controls for cloud accounts and workloads integrated into the cloud DevOps workflow.
- CWPP (Cloud Workload Protection Platform) – these solutions provide controls at the microservices instance/container level. These typically include threat detection, intrusion prevention, anti-malware, application control and vulnerability monitoring.

CSPM does not replace the controls provided by these tools. Rather, it provides visibility into IaaS and PaaS and helps organizations to ensure that the controls over their multi-cloud environment are deployed in a way that meets the organization's risk appetite.

Delivery Models

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

Deployment models for Cloud Security Posture Management include:

- As a physical appliance – that can be deployed on premises or in a data center.
- As a virtual appliance that can be deployed on-premises or in a cloud service.
- As 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.
- As 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 Security Posture Management solutions. These capabilities should include:

- **Basic capabilities** include creating a detailed inventory of the cloud services being used by the customer together with an analysis of the risks related to the way in which these cloud 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, and container-based DevOps.
- **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 GUI/Wizards provided for ease of use and CLI/APIs for automation. It is the sum of

capabilities the solutions provide to securely delegate administration to lines of business managers and application owners.

- **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, and Oracle as well as the common virtualization technologies such as Hyper-V, Nutanix, OpenStack, and VMWare.
- **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.
- **User and 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 Security Risks** – The solution should discover and analyze the data stored in cloud services to identify, report, and remediate data with excessive risk or that is being stored out of policy. This includes data without appropriate controls (e.g., not encrypted), data with public access, and data directly exposed to the Internet for a wide range of cloud storage types (File Systems, Object Stores, Databases, etc.).
- **Network Security Risks** - The solutions should discover and analyze cloud network security controls to support a Zero Trust approach to network management. It should discover and map cloud networks owned and identify, report, and remediate risky firewall configurations, risky permitted network protocols, as well as poor TLS certificate management and rotation.
- **Compute Service Risks** – 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.
- **DevOps Risks** – the solution should analyze container security. It should discover cloud container services used by the tenant to identify, report, and remediate insecure container images, container registries, and deployments for common container environments such as Kubernetes. It should analyze the DevOps packages to identify, report, and remediate apps exposed to the internet, apps with exposed vulnerabilities (e.g., SQL Injection), apps without appropriate traffic controls (e.g., WAF), APIs exposed to the internet and APIs without appropriate access controls, and apps with other risky deployments. In addition, it should monitor the

security controls on the CI/CD (Continuous Integration / Continuous Delivery) pipeline.

- **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 of pilot phase, based on the specific criteria of the customer.

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

- Product Leadership
- Innovation Leadership
- Market Leadership

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right.

Overall Leadership

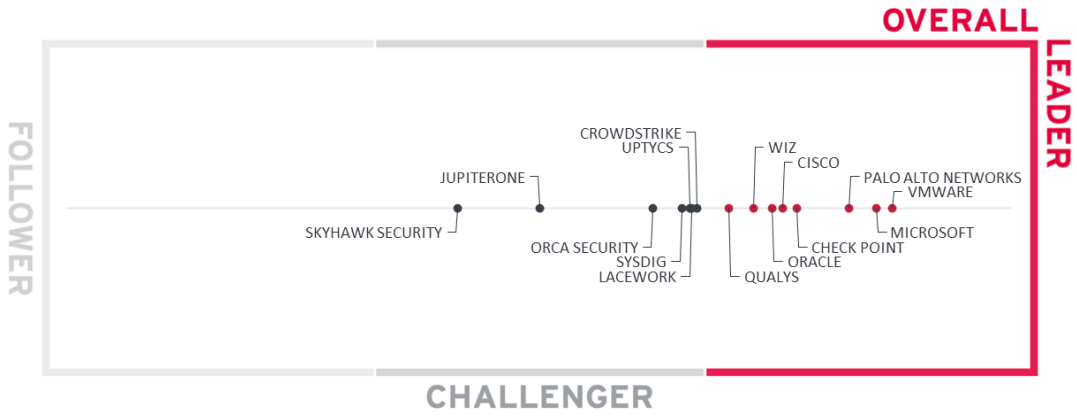


Figure 3: Overall Leaders in the Leadership Compass CSPM

The Overall Leaders are (in alphabetical order):

- Check Point
- Cisco
- Microsoft
- Oracle
- Palo Alto Networks
- Qualys
- VMware
- Wiz

the Overall Challengers are (in alphabetical order): CrowdStrike, JupiterOne, Lacework, Orca Security, Skyhawk Security, Sysdig, and Uptycs. There are no vendors in the Followers section.

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.

Figure 4: Product Leaders in in the Leadership Compass CSPM

All vendors in the Product Leadership deliver leading-edge capabilities across the depth and breadth of the Cloud Security Posture Management 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.

Product Leaders (in alphabetical order):

- Check Point
- Cisco
- JupiterOne
- Lacework
- Microsoft
- Orca Security
- Palo Alto Networks
- Sysdig
- Uptycs
- VMware
- Wiz

The Product Challengers are (in alphabetical order): CrowdStrike, Oracle, Qualys, and Skyhawk Security.

All these vendors have good offerings but lack 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.

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.

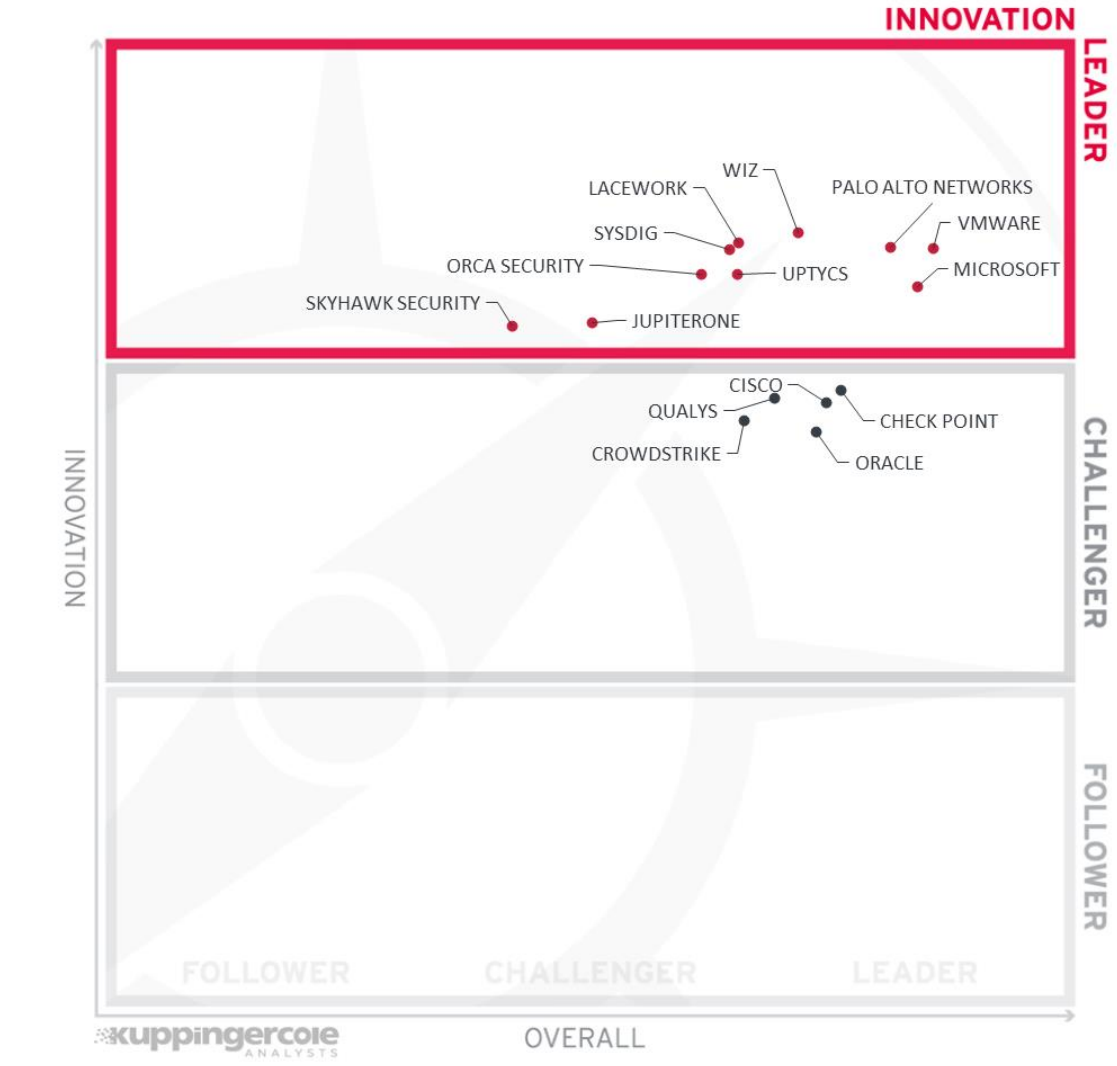


Figure 5: Innovation Leaders in the Leadership Compass CSPM

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.

Innovation Leaders (in alphabetical order):

- JupiterOne
- Lacework
- Microsoft
- Orca Security
- Palo Alto Networks
- Sysdig
- Uptycs
- Skyhawk Security
- VMware
- Wiz

The Innovation Challengers are (in alphabetical order):

These companies also have some specific innovations that make their offerings attractive to their customers but lack the breadth of innovation that other vendors demonstrate - Check Point, Cisco, CrowdStrike, Oracle, and Qualys.

Market Leadership

Lastly, we analyze **Market** Leadership. This is an amalgamation of the number of customers in this market sector, their geographic distribution, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and 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.

Figure 6: Market Leaders in the Leadership Compass CSPM

Market Leaders (in alphabetical order):

- Check Point
- Cisco
- CrowdStrike
- Microsoft
- Oracle
- Palo Alto Networks
- Qualys
- VMware

The Market Challengers are (in alphabetical order): JupiterOne, Lacework, Orca Security, Skyhawk Security, Sysdig, Uptycs, and Wiz.

Some of these vendors are relatively young, lack a comprehensive global presence, focus mainly on their home markets, or are still in their growth phase. The large vendors that are challengers, while having a large overall market, tend to have a limited presence in this market.

There are no Followers in this market segment.

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

The Market/Product Matrix

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

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

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

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: Check Point, Cisco, Microsoft, Palo Alto Networks, and VMware all as market champions positioned in the top right-hand box.

In the top center box, we see CrowdStrike, Oracle, and Qualys, each of which has a strong market presence but with products that are less feature-rich in this market.

Market Disrupters – 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 JupiterOne, 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. There is only one vendor, Skyhawk Security, in this position.

The Product/Innovation Matrix

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

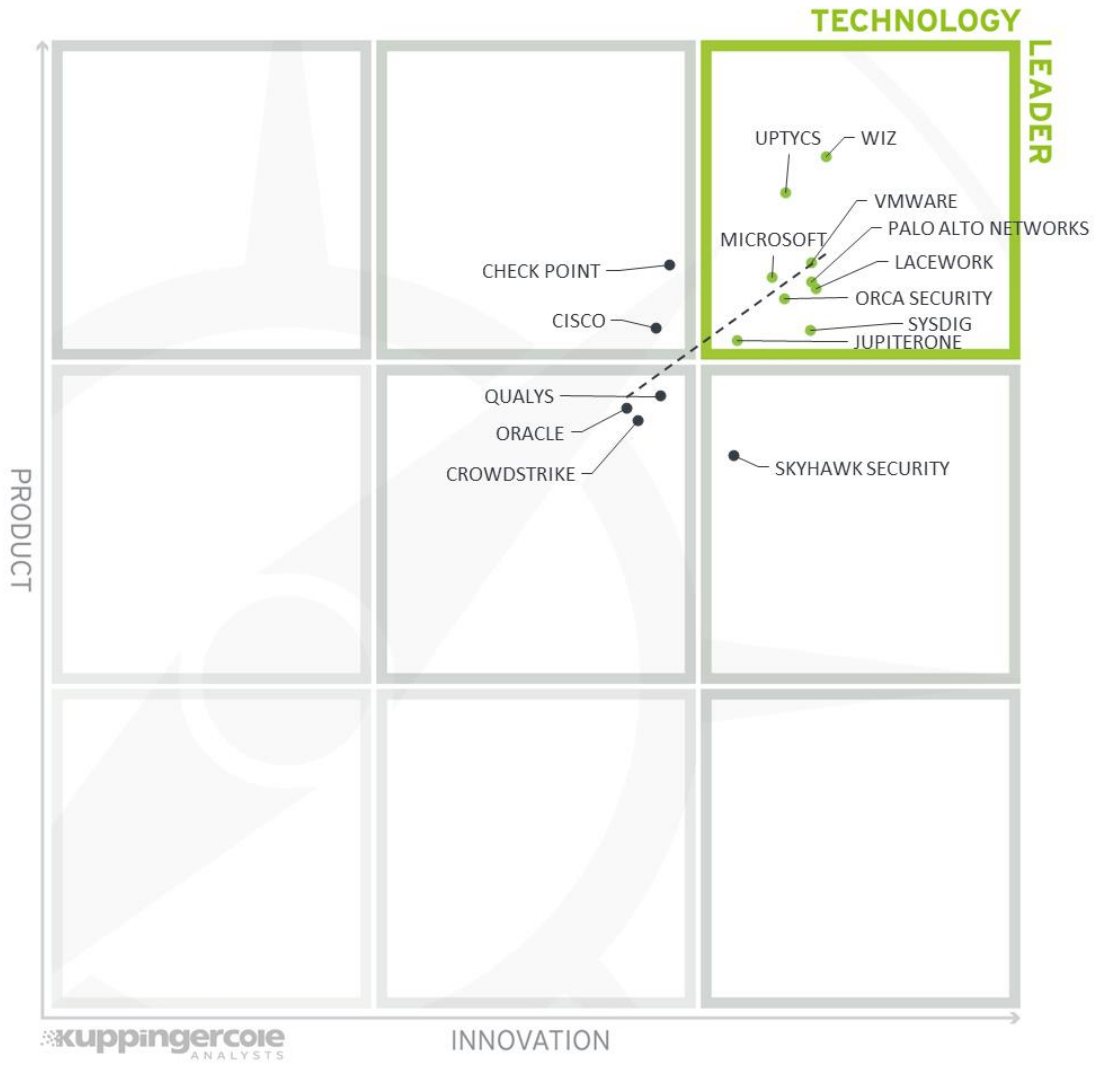


Figure 8: Product/Innovation Matrix for the Leadership Compass CSPM

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 in this box take different approaches to delivering CSPM, 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): JupiterOne, Lacework, Microsoft, Orca Security, Palo Alto Networks, Sysdig, Uptycs, Wiz, and VMware.

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

In the center right box are the technology disrupters. These have a high degree of innovation but have not yet created a market-leading product. In this box we find Skyhawk Security.

Three vendors appear in the center box, showing both good innovation and product capabilities. However, they remain at a Challenger level in both product and innovation ratings. These vendors include (in alphabetical order) CrowdStrike, Oracle, and Qualys. These vendors have a strong potential to further increase their position in the CSPM 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.

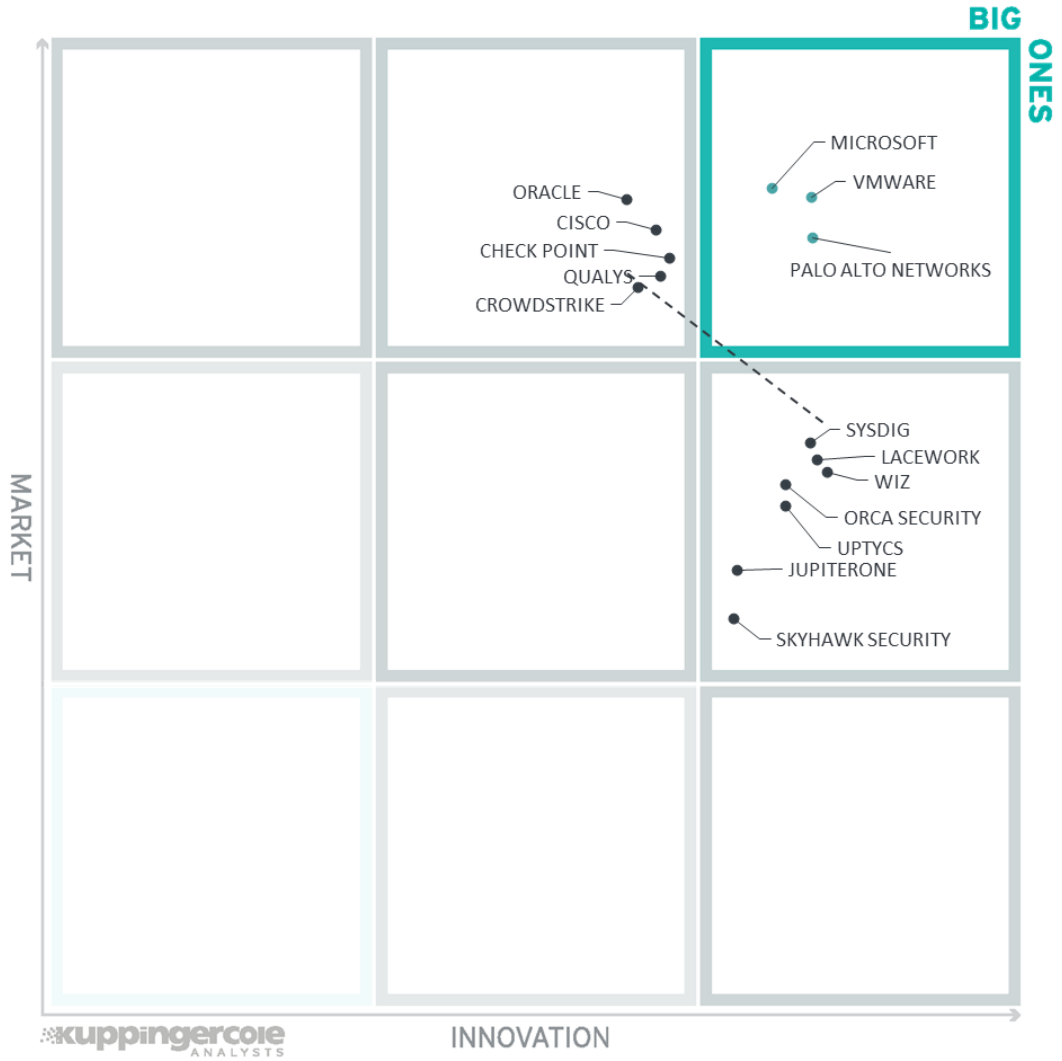


Figure 9: Market/Innovation Matrix for the Leadership Compass CSPM

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 CSPM market. We see (in alphabetical order) Microsoft, Palo Alto Networks and VMware. 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 three vendors each with a strong market presence and good innovation. These are (in alphabetical order) Check Point, Cisco, Oracle and Qualys.

Market Disruptors - Several vendors appear in the middle right box showing a good level of innovation but with less market presence than the vendors in the "Big Ones" category. These include (in alphabetical order) JupiterOne, Lacework, Orca Security, Skyhawk 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. These vendors and their solutions have the potential to change the market landscape.

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 Security Posture Management. 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. Since some vendors may have multiple products, these are listed according to the vendor's name.

Product(s) from Vendor	Security	Functionality	Deployment	Interoperability	Usability
CHECK POINT	strong positive	strong positive	strong positive	strong positive	strong positive
CISCO	strong positive	positive	strong positive	strong positive	strong positive
CROWDSTRIKE	strong positive	positive	strong positive	positive	positive
JUPITERONE	positive	positive	strong positive	strong positive	positive
LACEWORK	strong positive	strong positive	strong positive	strong positive	positive
MICROSOFT	strong positive	strong positive	strong positive	positive	strong positive
ORACLE	positive	positive	strong positive	neutral	strong positive
ORCA SECURITY	strong positive	strong positive	strong positive	positive	positive
PALO ALTO NETWORKS	strong positive	strong positive	strong positive	strong positive	strong positive
QUALYS	strong positive	positive	strong positive	positive	positive
SKYHAWK SECURITY	positive	positive	strong positive	positive	positive
SYSDIG	strong positive	positive	strong positive	positive	positive
UPTYCS	strong positive	strong positive	strong positive	strong positive	strong positive
VMWARE	strong positive	strong positive	strong positive	strong positive	strong positive
WIZ	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
CHECK POINT	positive	strong positive	strong positive	strong positive
CISCO	positive	strong positive	strong positive	strong positive
CROWDSTRIKE	positive	strong positive	strong positive	strong positive
JUPITERONE	strong positive	neutral	neutral	neutral
LACEWORK	strong positive	positive	positive	positive
MICROSOFT	strong positive	strong positive	strong positive	strong positive
ORACLE	positive	strong positive	strong positive	strong positive
ORCA SECURITY	strong positive	positive	positive	positive
PALO ALTO NETWORKS	strong positive	strong positive	strong positive	strong positive
QUALYS	positive	strong positive	strong positive	strong positive
SKYHAWK SECURITY	strong positive	neutral	neutral	weak
SYSDIG	strong positive	positive	positive	positive
UPTYCS	positive	positive	positive	neutral
VMWARE	strong positive	strong positive	strong positive	strong positive
WIZ	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 this Leadership Compass, we look at the following categories:

Basic Functionality provided by the solution includes the range of cloud services covered, together with an analysis of the risks related to the way in which these are configured and being used. They include how easy the solution is to deploy and administer, scalability, security of the solution itself and how well it interoperates with other relevant IT tools such as CMDB, SIEM and Workflow.

User Risks – The capabilities provided by the solution to discover and analyze the cloud users (people, services, and service elements) and their entitlements. The functionality it provides to identify, report, and remediate user accounts with excessive / abnormal privileges and other risks such as orphan accounts, and accounts with weak authentication policies.

Data Risks – The capabilities provided by the solution to discover and analyze the data being stored in the cloud services to identify, report, and remediate data with excessive risk or that is being stored out of policy. This includes data without appropriate controls (e.g., not encrypted), data with public access, and data directly exposed to the Internet for a wide range of cloud storage types (File Systems, Object Stores, Databases, etc.).

Network Risks - The capabilities provided by the solution to discover and analyze cloud network security controls to support a Zero Trust approach to network management. It includes how well it can discover and map cloud networks owned and identify, report, and remediate risky firewall configurations, risky permitted network protocols, as well as poor TLS certificate management and rotation.

Compute Risks – The capabilities provided by the solution to discover and analyze the cloud compute services being used. The functionality it provides to identify, report, and remediate VMs with risky patch levels, VMs with unmanaged vulnerabilities, and risky configurations for a wide range of VM and OS types. These capabilities should also cover serverless computing elements.

DevOps Risks – The capabilities provided by the solution to analyze container security. How well it can discover cloud container services owned and identify, report, and remediate insecure container images, container registries, and deployments for common container environments such as Kubernetes. In addition, how well this covers DevOps packages to

identify, report, and remediate apps exposed to the internet, apps with exposed vulnerabilities (e.g., SQL Injection), apps without appropriate traffic controls (e.g., WAF), APIs exposed to the internet and APIs without appropriate access controls, and apps with other risky deployments.

Risk Reporting – The capabilities provided by the solutions to report on the risks that have been discovered. The information that the solution provides on both the likelihood of the risk and its impact. The functionality to aggregate overall risk / security posture suitable for presentation to board level management. The extent to which the reporting capabilities are interactive and allow the user to expand the overall risks to identify the underlying causes. The level of integration with workflow / ticketing systems to recommend, initiate, and track remediation.

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

CHECK POINT – CloudGuard CNAPP

Check Point Software Technologies Ltd. was founded in 1993 and provides cyber security 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 focusses 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, CloudGuard 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 allows for customization through its proprietary query language, GSL (Governance Specification Language). CloudGuard GSL is human readable and offers a unified language across multiple cloud providers.

It offers compliance management and contextual cloud security across 70+ cloud-native services. It includes out-of-the-box assessments for more than 50 compliance frameworks and 2,400 security rules. These include standards such as PCI DSS, HIPAA, CIS Benchmarks, NIST CSF/800-53 and more with automated data aggregation and assessment as well as remediation and reporting.

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 least privilege policies based on actual permission usage. CloudGuard Spectral automated tools integrate with developers' tools to detect code vulnerabilities and 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.

Security	strong positive	
Functionality	strong positive	
Deployment	strong positive	
Interoperability	strong positive	
Usability	strong positive	

Table 3: Check Point's rating

Strengths

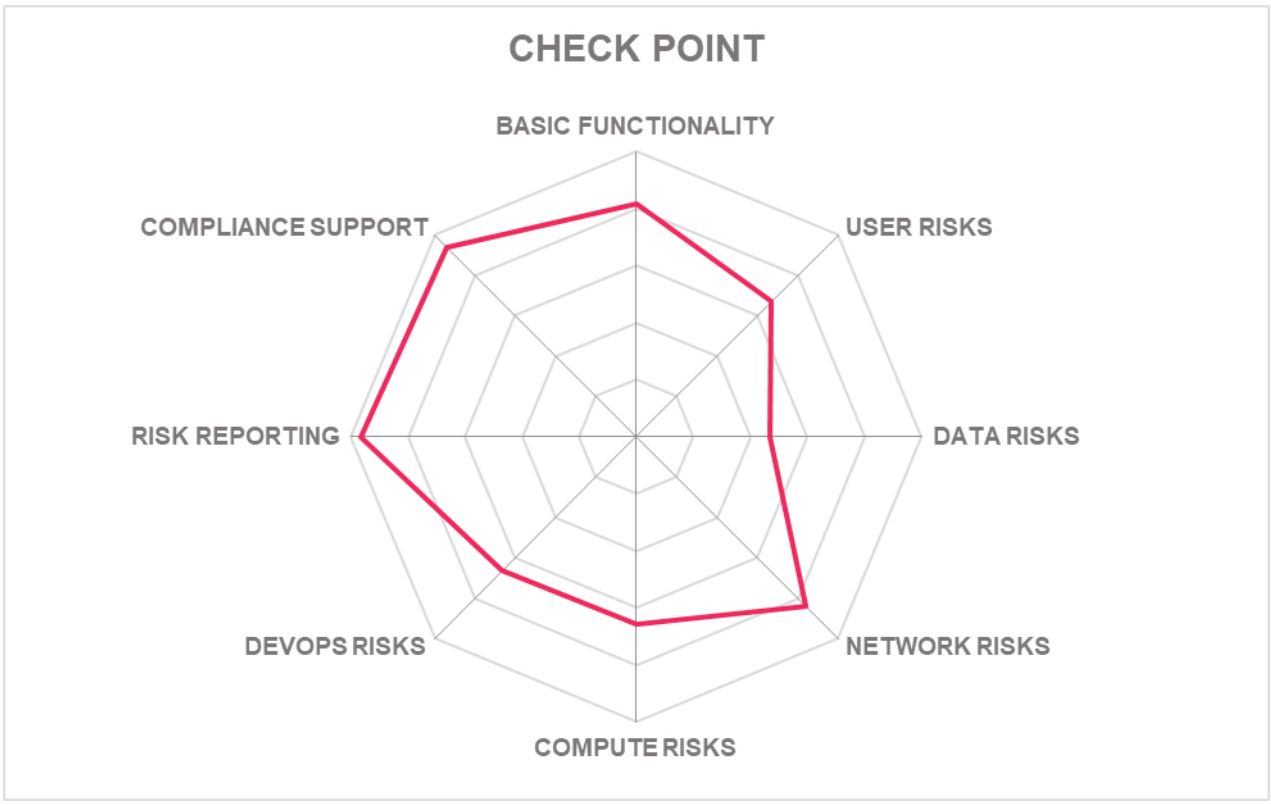
- Cloud Guard CSPM is part of their comprehensive Cloud Native Application Protection Platform.
- CloudGuard's Effective Risk Management (ERM) engine prioritizes risks and provides remediation guidance using AI and risk scoring to reduce the attack surface.
- Delivered as SaaS for ease of deployment.
- It can be either agent powered or agentless depending upon customer requirements.
- Covers a wide range of services from the major public cloud service providers.
- Provides a common policy language for securing multiple cloud services.
- Comprehensive range of policies and rules out of the box.
- Supports automated remediation of detected risky configurations.
- Integrates with a wide range of CMDB platforms out of the box.
- Interoperates with a wide range of SIEM and incident management solutions.
- Good coverage of user and entitlements risks for people, devices, and services.
- Automatic recommendation of least privilege policies based on permission usage.
- Leverages AI to provide context behind the analysis to focus on the risks that matter.
- Integrated CNAPP solution which provides advanced cloud security across the entire stack within a single platform.
- These capabilities support shift-left and provide cloud detection and response.

Challenges

- Documentation is only available in English and Chinese. However, support services are available in many languages from offices across the world.
- Does not detect sensitive types of data in storage. This is on the roadmap.
- Does not detect missing / misconfigured anti-malware protection.
- Only covers risks in Linux variants.
- Missing out-of-the-box policies for local compliance regulations e.g. (HDS, TISAX, C5)

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


CHECK POINT
BASIC FUNCTIONALITY
USER RISKS
DATA RISKS
NETWORK RISKS
COMPUTE RISKS
DEVOPS RISKS
RISK REPORTING
COMPLIANCE SUPPORT

CISCO – Cisco Attack Surface Management

Cisco Systems, Inc. is a well-established digital communications technology conglomerate with its headquarters in in San Jose, California. Cisco offers a wide range of cyber security products including firewalls, intrusion prevention systems, secure access systems, security analytics and malware defense. This report focusses on Cisco Attack Surface Management, which offers CSPM capabilities. Note that in May 2023, Cisco announced its intent to acquire Lightspin Technologies Ltd., a privately held cloud security software company with a CSPM solution.

Cisco Attack Surface Management, which was previously offered as Cisco Secure Cloud Insights, is a cloud-native security platform that connects across an organization's security tools, providing visibility into security risks across their IT assets. It is a component of Cisco XDR (Extended Detection and Response) and integrates the cyber asset discovery and vulnerability analysis capabilities provided by JupiterOne.

Cisco Attack Surface Management (ASM) collects and analyzes data from across an organization's technology stack and digital operations, providing comprehensive visibility and proactive risk management within the Cisco XDR framework. It provides an open and extensible platform that collects and analyses data from all the elements in the organization's technology stack and digital operations. It covers cloud services, code repositories, endpoints, SaaS apps, IAM policies, security controls, and vulnerability findings. It covers the major cloud services providers including AWS, Azure, and Google Cloud as well as VMware and other virtualized infrastructure.

It provides a consistent object model to represent all these assets and their properties consistently and a query language to investigate anomalies. It has a graphical user interface to display the assets in the context of their properties and relationships. It continuously monitors the environment for changes and provides alerts when action is needed. It provides documented APIs to enable integration with existing security tools to interchange data with EASM, SIEM, SOAR, XDR, and vulnerability management solutions to provide a consolidated view of risks and priorities.

It provides CIEM (Cloud Infrastructure Entitlement Management) capabilities to help organizations manage access to cloud resources and data as part of a Zero Trust approach. This helps security teams to identify and manage risks associated with user privileges and helps organizations comply with regulatory requirements. Capabilities include continuous monitoring of user privileges and access to cloud resources and data, detecting changes, and automated remediation.

It integrates with DLP (Data Leakage Prevention) solutions to monitor risks related to sensitive data. It includes monitoring of a comprehensive range of cloud service storage elements for risks including public access and internet exposure. It supports a Zero Trust approach to network security. It detects misconfigurations of network assets, analyses exposure paths, and provides context around anomalous events.

It includes predefined policies and reports that support a wide range of security best practices and compliance frameworks including SOC2, HIPAA, FedRAMP, CIS, and others.

Organizations looking for a CSPM solution that is part of an integrated range of security solutions from a mature security vendor should consider Cisco Attack Surface Management.

Security	strong positive
Functionality	positive
Deployment	strong positive
Interoperability	strong positive
Usability	strong positive

Table 4: Cisco's rating

Strengths

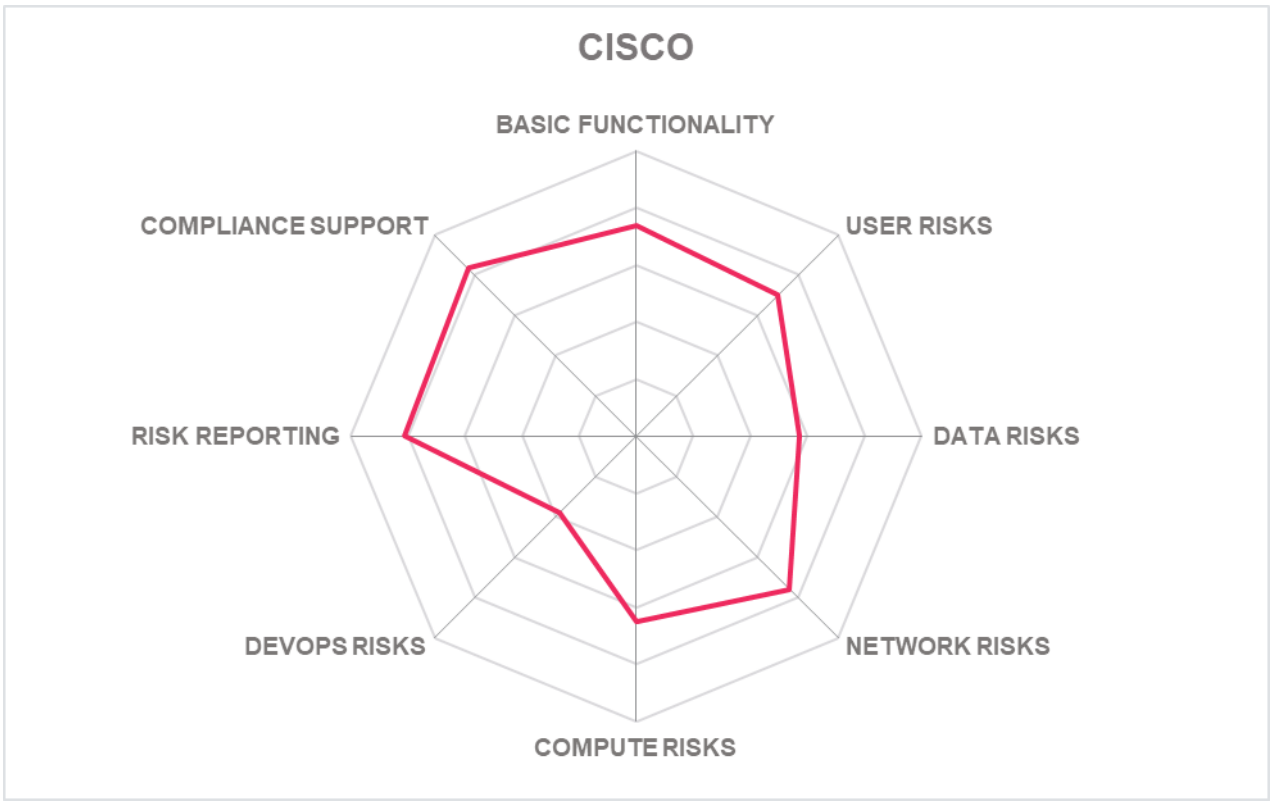
- Provides visibility of cyber risk management, digital assets, with real-time assessments.
- Collects data on a wide range of cloud services, code repositories, endpoints, SaaS apps, IAM policies, security controls, and their vulnerabilities.
- Continuously discovers assets and analyses attack paths.
- Prioritizes vulnerability findings to optimize use of security resources.
- Provides a common policy model that covers multiple cloud services and asset types.
- Includes a comprehensive range of policies and rules out of the box.
- Supports automated remediation of detected misconfigurations, vulnerabilities, and risks.
- Open APIs enable integration with a wide range of assets and security tools.
- Interoperates with a wide range of SIEM and incident management solutions.
- Covers user and entitlements risks for people, devices, and services.
- 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.

Challenges

- Integration of Lightspin technology.
- Full data risk analysis requires integration with a DLP tool.
- Depends upon integration with external solutions like vulnerability and code scanners.
- Limited integration with DevOps.
- Does not support code vulnerability scanning out-of-the-box.

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


CISCO
BASIC FUNCTIONALITY
USER RISKS
DATA RISKS
NETWORK RISKS
COMPUTE RISKS
DEVOPS RISKS
RISK REPORTING
COMPLIANCE SUPPORT

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 focusses 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 visibility into cloud infrastructure and resources across AWS, Azure, and Google clouds. These services are automatically configured when the services are deployed and compared against industry benchmarks and best practices. This can identify risks such as misconfigurations, public workloads, and unauthorized modifications, and the service includes guided remediation as well as guardrails against future mistakes.

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 works across both public and private clouds and covers compute and container workloads running across AWS, Azure, and Google clouds. 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 cloud control plane to cloud run-time. Together, these functions provide visibility, detect misconfigurations and anomalous behavior, and offer guidance on the appropriate response to threats to reduce attack surfaces.

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 features Kubernetes Operator and Helm Charts to provide ease-of-use based on familiar tools. It integrates with native cloud tools as well as GitHub, Jenkins, and other build tools to support secure DevOps.

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. It supports entitlements modelling to uncover and help to minimize risks from excessive entitlement combinations.

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

Security	strong positive
Functionality	positive
Deployment	strong positive
Interoperability	positive
Usability	positive

Table 5: CrowdStrike's rating

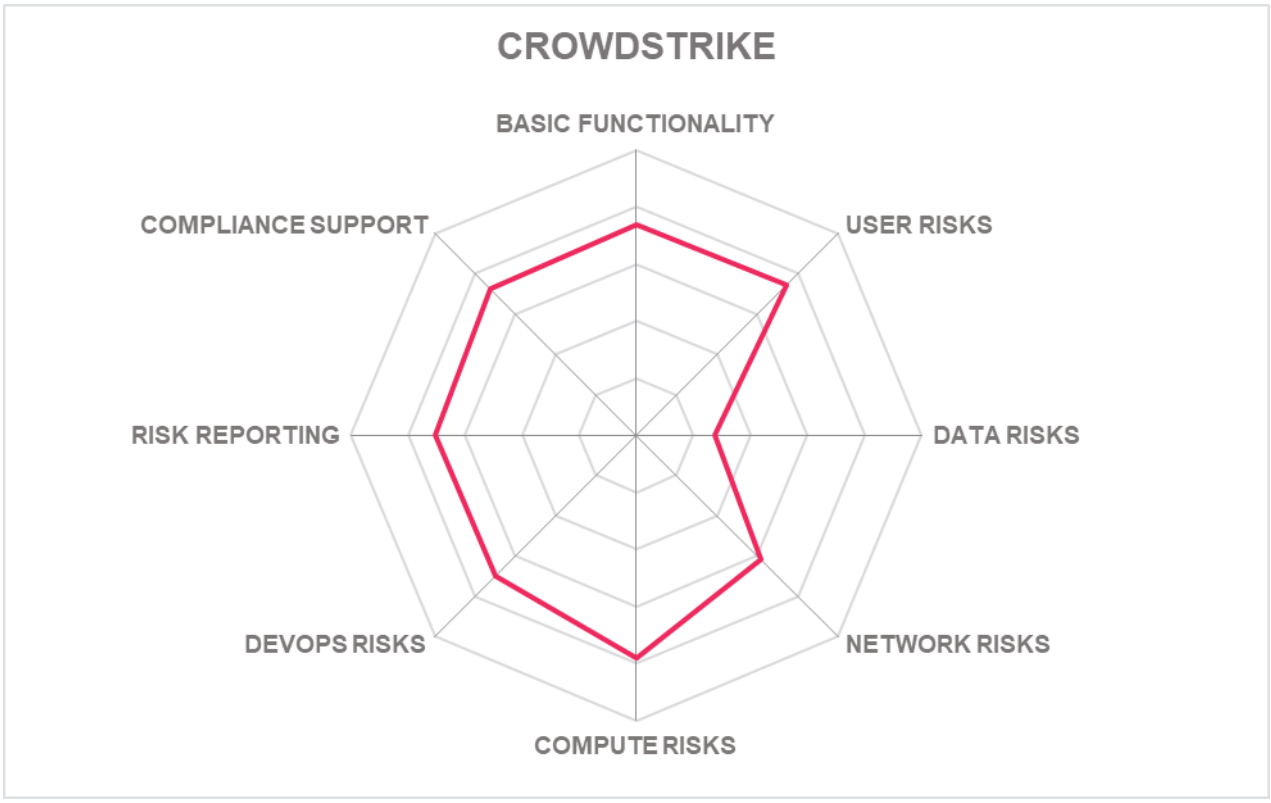
Strengths

- The solution is part of a complete security platform.
- Integrated graphical representation of cloud service elements and topology and risks in context.
- Detects risks related to users and excessive entitlements.
- Visualizes entitlement paths to show unexpected attack paths.
- Detects misconfigurations in cloud service elements including compute, network, and storage.
- Detects risks related to storage elements including public access, lack of encryption and backup.
- Detects risks related to CVEs and misconfigurations in hosts and containers.
- Integrated with Kubernetes and CI/CD pipeline.
- Integrates with common DevOps tools.
- Open APIs for ease of integration.
- 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.

Challenges

- Does not include scanning of stored data to identify risks related to sensitive / regulated data.
- Support and documentation only available in English and Japanese.
- Integration with Identity Providers limited to Microsoft Active Directory and AWS IAM.

Leader in


CROWDSTRIKE
BASIC FUNCTIONALITY
USER RISKS
DATA RISKS
NETWORK RISKS
COMPUTE RISKS
DEVOPS RISKS
RISK REPORTING
COMPLIANCE SUPPORT

JUPITERONE – JupiterOne

JupiterOne was founded in 2020 and has its headquarters in Morrisville, NC in the USA. Its product JupiterOne is a cyber asset attack surface management (CAASM) platform that provides visibility into the security of an organization's cyber assets. JupiterOne provides a knowledge base that helps an organization to manage the security and compliance posture of all their cyber assets both cloud and non-cloud. JupiterOne is also offered as a component of Cisco Cloud Protection Suite.

JupiterOne is deployed as a SaaS solution that integrates with the customer's cloud service provider infrastructure to deliver CSPM capabilities. It creates and an inventory of the customer's cloud service components across AWS, Microsoft Azure, Google Cloud, Alibaba, and Oracle Cloud. In addition, it can cover SaaS as well as IaaS and PaaS. The JupiterOne platform supports documented APIs that can be used to integrate with other tools and services; out of the box integrations include GitHub, GitLab, Jira, PagerDuty, Slack, Splunk, and more.

JupiterOne uses cloud native APIs and services to collect data on cloud resources and these data are normalized and mapped into a common schema. Data is stored in a graph database and includes the relationships between resources, their properties, their users, and their access. These relationships can provide insights into potential risks. For example, the relationships between cloud resources and cloud user account permissions can help to highlight user accounts with excessive or abnormal privileges as well as potential attack paths.

For data security, JupiterOne analyses cloud infrastructure, network, datastore, and access configurations which provides context around data asset classifications and helps to identify data at risk. JupiterOne can integrate with a DLP tool to identify sensitive and regulated data within this context to provide further actionable insights. These can include identifying data that are out of policy for example, by being stored unencrypted, or by being exposed to the internet with public access rights.

JupiterOne integrates with the native cloud capabilities and a wide range of network security tools to analyze cloud network security controls in support of network security management. It discovers and maps the cloud networks owned by the customer and can identify risky firewall configurations, risky permitted network protocols, as well as TLS certificate mapping and rotation.

In conjunction with other tools JupiterOne can discover and report on cloud apps deployed and identify 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. It can also discover APIs exposed to the internet and APIs without appropriate access controls.

JupiterOne provides out-of-the-box support for many of the major compliance frameworks including SOC 2, NIST, CIS, PCI, ISO, and HIPAA. In addition, JupiterOne supports custom frameworks and policies.

Organizations looking for a CSPM solution that is part of a wider Cyber Attack Surface Management platform should consider JupiterOne.

Security	positive
Functionality	positive
Deployment	strong positive
Interoperability	strong positive
Usability	positive

Table 6: JupiterOne's rating

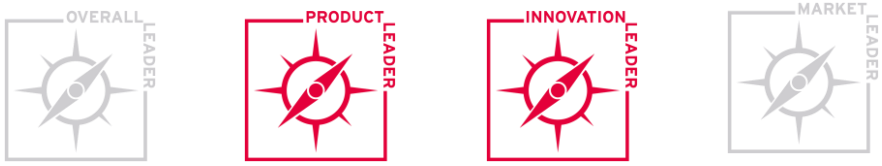
Strengths

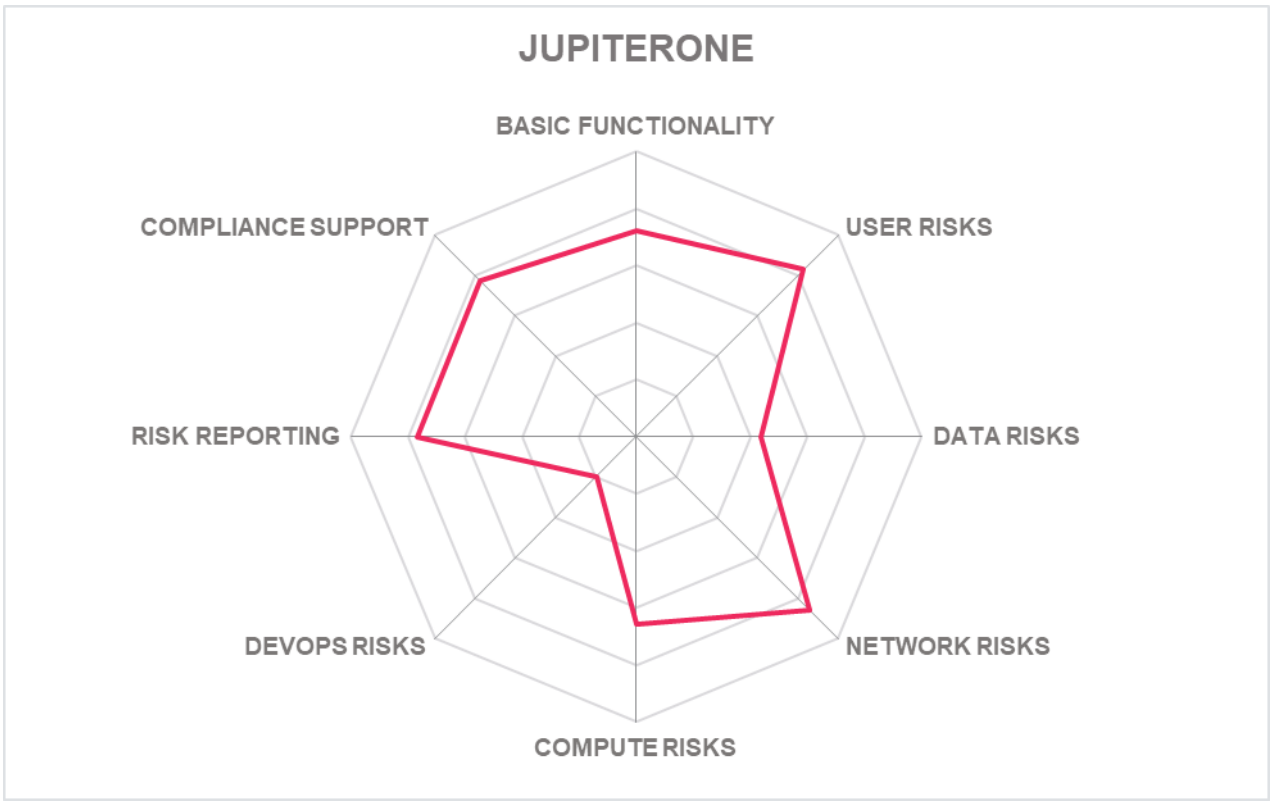
- JupiterOne provides a consolidated view into cloud and non-cloud IT resources.
- Open platform with published APIs to enable integration of resources and tools.
- Integrated graphical representation of cloud service elements and topology and risks in context.
- Out of the box coverage of AWS, Microsoft Azure, Google Cloud, Alibaba, and Oracle Cloud.
- Continuously discovers assets and analyses relationships for attack paths.
- Provides a common policy model that covers multiple cloud services and asset types.
- Includes a comprehensive range of policies and rules out of the box.
- Interoperates with a wide range of SIEM and incident management solutions.
- Covers user and entitlements risks for people, devices, and services.
- Out-of-the-box audit reports covering a wide range of security best practices and compliance frameworks.

Challenges

- Does not cover risks in servers and hosts operating systems due to misconfigurations and missing patches out of the box. But it can integrate with other tools for this.
- Does not cover risks related to container images, registries, and cloud workloads out of the box.
- Full data security risk analysis depends upon integration with external tools such as DLP.
- Does not support scanning of apps for code vulnerabilities but integrates with many code scanning solutions.

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


JUPITERONE
BASIC FUNCTIONALITY
USER RISKS
DATA RISKS
NETWORK RISKS
COMPUTE RISKS
DEVOPS RISKS
RISK REPORTING
COMPLIANCE SUPPORT

LACEWORK – Polygraph® Data Platform

Lacework was founded in 2015 and has its headquarters in Mountain View, California. It is backed by venture capital and has received around $1.8 billion dollars of funding. Lacework products help to provide security for DevOps, containers, and cloud environments. This report focusses on the CSPM capabilities of the Lacework Polygraph Data Platform which provides a complete CNAPP including CWPP.

Lacework's Polygraph Data Platform is a patented, data-driven security technology platform that delivers end-to-end visibility into what is happening across a customer's cloud environment. This includes detecting security vulnerabilities, misconfigurations, unusual activity, and potential attacks. It covers AWS, Azure, Google Cloud and Oracle OCI providing a single consolidated security and compliance dashboard. It ingests millions of incoming data points, correlates them into behaviors, and detects potential security events. It helps the customer to understand their cloud security posture and to prioritize the security and compliance risks that need action.

It is delivered as SaaS and can rapidly be deployed for large cloud environments. Lacework Terraform modules help to accelerate deployment and integration with alert channels. It uses a combination of both agentless and agent-based approaches to gather the information. Agents are not mandatory but can provide deep insights into running hosts and containers. The Lacework CLI enables integration with the inline scanner for container image and registry scanning. It also provides a Helm chart to deploy the agent and KSPM (Kubernetes Security Posture management) collectors.

It provides a complete inventory of the Clouds and IaaS / PaaS services in use and integrates with the native cloud security services. It features a wide range of pre-built policies for standards like PCI, HIPAA, NIST, ISO 27001, SOC 2, and others to help identify risks and manage compliance.

It detects deviations from normal behavior across the cloud infrastructure including activity in Kubernetes, VM workloads, and containerized workloads. This covers a wide variety of threats such as escalation of privileges and misconfigurations. As threats are identified, it provides a comprehensive event card that displays the details of the event as a graphical representation. This includes attack path analysis and other context-based guidance to help to fix misconfigurations.

It exploits ML (Machine Learning) capabilities that automatically cluster processes into groups of related activity and identify the applications in use. It uses analytics and ML techniques to detect anomalies that may indicate threats. This can identify rare anomalous events while not triggering alerts on events that it has learnt are typical for the environment.

Organizations looking for a CSPM that is part of a complete CNAPP and is based on machine learning and data analysis should consider Lacework Polygraph Data Platform.

Security	strong positive
Functionality	strong positive
Deployment	strong positive
Interoperability	strong positive
Usability	positive

Table 7: Lacework's rating

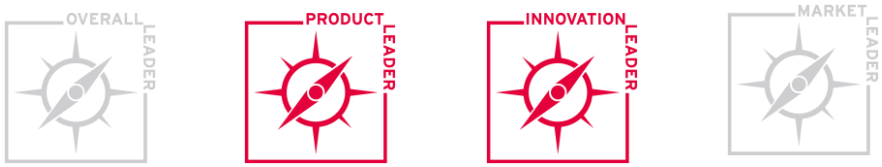
Strengths

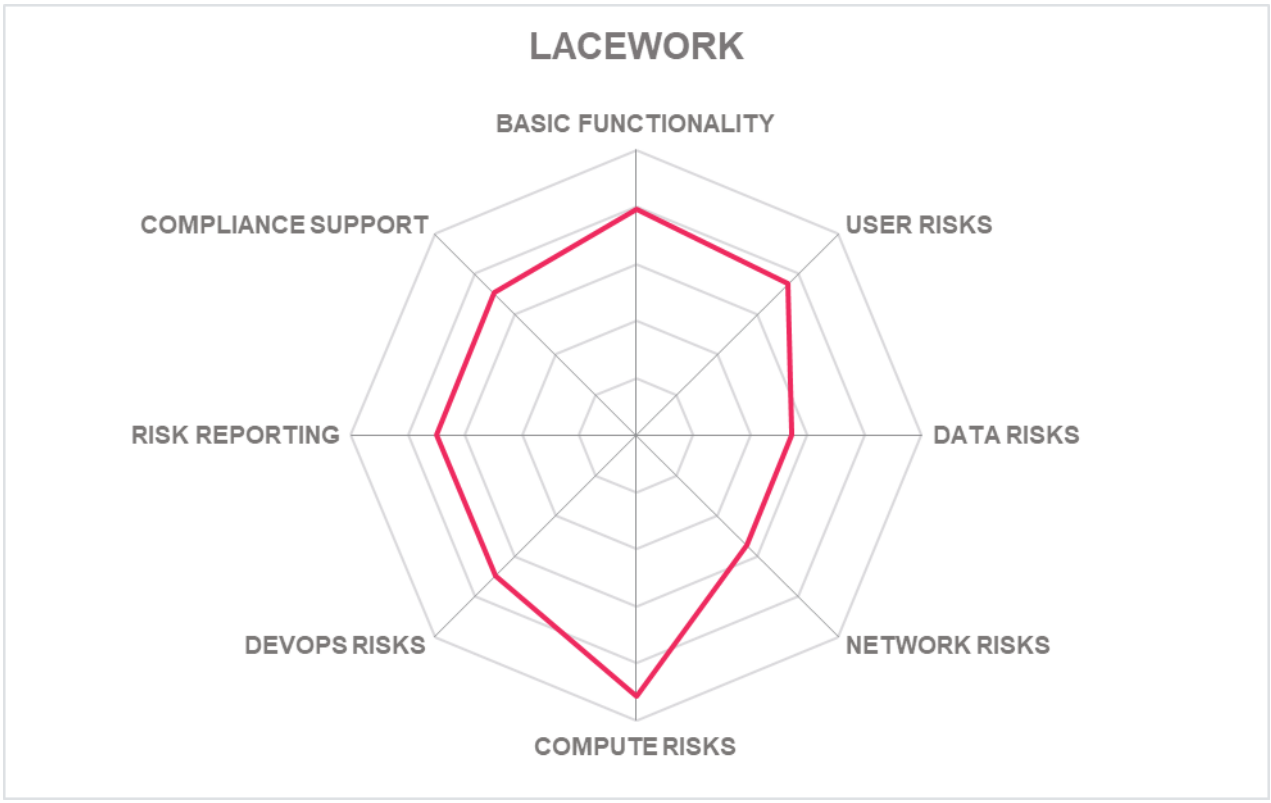
- CSPM solution that is part of a comprehensive CNAPP platform.
- Easy to deploy as an agentless SaaS. Optional agents provide deep insight into running hosts and containers.
- ML and data analytics reduce false positives, help prioritize risks, and determine where remediation is needed.
- Prioritizes 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.
- Integrates with a wide range of common SIEM and workflow / incident management platforms.
- Covers 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.
- Attack path analysis capabilities assess risks based on network path exposure.
- Detects known vulnerabilities and exposures in compute service elements and can also assess for vulnerable software actively in use.
- 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.
- Provides a vulnerability risk score based on industry standards like CVSS and asset specific information within a customer's environment.

Challenges

- Coverage of risks related to the security of data based on content is limited to secrets detected through workload scanning.
- Does not cover compliance risks related to the geographical location where data is stored.
- Does not detect risk related to the configuration of virtual network routing control points such as firewalls.

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


LACEWORK
BASIC FUNCTIONALITY
USER RISKS
DATA RISKS
NETWORK RISKS
COMPUTE RISKS
DEVOPS RISKS
RISK REPORTING
COMPLIANCE SUPPORT

MICROSOFT – 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 cyber security tools. This report focusses 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, 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 CSPM capabilities including agentless vulnerability scanning, container image scanning, attack path analysis, integrated data-aware security posture, and an intelligent cloud security graph. It supports these capabilities for AWS and Google Cloud as well as Microsoft Azure. The solution features Microsoft cloud security benchmark as a built-in standard providing detailed technical guidance for Azure as well as other cloud providers.

The CWPP capabilities of Microsoft Defender for Cloud cover file integrity monitoring, vulnerability assessment for servers and adaptative 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 features “data-aware security posture” capabilities that automatically discover data stores containing sensitive data. Additionally, it provides data flow awareness, which extends beyond the control plane configuration data to highlight the true risk associated with workloads. This helps to identify the resources where vulnerabilities pose the highest risk and therefore aids in prioritizing the actions needed.

Its features agentless vulnerability scanning, including application vulnerability scanning, which provides visibility into the software being used together with known CVEs (Common Vulnerabilities and Exposures) that pose risks if not mitigated. This scanning includes snapshots of storage discs and data for insecure secrets such as security certificates and encryption keys.

The solution provides a dashboard to visualize the security posture and to highlight current threats as well as risk areas in need of improvement. This includes a security score that summarizes the security posture based on the security recommendations. This can be used to track improvements as recommendations are implemented.

It supports securing code by providing capabilities to protect applications and resources from code to cloud across multi-pipeline environments, including GitHub 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 CSPM which provides multi-cloud capabilities including data aware security posture should consider Microsoft Defender for Cloud.

Security	strong positive
Functionality	strong positive
Deployment	strong positive
Interoperability	positive
Usability	strong positive

Table 8: Microsoft's rating

Strengths

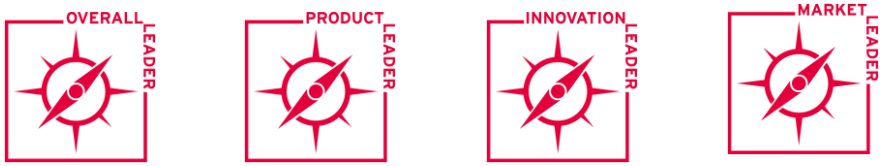
- This solution is part of Microsoft's vision to provide vulnerability, risk, and posture management capabilities beyond the cloud platform, across the whole enterprise IT estate.
- The solution is part of a complete CNAPP platform.
- It covers Azure, AWS, and Google Cloud, with support for additional cloud providers planned.
- It supports automatic and agentless discovery of the cloud data estate including managed and shadow data resources.
- It features "data-aware security posture" capabilities that automatically discover data stores containing sensitive data together with data flows and risks.
- Built-in policies and controls based around the Microsoft cloud security benchmark.
- Out-of-the-box assessment of posture against a very wide range of security best practices and regulatory compliance frameworks as well as support for custom frameworks.
- Built-in integration with Defender External Attack Surface Management, Microsoft Entra Permissions Management and Microsoft Defender Vulnerability Management.
- 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.
- Integrated into CI/CD tools to assess cloud workloads, containers, and IaC artifacts.
- All features are accessible via REST APIs.

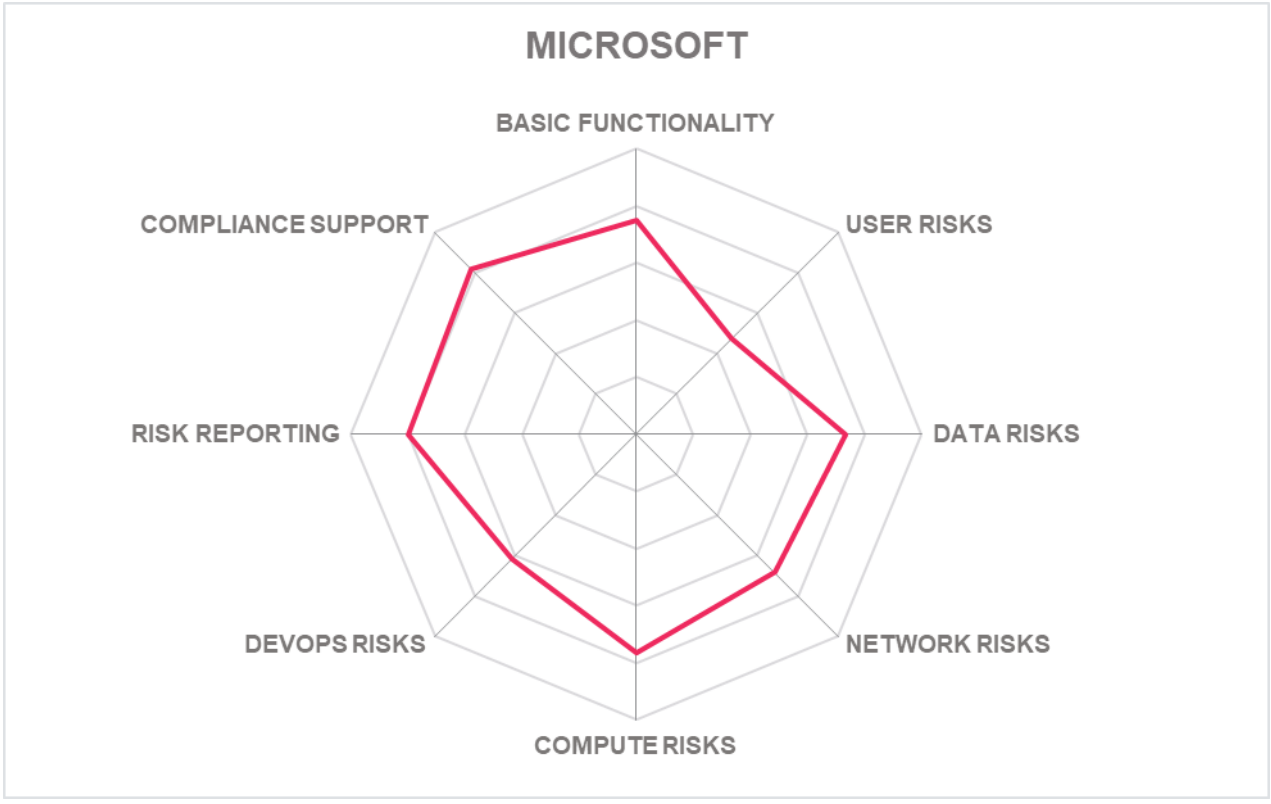
- Defender for Containers include host-level threat detection with over 60 Kubernetes-aware analytics, AI, & anomaly detections based on the runtime workload.
- Integration with workflow / incident management platforms such as ServiceNow to help automate IT workflows.

Challenges

- Delivering on the vision for security posture to cover the entire hybrid IT estate.
- Detection of excessive cloud entitlements relative to policy and usage.
- Detection of cloud administrative orphan accounts.

Leader in





ORACLE – Cloud Guard

Oracle is a major IT software and hardware vendor. Oracle Cloud Infrastructure (OCI) is an IaaS that provides high-performance computing power to run cloud native and enterprise IT workloads in the cloud and on premises. OCI offers a complete range of security capabilities to be used by their tenants and these include Oracle Cloud Guard.

Oracle Cloud Guard is an OCI service that helps tenants to monitor, identify, achieve, and maintain a strong security posture on Oracle Cloud. The tenant can use the service to examine their OCI resources for security weakness related to their configuration and their administrators for risky activities. When Cloud Guard detects weaknesses, it can identify the corrective actions needed and assist or automate their implementation.

Cloud Guard detects security problems within a customer tenancy by ingesting activity and configuration data about the resources in each region. It then processes this data against detector rules and correlates the problems at the reporting region. The problems identified include changes in roles or privileges and suspicious activity around sensitive objects. These are displayed as metrics on dashboards and may also trigger one or more of the responders provided in the solution to help resolve the problem.

Oracle Cloud Guard works together with Oracle Security Zones to provide an always-on security posture. With Security Zones and Cloud Guard the tenant can define policy compliance requirements for groups of resources. Security Zones and Cloud Guard can then enforce these policies automatically correcting and logging any violations.

Targets define the scope of what Cloud Guard is to check. For Oracle Cloud, customers can define multiple targets in multiple regions, and Cloud Guard aggregates all of these for a holistic view. Detectors perform checks and identify potential security issues based on their type and configuration. Oracle Cloud Guard includes Oracle defined checks and the tenant can create their own or modify the ones provided. If any check is triggered, the detector reports a problem. Responders define the actions that Cloud Guard can take when a detector has identified a problem. The available actions depend upon the type of resource and Oracle provides responses which can be used or modified by the tenant. For example, if a protected object storage bucket has been given public access it can automatically remove the public access permissions.

As well as mitigating problems, Cloud Guard provides a Risk Score and a Security Score as measures of the overall security posture. The Security Score provides an assessment of the overall strength of security posture. The Risk Score complements the Security Score by providing an assessment of the total risk exposure of the tenant.

Oracle Cloud Guard features deep integration with other OCI security capabilities including Oracle Data Safe for database security, OCI IAM for identity and access entitlements security, as well as Threat Detection, Threat Intelligence, and Vulnerability Scanning for risk prevention.

Oracle Cloud Guard should be considered by organizations looking to monitor their security posture when using OCI and Oracle Fusion Apps.

Security	positive
Functionality	positive
Deployment	strong positive
Interoperability	neutral
Usability	strong positive

Table 9: Oracle's rating

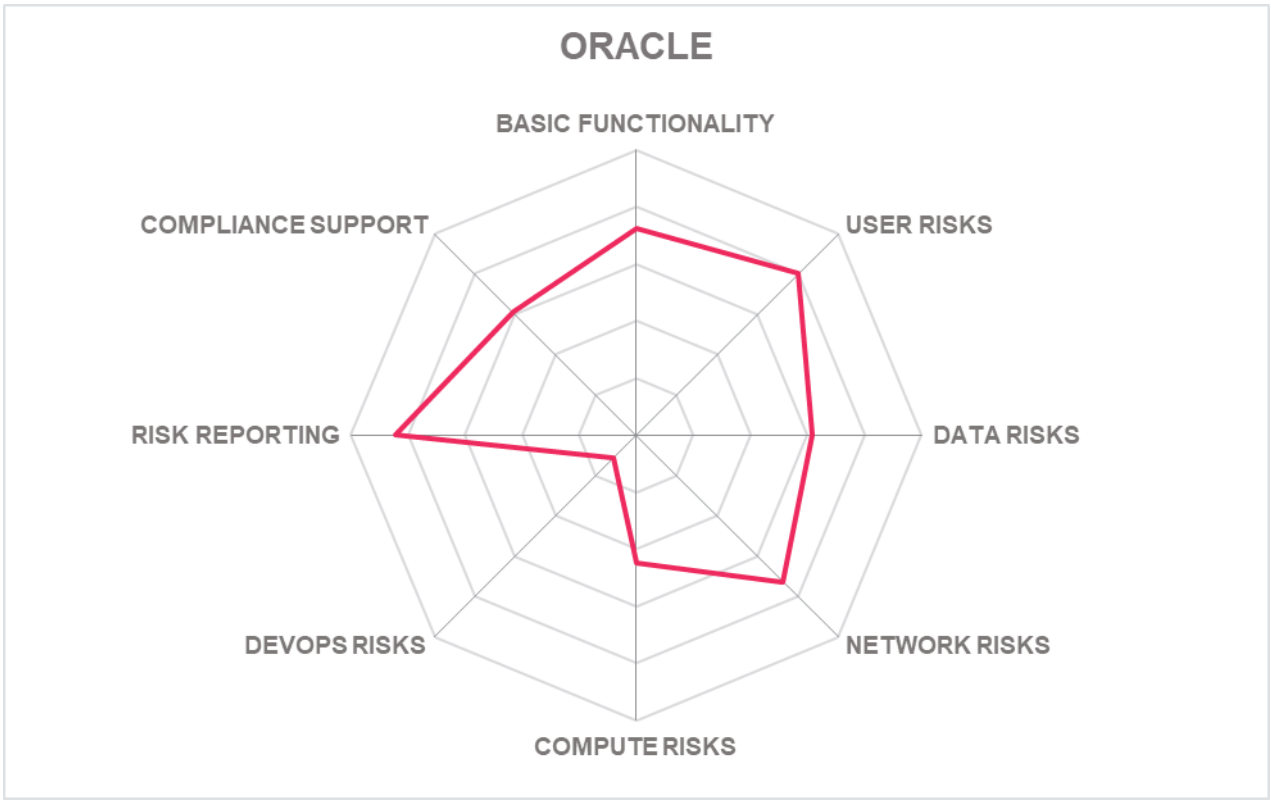
Strengths

- It aligns with the CIS foundation standards for OCI.
- It exploits native integration with OCI capabilities.
- It covers OCI and some Oracle Fusion Apps.
- It enhances the enforcement of posture management for resources included in OCI Secure Zones.
- It detects OCI Object Storage buckets which have public access permissions.
- It monitors for risks in the cloud network configuration.
- It integrates with OCI IAM to detect and manage a wide range of access and entitlements risks.
- In conjunction with Oracle Data Safe, it detects over 170 predefined sensitive data types and enhances the security of data stored in OCI.
- Exploits machine learning algorithms to enhance detection and reduce false alerts.
- Provides automated remediation of detected risky configurations.
- It included many predefined remediate actions based on OCI best practices.

Challenges

- No out-of-the-box policies for common standards or frameworks other than CIS.
- Does detect accounts orphan accounts out-of-the box.
- Does not cover container workload security posture out-of-the box.
- Limited coverage of risks relating to the management of TLS Certificates.
- Does not detect risks related to malware protection not according to policy.
- No support for AWS, Azure, Google, or other major IaaS providers; it only covers OCI and Oracle Fusion Apps.

Leader in


ORACLE
BASIC FUNCTIONALITY
USER RISKS
DATA RISKS
NETWORK RISKS
COMPUTE RISKS
DEVOPS RISKS
RISK REPORTING
COMPLIANCE SUPPORT

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.

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 services such as ECS, EKS, GKE, GCS, AKS, ACI, and AWS Fargate.

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 detects at-risk sensitive data across both the workload and control planes. This includes improperly secured Personally Identifiable Information (PII) such as email addresses, credit card numbers, and Social Security identifiers.

Orca Cloud Security Platform leverages workload and cloud account configuration data to detect and prioritize misconfigurations across the complete cloud estate. Orca supports over 1,000 unique configuration controls across more than 100 compliance frameworks. Each control can generate a unique alert to improve the organization's cloud security posture.

Orca Cloud Security Platform should be considered by organizations looking for a comprehensive and innovative approach to Cloud Security Posture Management.

Security	strong positive
Functionality	strong positive
Deployment	strong positive
Interoperability	positive
Usability	positive

Table 10: Orca Security's rating

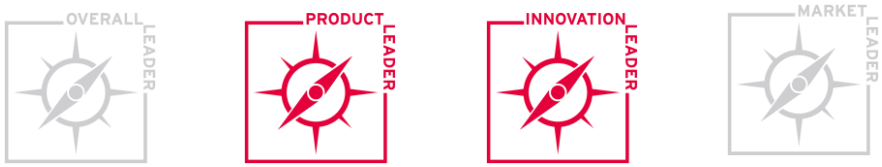
Strengths

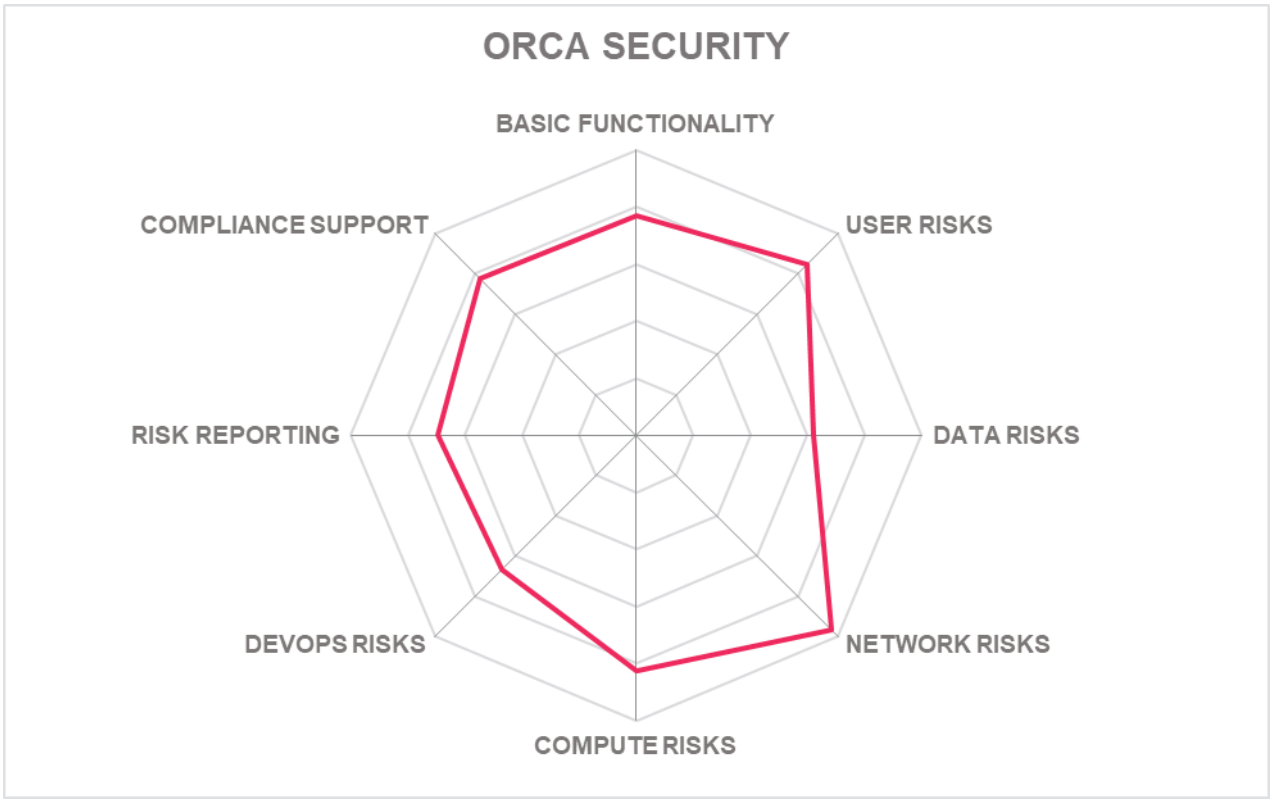
- Orca Security's patented SideScanning™ approach does not require agents and does not impact running workloads.
- Integrates with the Alibaba, AWS, Azure, Google, and Oracle OCI Cloud IaaS services.
- Leverages context-aware intelligence to detect vulnerabilities that could enable lateral movement.
- Prioritizes risks based on the severity of the underlying security issue, its accessibility, and business impact to highlight the most critical issues.
- Integrates with ChatGPT to provide remediation guidance.
- Provides a complete inventory of all customer's cloud assets.
- Automatic scanning of cloud databases for PII exposure and compliance.
- Monitors for risky Identity and Access Management (IAM) misconfigurations.
- Detects vulnerabilities based on data from over 20 data sources.
- Detects security risks, misconfigurations, and vulnerabilities in containers and Kubernetes components.
- 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.
- Detects malware across the cloud estate including paused / idle workloads and orphaned VMs.
- Out-of-the-box third-party integrations, including a wide range of SIEM and workflow / incident management platforms.
- Monitors cloud infrastructure resources including storage buckets, security groups, VPCs, IAM roles and permissions, KMS keys, and more.

Challenges

- Does not directly integrate with Microsoft Azure Active Directory.
- Does not currently cover risks in Red Hat OpenShift.
- Limited detection of vulnerabilities in Kubernetes service accounts.
- Does not support customer defined sensitive data types.
- Only supports OKTA as the source of user accounts and entitlements.

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


ORCA SECURITY
BASIC FUNCTIONALITY
USER RISKS
DATA RISKS
NETWORK RISKS
COMPUTE RISKS
DEVOPS RISKS
RISK REPORTING
COMPLIANCE SUPPORT

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 endpoint security, SOAR, XDR, threat intelligence feeds, Cloud Native Application Protection Platform (CNAPP), and other security products. This report focusses on the CSPM capabilities offered by Prisma Cloud.

Prisma Cloud by Palo Alto Networks is a comprehensive CNAPP, which includes both CSPM and CWPP amongst its capabilities. Prisma Cloud provides visibility across public cloud infrastructure with continuous, automated monitoring that provides insights into threats and vulnerabilities.

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.

Prisma Cloud supports multiple cloud platforms including Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure (OCI) 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 70 compliance frameworks out-of-the-box, and the customer can add custom frameworks.

It provides context-based prioritization of risks. The platform analyses 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 analyses 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.

Prisma Cloud provides visibility into Amazon S3 and Microsoft Azure Storage buckets and objects, including contents by region, owner, and exposure level. It includes predefined data identifiers such as driver's license, Social Security number, credit card numbers, or other patterns to identify and monitor sensitive content. The customer can fine tune this as required. It can also identify and protect against file-based threats that have infiltrated S3 buckets and Azure Storage Blob, leveraging the Palo Alto Networks WildFire malware prevention service.

Prisma Cloud includes predefined policies to assess compliance against a wide range of frameworks and regulations such as PCI, GDPR, SOC 2, and HIPAA and generates audit-ready reports. Palo Alto Networks has obtained many security certifications, including ISO 27001/27018, SOC 2 Type 2, Common Criteria, French ANSSI, German C5, ICSA Labs, UK NSCS, and US FedRAMP.

Organizations looking for CSPM capabilities delivered as part of a much wider security platform should consider Palo Alto Prisma Cloud.

Security	strong positive	
Functionality	strong positive	
Deployment	strong positive	
Interoperability	strong positive	
Usability	strong positive	

Table 11: Palo Alto Network's rating

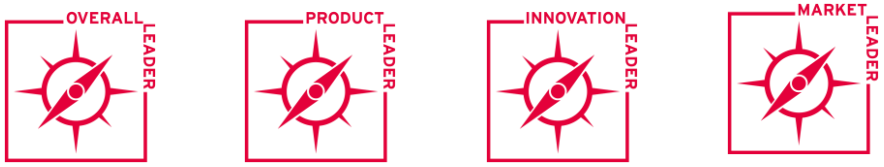
Strengths

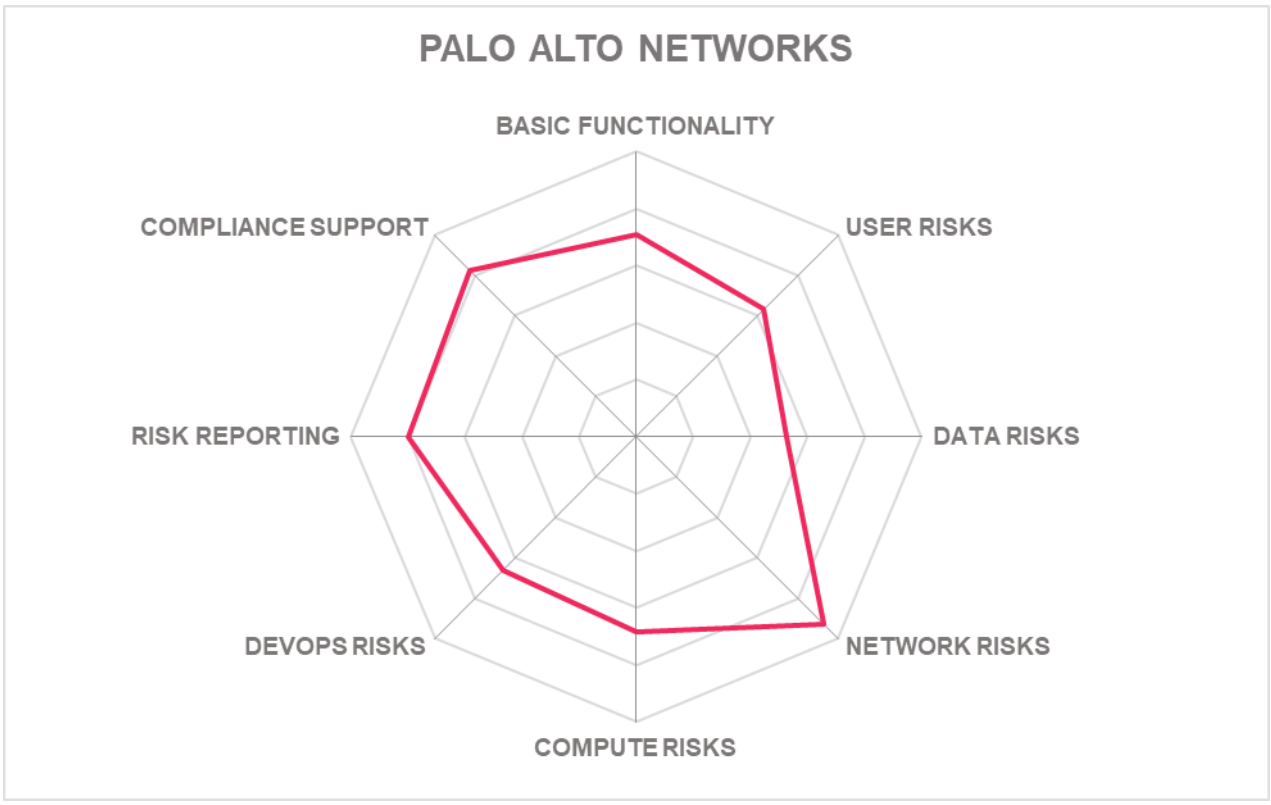
- CSPM capabilities form part of a Cloud-Native Application Security Platform.
- Prisma Cloud also includes CWP and DLP capabilities.
- Provides a single control point for the entire lifecycle of IaaS cloud use.
- Covers all the major public IaaS clouds including Alibaba, AWS, Azure, Google Cloud, and Oracle OCI.
- Identifies risks related to IaC tools such as Terraform, CloudFormation, and Kubernetes YAMLs.
- Out-of-the-box policies that help to govern IAM best practices. These compute a calculation of the net effective permissions a user has based on context.
- Detects and prevents vulnerabilities in container images, functions, hosts as well as IaC templates.
- Helps to implement 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.
- Supports automated remediation of detected deviations from policy.
- Integrates with Continuous Integration (CI) and developer tools.
- Supports Resource Query Language (RQL) for host and serverless vulnerabilities.
- 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 very wide range of regulations such as GDPR, HIPAA, HITRUST, PCI-DSS, and SOX.

Challenges

- Requires subscription to multiple options to get the full benefits.
- Complex subscription model.
- Full data security capabilities depend upon Palo Alto Networks Enterprise DLP and Wildfire.

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


PALO ALTO NETWORKS
BASIC FUNCTIONALITY
USER RISKS
DATA RISKS
NETWORK RISKS
COMPUTE RISKS
DEVOPS RISKS
RISK REPORTING
COMPLIANCE SUPPORT

QUALYS – TotalCloud

Qualys, Inc. is an American company based in Foster City, California, specializing in cloud security, compliance, and related services. Qualys provides cloud-based security and compliance solutions, and this report focusses on Qualys TotalCloud.

Qualys TotalCloud CSPM is a cloud-native, agentless security solution that provides cybersecurity risk and compliance assessment of a customer's cloud infrastructure. TotalCloud CWP (Cloud Workload Protection Platform) supports agent and agentless methods of scanning for vulnerabilities. Qualys TotalCloud can detect vulnerabilities and misconfigurations as well as providing advice on how to mitigate these. It covers workloads running in AWS, Azure, Google, and Oracle OCI cloud services. It provides a complete inventory of the cloud service resources being used.

Qualys TotalCloud CSPM is one element of a complete CNAPP solution covering IaC, CWPP, Cloud Detection & Response (CDR), and Kubernetes container security. It features flexible licensing such that a customer can use licenses against any or all these capabilities. It extends Qualys VMDR (Vulnerability Management Detection and Response) to unify Cloud Security Posture Management and Cloud Workload Protection in a single view with insights into the actions needed. It provides high accuracy scan results, Qualys claim Six-Sigma (99.99966%) accuracy scanning through using multiple scanning approaches to reduce false positives.

The multiple scanning methods that can be used on the same workload, include no-touch, agentless, API-based scanning that can provide scan results in under 5 minutes and snapshot-based scanning. It also provides agent-based scanning and network-based scanning for in-depth assessment. This approach provides more comprehensive results than a single method alone with lower false negatives.

It detects software vulnerabilities across a wide range of assets categories including container images and running containers for vulnerabilities, unapproved images, and over-privileged entitlements. It includes IaC templates that offer visibility to misconfigurations in cloud deployments with support for Terraform, AWS CloudFormation, and Azure ARM, as well as AWS, Azure, and Google Cloud. Qualys Container Security supports major container frameworks, Kubernetes, OpenShift, AKS, EKS, GKE, ECS, Mesos DC/OS, Docker Swarm, and multiple container runtimes.

TotalCloud Unified Cloud Dashboard provides a single risk metric, TruRisk™, as a measure of the total risk from vulnerabilities and misconfigurations across the customer's hybrid multi-cloud IT environment. It also provides a way to view the risk by application, cloud or Qualys tags, or grouping of the cloud accounts. Furthermore, it highlights the remediation actions that could reduce the risk. These include, out-of-box, one-click remediation for more than 50 highly exploited misconfigurations. The customer can use Qualys QFlow™ no-code workflow engine to automate the various assessment and remediation tasks.

Qualys TotalCloud CSPM supports over 30 compliance standards and frameworks such as PCI DSS, HIPAA, NIST CSF, and GDPR out of the box. It also includes over 1,000 predefined controls and the customer can create their own custom controls.

Organizations looking for CSPM as part of a complete CNAPP from a vendor with proven experience in vulnerability assessments should consider Qualys TotalCloud.

Security	strong positive
Functionality	positive
Deployment	strong positive
Interoperability	positive
Usability	positive

Table 12: Qualys' rating

Strengths

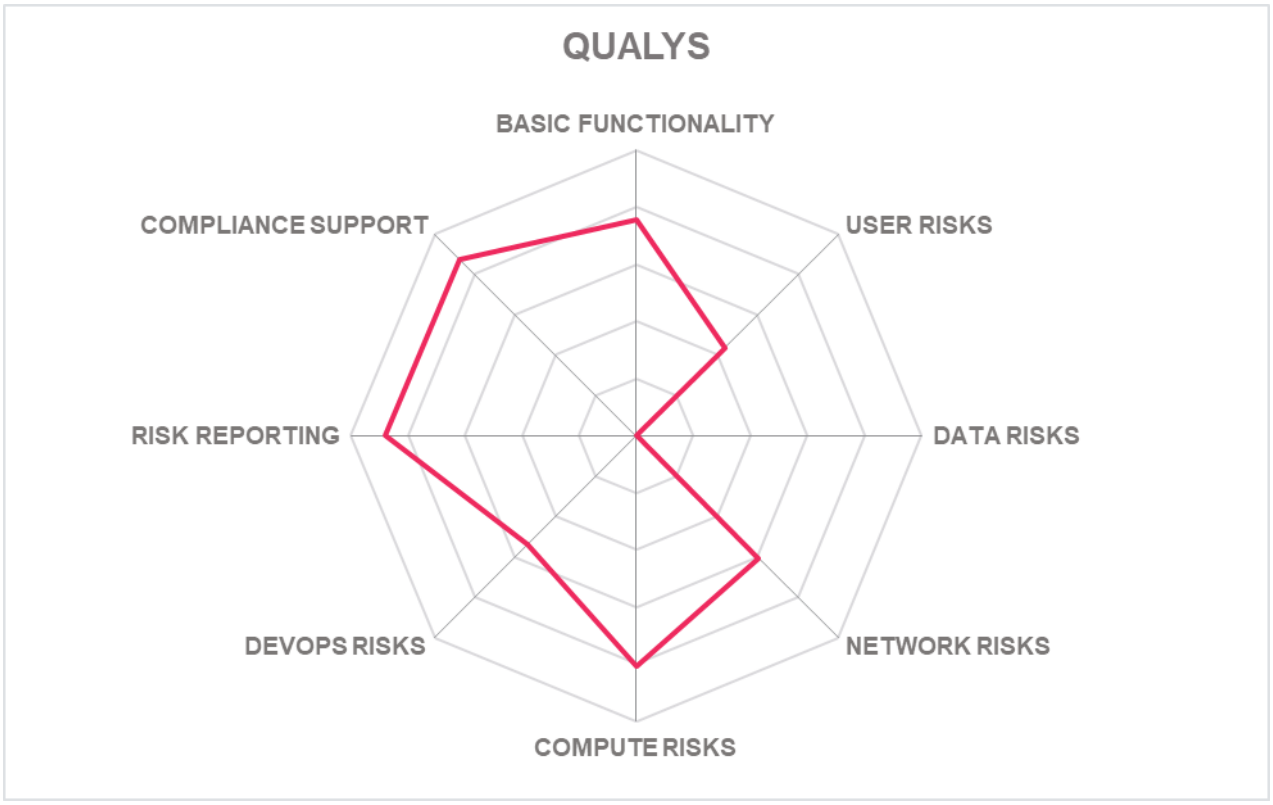
- Solution is part of a complete CNAPP platform.
- Coverage of the major public clouds, AWS, Azure, Google, and Oracle.
- Flexible licensing allows the user to easily adapt the capabilities used.
- Create custom controls and remediations using drag-and-drop no-code workflow UI.
- Multiple assessment options, including agent and agentless, provide high accuracy vulnerability detection.
- High accuracy - Six Sigma level accuracy with insights from over 180k vulnerabilities sourced from over 25+ threat sources.
- Qualys CNAPP platform has CDR capability that can detect active exploitation and mitigate runtime risk by inspecting cloud network traffic with full packet capture.
- Detects a range of risks from excessive user entitlements.
- Provides consolidated security posture for an asset from multiple products.
- Prioritizes misconfigurations, vulnerabilities, and assets based on their business criticality and risk.
- Integrated into CI/CD tools to assess cloud workloads, containers, and IaC artifacts.
- All features are accessible via REST APIs.
- Integration with ITSM solutions such as ServiceNow to help automate IT workflows.
- Out-of-the-box support for a wide range of security frameworks, best practices, and industry regulations.

Challenges

- Does not cover security and compliance risks related to data in the cloud.
- Does not cover risks related to TLS certificate management. This is covered by a separate product called Qualys CertView for certificate management.
- Documentation is only available in English and Japanese.
- Does not detect risks related to accounts without an owner.

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


QUALYS
BASIC FUNCTIONALITY
USER RISKS
DATA RISKS
NETWORK RISKS
COMPUTE RISKS
DEVOPS RISKS
RISK REPORTING
COMPLIANCE SUPPORT

SKYHAWK SECURITY – Synthesis Security Platform

Skyhawk Security was founded in 2022 as a spinoff of Radware's Cloud Native Protector (CNP) business. Skyhawk Security is also supported by a $35M investment from Tiger Global Management. This report focusses on Skyhawk Security Synthesis Platform.

Skyhawk Synthesis helps organizations detect cloud misconfigurations across a wide range of potential issues and provides detailed explanations in terms of their impact and how to fix them. It features risk-prioritized alerts based on an assessment to enable security teams to respond to those with the highest likelihood or impact.

Skyhawk Security leverages malicious behavior indicators to identify attack sequences. Malicious behavior indicators (MBIs) are behaviors and activities built from the metadata and logs collected from the cloud. Skyhawk uses sequences of MBIs, which are stronger indicators of an attack than individual ones, to identify threats. An attack sequence provides a complete overview of how an attacker got in and then moved around the organization. This helps to identify the vulnerabilities and the actions needed in real-time.

Skyhawk Synthesis provides reports on how the cloud services in use comply with internal policies, common industry regulations, and security best practices. These include reports on AWS and Azure alignment with best practices and CIS benchmarks. The reports also cover PCI DSS, SOC2, NIST Cyber Security Framework, ISO 27001, and others to provide high-level verification of compliance status, as well as line-by-line assessment against each individual criterion in the standard. The reports also provide a risk score to help identify the deviations that pose the greatest risk. Skyhawk Synthesis allows the user to create custom policies. These custom policies allow cloud security teams to tailor reporting against those controls that are most relevant to the business needs.

The solution is deployed as SaaS and covers AWS, Azure, and Google Cloud services. It features a GUI based administration as well as secured APIs. It integrates with a wide range of SIEM and workflow / incident management solutions. It covers risks related to users and entitlements, data stored in a wide range of cloud storage services, network misconfigurations, and compute services but does not currently cover risk related to container services.

Skyhawk Security offers a free tier allowing users to monitor misconfigurations and manage compliance and governance free for up to 1,000 assets in their cloud.

This is an innovative solution that features the use of ML to detect anomalous behavior and integration with ChatGPT to provide explanations and background information on risks detected and their remediation.

Security	positive
Functionality	positive
Deployment	strong positive
Interoperability	positive
Usability	positive

Table 13: Skyhawk Security's rating

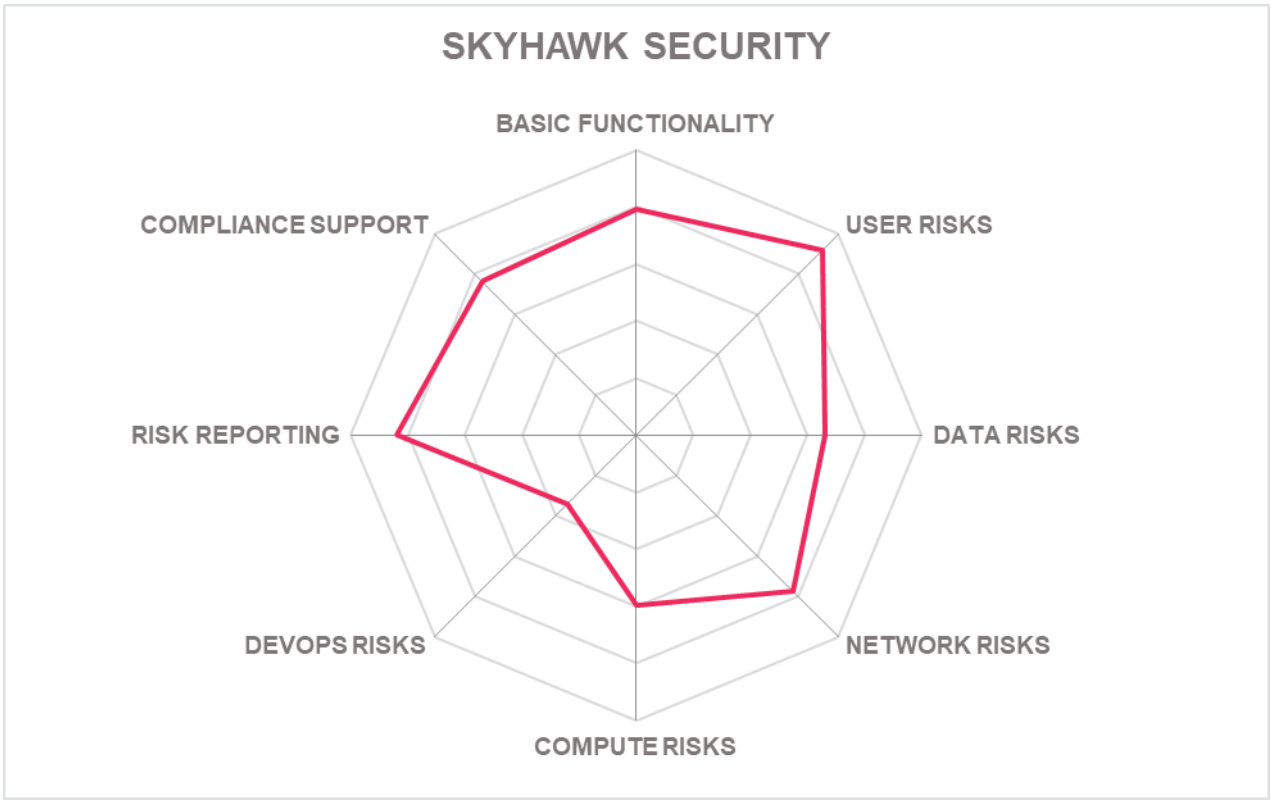
Strengths

- Innovative approach based on exploiting Machine Learning and ChatGPT.
- Detects threats in real time as well as analyses static configurations.
- Integration with Threat Detection to provide an accurate picture of risk.
- Analysis of sequences of events minimizes false alerts.
- Leverages information across their entire customer cloud database to identify misconfigurations that are being exploited.
- Delivered as SaaS without the need for agents eases deployment.
- Detects a wide range of cloud service misconfigurations.
- Supports automated remediation of detected risky configurations.
- Interoperates with SIEM and incident management solutions.
- Free tier CSPM for up to 1,000 cloud assets.
- Dashboards with prioritized reporting of risks and their remediation.

Challenges

- Documentation is only available in English.
- Currently provides limited coverage of risks related to container-based DevOps.
- Does not detect risks related to malware protection not according to policy / best practices. But it does detect the consequences of malware (e.g. crypto mining).
- Does not detect risks related to known CVEs within the compute OS.
- Does not detect risks related to the management of TLS certificates.

Leader in


SKYHAWK SECURITY
BASIC FUNCTIONALITY
USER RISKS
DATA RISKS
NETWORK RISKS
COMPUTE RISKS
DEVOPS RISKS
RISK REPORTING
COMPLIANCE SUPPORT

SYSDIG – Secure

Sysdig was founded in 2013 and has its corporate HQ in San Francisco, CA in the USA. It offers the Sysdig Secure platform which enables teams to secure builds, detect and respond to runtime threats, and continuously manage cloud configurations, permissions, and compliance.

Sysdig Secure CSPM is an agentless solution that is delivered as SaaS and uses API-based queries to access the managed environments. It supports AWS, Azure, Google Cloud, IBM Cloud, and Kubernetes. It 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. It supports common frameworks, regulatory requirements, and internal company policies to assess target environments against security standards.

Sysdig CSPM 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.

Sysdig CSPM supports Policy as Code. It provides a policy 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 and compares these with the policies to detect and remediate any deviations. It supports IaC formats including Terraform, Helm, Kustomize, and YAML.

Sysdig CSPM supports inventory, allowing customers to gain visibility across cloud (Azure, AWS, and GCP) and Kubernetes. Inventory displays all resources from cloud accounts, Kubernetes data sources, and IaC Git resources connected to Sysdig, along with their compliance policy passing score.

Sysdig CSPM supports DevOps security by continuously evaluating IaC artifacts throughout the CI/CD pipeline and workload life cycle. It also analyses 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.

Sysdig Secure 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.

Sysdig Secure analyses the audit logs of all executed cloud commands in an organization's accounts and correlates them with policies, roles, and users. This results in policy suggestions that limit the permissions granted to only those that are needed. Users are

given labels to indicate their level of risk, such as root users, for example. Similarly, resources such as S3 buckets are labelled to highlight those which are most at risk.

Sysdig cloud-native vulnerability management protects workloads throughout their lifecycle by enabling both shift-left best practices (via local machine and CI/CD-integrated scanning) and continuous monitoring of the workloads' vulnerability state in production.

Sysdig CSPM should be considered by organizations looking for preventive and detective posture management, as well as the supporting investigative actions required when a security incident occurs.

Security	strong positive
Functionality	positive
Deployment	strong positive
Interoperability	positive
Usability	positive

Table 14: Sysdig's rating

Strengths

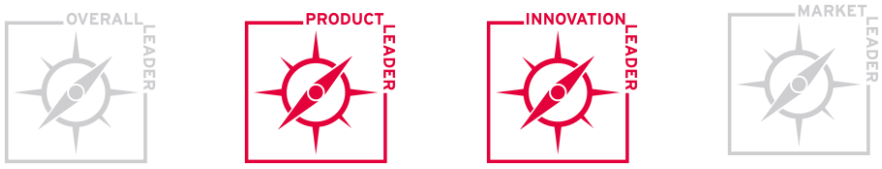
- Agentless and delivered as SaaS helps with rapid deployment.
- Provides visibility into cloud assets, misconfigurations, and suspicious activity.
- Measures security and compliance against a very wide range of frameworks.
- Helps to prioritize risks that need remediation by consolidating issues based on root cause and impact.
- Security and compliance policies based on Open Policy Agent standard.
- Policy creation wizard removes the need to manually code policies.
- Supports the evaluation of Infrastructure as Code throughout the lifecycle.
- Automates remediation through pull requests, playbooks, and manual patches.
- Deep support for Kubernetes and container-based workloads.
- Provides runtime insights through monitoring of cloud workloads, users, and activity.
- Risk Spotlight helps to prioritize the vulnerabilities that pose an actual risk.
- Zones allow users to group resources to represent key business areas.
- Custom policies can be created by editing snippets from out-of-the-box rules.
- Integrates with a wide range of SIEM and workflow / incident management solutions.

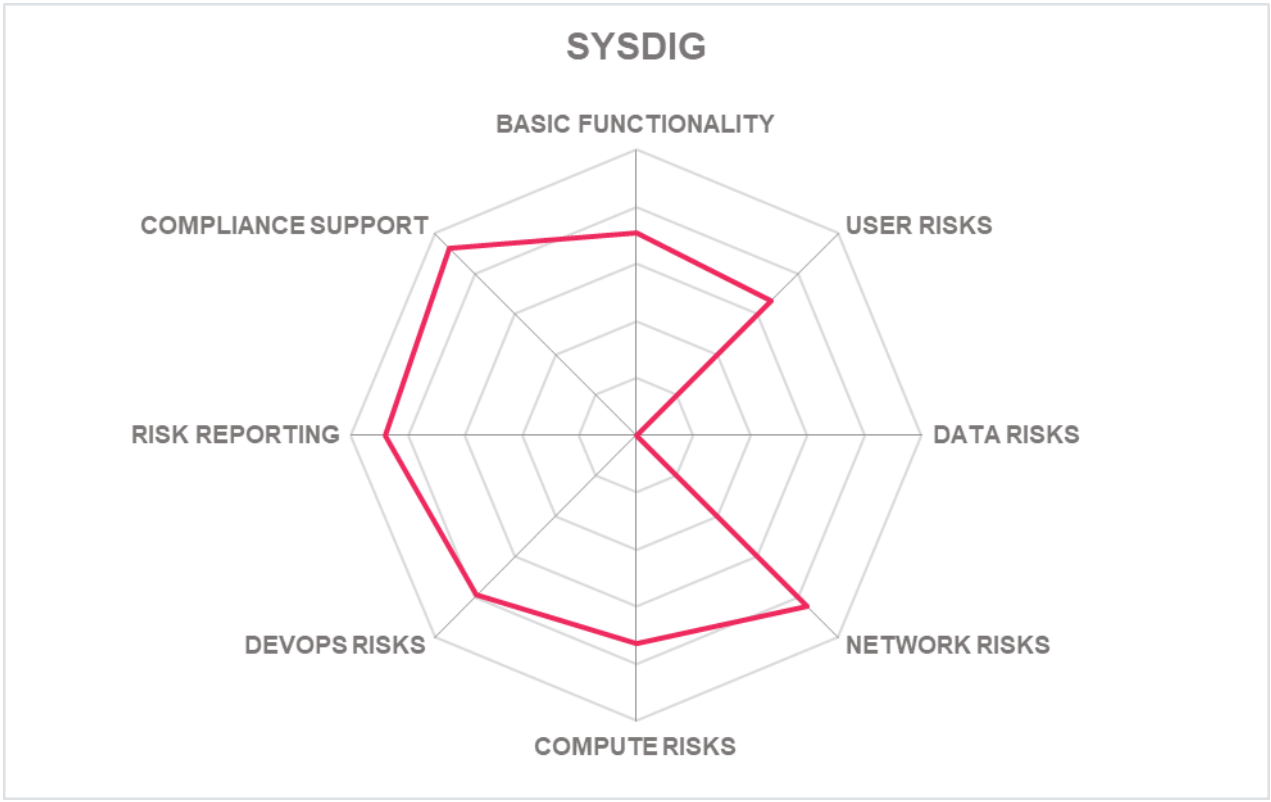
Challenges

- Does not support the evaluation of risks associated with data stored in the cloud.
- Does not integrate with common CMBD platforms out of the box.
- Does not currently support Azure Active Directory and other major identity providers, although Azure and Okta IdP support is on the roadmap.
- Does not detect orphan user accounts.

- Does not currently support Oracle OCI and OpenStack compute service risks.

Leader in





UPTYCS – Unified CNAPP and XDR

Uptycs is a venture funded technology company that was founded in 2016 and has its headquarters in Waltham, Massachusetts. It provides unified solutions for cloud and endpoint security. This report focusses on how the Uptycs unified CNAPP and XDR platform supports CSPM.

The Uptycs unified CNAPP and XDR platform incorporates cloud workload protection, cloud security posture management, cloud infrastructure entitlements management, and cloud detection and response. This 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. This enables their 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.

It 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, and SOC 2. 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.

One of the major threats to cloud environments is misconfigured or excessive account permissions. 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 are actually being used. This helps to establish a least privilege Zero Trust approach.

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.

To include DevOps into the security posture, Uptycs offers Kubernetes security posture management (KSPM) and (CWPP). This provides visibility into the vulnerabilities and compliance of images, containers, pods, and hosts. It integrates with the CI pipeline and includes an embedded gatekeeper (OPA) supporting enforcement as well as auditing.

Organizations looking for comprehensive CSPM capabilities as part of a complete CNAPP and XDR platform should consider Uptycs Unified CNAPP and XDR.

Security	strong positive
Functionality	strong positive
Deployment	strong positive
Interoperability	strong positive
Usability	strong positive

Table 15: Uptycs' rating

Strengths

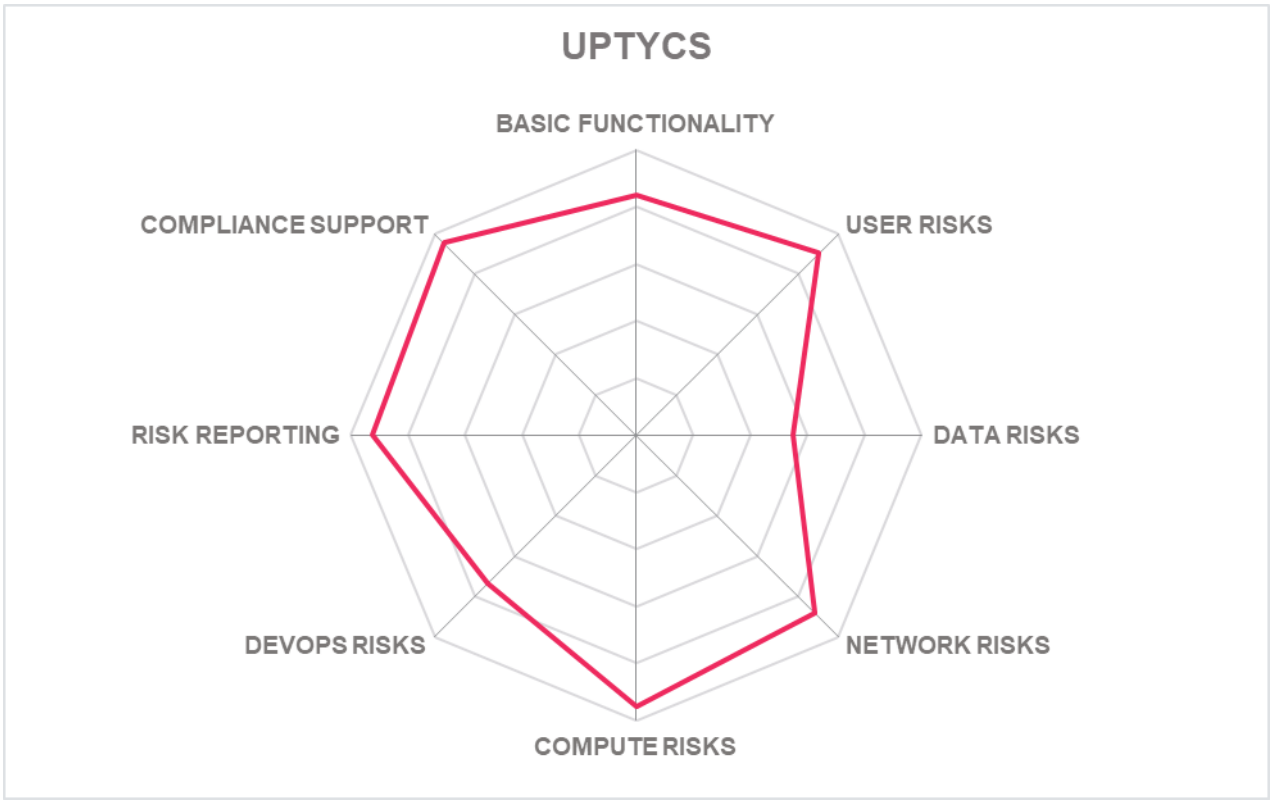
- "Shift up" vision where CSPM is part of an integrated CNAPP and XDR Platform.
- Provides a complete inventory snapshot across all cloud accounts and services.
- Displays continuously updated security metrics through a single dashboard.
- Exposes relationships across resources – including alterations 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 misconfigurations and vulnerabilities that could put user accounts and cloud resources at risk.
- Scans compute instances for over 1000 types of stored secrets.
- Identifies resources like EC2, S3, EFS, Lambda, and RDS that are exposed to inbound internet traffic.
- Discovers risks, vulnerabilities, and exposures across a wide range of cloud compute service environments.
- 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.
- Detected risks are given a risk score classified on severity (high, medium, and low).
- Supports compliance reporting against a wide range of frameworks and standards including NSA, HIPAA, US FedRAMP, PCI, ISO, DISA, and VDA.

Challenges

- Growing the customer base to achieve profitability.
- Expanding the partner ecosystem.
- Does not detect risks related to data stored in cloud DBMs or cloud Data Lakes.
- Does not detect application code vulnerabilities such as SQL Injection.

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


UPTYCS
BASIC FUNCTIONALITY
USER RISKS
DATA RISKS
NETWORK RISKS
COMPUTE RISKS
DEVOPS RISKS
RISK REPORTING
COMPLIANCE SUPPORT

VMWARE – Aria Guardrails

VMware is a technology company with its headquarters in Palo Alto, California. It was founded in 1998 and is a subsidiary of Dell Technologies. It offers VMware Aria, which was previously known as vRealize, which is 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.

This report focuses on VMware Aria Guardrails which is a multi-cloud governance service to help to automate end-to-end policy enforcement across heterogeneous cloud and Kubernetes environments. This is built upon the VMware Aria Platform and uses VMware Aria Graph to capture and map customers' multi-cloud environments including applications, users, configurations, and associated dependencies providing a single view into their complete inventory. It covers all the major hyperscale public clouds as well as infrastructure virtualization environments such as Nutanix, Hyper-V, and OpenStack as well as VMware. However, for non-VMware hypervisors environments, VMware supports workload/container scanning only, not at the hypervisor layer.

It supports policy templates that represent the desired state and the required controls for cloud infrastructure resources. These can be used to detect the security and compliance risks from misconfigured resources as well as from configuration drift. It features out-of-the-box policies for a wide range of security best practices and compliance frameworks. More than 1200 predefined policies map to over 20 industry frameworks including SOC2, HIPPA, NIST 800-53, and MITRE ATT&CK. These can be used to help to ensure that cloud and Kubernetes resources are compliant. The customer can also create their own policies without requiring specific coding skills.

VMware Aria Guardrails supports the governance of cloud service user accounts and entitlements. It can visualize the paths a user can take to access a cloud resource by mapping relationships between a human user or workload, entitlements, and resources. This helps to identify risks from unexpected attack paths and to ensure that entitlements are not excessive.

It supports DevOps security and compliance through integration with Kubernetes. VMware Aria Guardrails integrates with CI/CD pipelines to ensure that security policies are enforced throughout the software development lifecycle.

For workloads, VMware Aria Guardrails includes OS configuration and compliance management capabilities with a broad set of out-of-the-box application-aware content, event-driven detection of configuration changes, and automated remediation. It also can scan the environment for OS-level system vulnerabilities, cross-checking against common vulnerabilities and exposures (CVEs) and mitigate security risks for hosts from these.

It supports a Zero Trust approach to network security. Aria Networks' Network Assurance and Verification feature supports intent-based verification of network policies including segmentation.

Organizations looking for comprehensive hybrid multi-cloud security and compliance posture management solution as part of wider management platform should consider VMware Aria Guardrails.

Security	strong positive
Functionality	strong positive
Deployment	strong positive
Interoperability	strong positive
Usability	strong positive

Table 16: VMware's rating

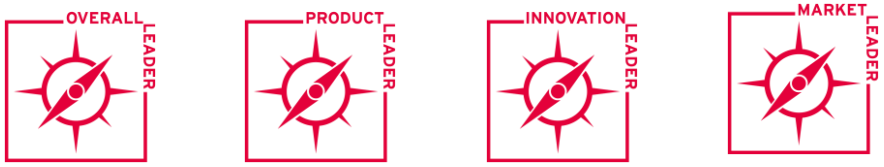
Strengths

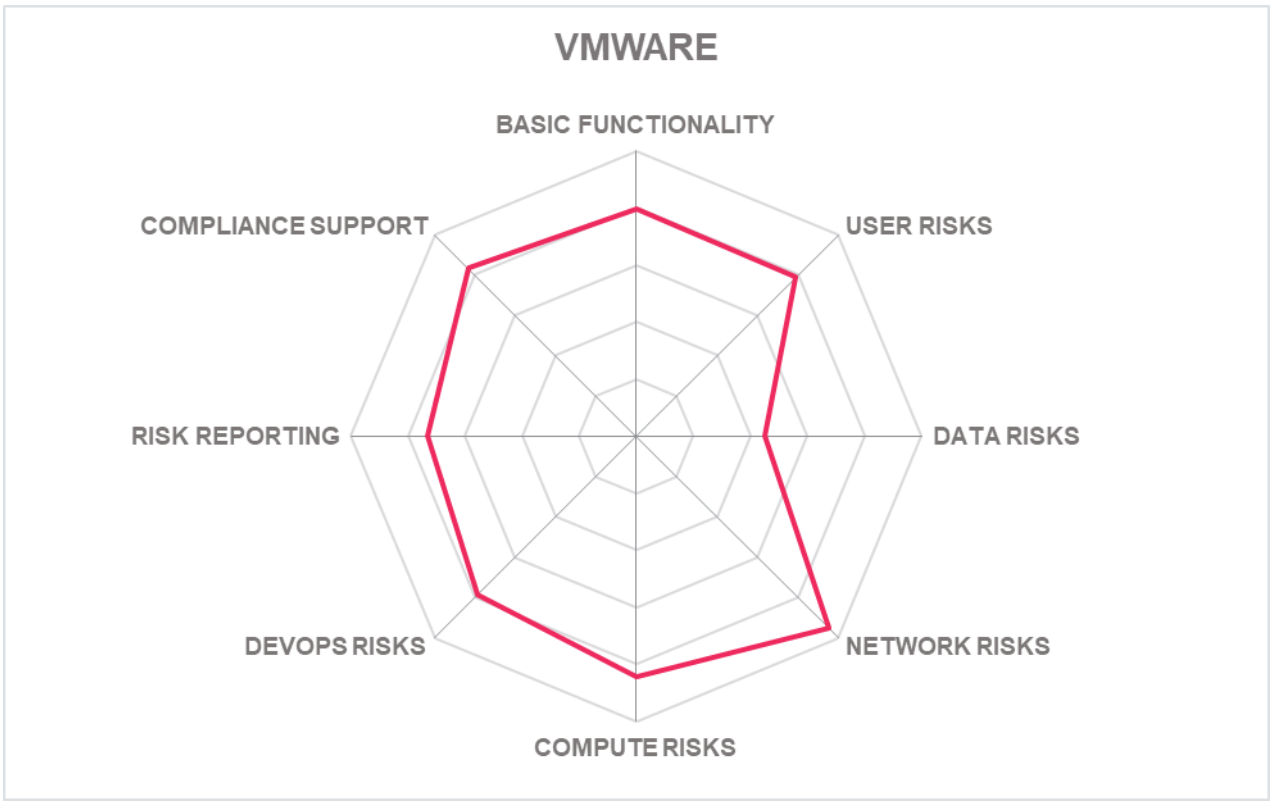
- VMware Aria Guardrails is part of comprehensive hybrid multi-cloud governance platform.
- Delivered as SaaS and not requiring agents makes for easy deployment.
- Covers a wide range of services from the major public cloud service providers.
- Supports on-premises as well as cloud deployments.
- Provides a common visualization and data model that covers multiple service environments and deployment models.
- Comprehensive range of policies and rules out of the box.
- Automated policies (IaC) support compliance from when an account is created.
- Fast detection, VMware claims 95% of risks are detected within 6 seconds of change.
- Comprehensive coverage of Zero Trust network related risks.
- Integrates with Kubernetes and CI/CD pipeline to detect DevOps related risk.
- Maintains a real-time history of events that can be used for forensics.
- Supports automated remediation of detected risky configurations.
- Does not require blanket elevated permissions to take remedial actions.
- Integrates with a wide range of CMDB platforms out of the box.
- Provides out of the box detection for configuring encrypting data at rest and in transit for cloud services such as block storage, databases, object stores.
- Interoperates with a wide range of SIEM and incident management solutions.
- Good coverage of user and entitlements risks for people, devices, and services.
- Automatic recommendation of least privilege policies based on permission usage.

Challenges

- Does not cover risks related to the security of data based on content.
- Does not cover compliance risks related to the location where data is stored.
- Does not include out-of-the-box scanning of data in transit or at rest.
- Only supports Azure Active Directory as the source for user accounts and entitlements. Expanding this is on the roadmap.
- Does not cover Red Hat OpenShift, OpenStack, and Oracle OCI compute service risks.

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


VMWARE
BASIC FUNCTIONALITY
USER RISKS
DATA RISKS
NETWORK RISKS
COMPUTE RISKS
DEVOPS RISKS
RISK REPORTING
COMPLIANCE SUPPORT

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, vulnerability management, IaC scanning, CIEM, DSPM, and container and Kubernetes security. This report focusses on the CSPM aspects of this platform.

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.

It 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, PCI, 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 integrates into the CI/CD pipeline to detect and prevent security misconfigurations and vulnerabilities early in the development cycle. It provides CI/CD guardrails supporting a single set of policies covering container and VM image scanning, IaC template scanning, and Kubernetes Admission Control.

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. 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.

It helps to assess the security posture against more than 100 built-in frameworks such as CIS, PCI, NIST, HIPAA, and GDPR. The misconfiguration rules are mapped to the control lists and recommendations of each framework. It can provide a compliance score for each framework, and a heatmap of overall compliance posture. It can generate compliance reports which can be as granular as required.

Organizations looking for a CSPM solution that is part of a comprehensive CNAPP platform should consider Wiz.

Security	strong positive
Functionality	strong positive
Deployment	strong positive
Interoperability	strong positive
Usability	strong positive

Table 17: Wiz' rating

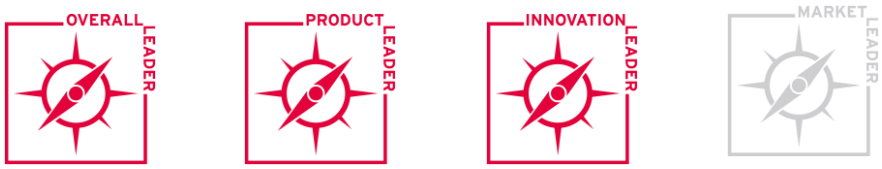
Strengths

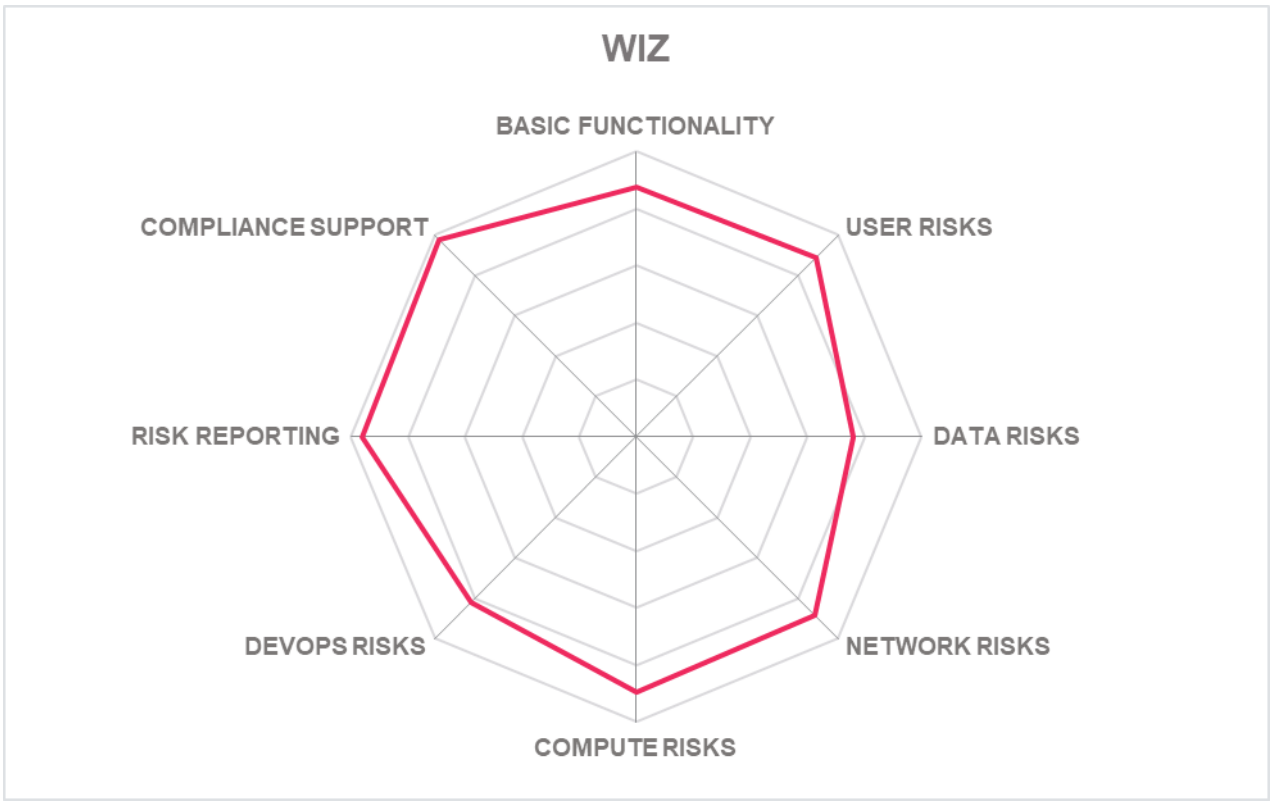
- Delivered as an agentless SaaS for easy and rapid deployment.
- Covers a wide range of environments - Alibaba Cloud, AWS, Azure, Google Cloud, Oracle Cloud, Kubernetes, and VMware
- Comprehensive functionality - CNAPP that includes CSPM, KSPM, CWPP, Vulnerability Management, IaC scanning, CIEM, DSPM 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, and identities.
- Identifies the toxic combinations of issues that in combination represent the major risks.
- Provides an analysis of chains of exposures and attack paths to high value assets.
- Provides out-of-the-box compliance status reports against over 100 frameworks such as CIS, PCI, NIST, HIPAA.
- Supports custom policies using Rego, the language used by OPA (Open Policy Agent).
- RBAC based controls allow multiple teams to monitor and remediate their own areas within the overall cloud usage.
- Integrates into the CI/CD pipeline to detect and prevent security misconfigurations and vulnerabilities early in the development cycle.
- Integrates with a wide range of workflow / incident management solutions.
- Integrates with a wide range of SIEM solutions.

Challenges

- Relatively young but fast-growing organization.
- Does not yet integrate with SAP HANA.
- Does not cover OpenStack as a cloud environment.
- Limited list of integrations with cloud vendor specific databases and data lakes.
- Some limitations around the detection of risks related to TLS certificates.
- Support and documentation are only available in English language.

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


WIZ
BASIC FUNCTIONALITY
USER RISKS
DATA RISKS
NETWORK RISKS
COMPUTE RISKS
DEVOPS RISKS
RISK REPORTING
COMPLIANCE SUPPORT

Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other vendors in the market that readers should be aware of. These vendors do not fully fit the market definition but offer a significant contribution to the market space. This may be for their supportive capabilities to the solutions reviewed in this document, for their unique methods of addressing the challenges of this segment or may be a fast-growing startup that could become a strong competitor in the future.

Aqua Security

Was founded in 2015, Aqua with its headquarters in Boston, MA and Ramat Gan, Israel. It provides a Cloud Native Application Protection Platform covering the application lifecycle from code to cloud.

Why it is worth watching: the platform includes some CSPM capabilities such as compliance reporting. Aqua Security claims that it can stop cloud native attacks across the application lifecycle offers a $1M Cloud Native Protection Warranty to guarantee it.

AWS

AWS provides a broad range of security services to protect users of its cloud. These include Amazon GuardDuty a security monitoring service that analyzes and processes foundational data sources such as AWS CloudTrail management events, AWS CloudTrail event logs, VPC flow logs (from Amazon EC2 instances), and DNS logs.

Why it is worth watching: AWS Security Hub provides a comprehensive view of high-priority security alerts and compliance status across AWS accounts. This provides CSPM capabilities for organizations that only use AWS.

Balbix

Balbix is a US company that was founded in 2015 and has its headquarters in San Jose California. It offers the Balbix Security Cloud™ which is a cybersecurity posture automation platform.

Why it is worth watching: the Balbix Security Cloud™ is a cybersecurity posture automation platform that ingests data from security and IT tools to create a unified view of cyber risk in financial terms based on the value of assets and the likelihood of occurrence.

Barracuda Networks

Barracuda Networks was founded in 2003 and has its headquarters in Campbell, California. In 2022 the global investment company KKR & Co. Inc. acquired Barracuda networks. It offers the Barracuda Cloud Security Guardian.

Why it is worth watching: Barracuda Cloud Security Guardian is a software platform for public-cloud security and compliance orchestration. It continually scans infrastructure to

detect misconfigurations, enforces security best practices, and can automatically remediate violations.

Caveonix

Caveonix was founded in 2019 and has its headquarters in Reston, Virginia. It offers unified cloud security posture management and cloud workload protection solution as well as CNAPP.

Why it is worth watching: Caveonix Cloud's CSPM covers hybrid multi-cloud environments. The platform's AI based Neural-Insight™ Engine helps provide risk analytics to guide prioritized risk management activity and remediation.

Cymulate

Cymulate was founded in 2016 and has its headquarters in Israel. It provides a breach and attack simulation platform as SaaS. Its platform enables companies to simulate end-to-end attacks, to measure and track their security performance, and to focus efforts based on the insights that this provides.

Why it is worth watching: This platform is effectively an extended security posture management solution that covers IT assets wherever they are implemented, not just cloud.

Ermetic

Ermetic was founded in 2019 and has its headquarters in Tel Aviv, Israel. Ermetic provides a full asset inventory for AWS, Azure and GCP. This covers cloud infrastructure, workloads, identities, and data.

Why it is worth watching: Ermetic CSPM is part of an identity-first cloud native application protection platform (CNAPP). It provides visibility into attack vectors that could exploit cloud identity entitlements and resource settings. It also supports compliance reporting against a wide range of best practice frameworks.

Fidelis Cybersecurity

Fidelis Cybersecurity was founded in 2002 and has its headquarters in Bethesda, Maryland. Fidelis CloudPassage Halo® includes cloud security posture management capabilities that provide visibility across hybrid environments, automate threat and data theft detection, support threat hunting, and help to optimize incident response.

Why it is worth watching: Fidelis CloudPassage Halo is a cloud-native application protection platform (CNAPP) that covers the infrastructure asset lifecycle to help protect, detect, remediate, and improve security for public, private, hybrid and multi-cloud environments.

IBM

IBM is a multinational technology corporation headquartered in Armonk, New York. The Posture Management component of IBM's Cloud® Security and Compliance Center provides

capabilities that can help to assess, reduce, and manage risk resulting from reduced visibility, complex compliance requirements and misconfiguration across public multi-cloud.

Why it is worth watching: IBM has experience in helping organizations in highly regulated industry sectors such as finance and telecoms to meet their compliance obligations and can provide tailored solutions for these.

Netskope

Netskope was founded in 2012 and has its headquarters in Santa Clara, California. Netskope Cloud Security Posture Management is a service that provides insights into the security posture of an organization's public cloud resources. It utilizes Netskope's API-enabled controls and real-time protection capabilities to discover misconfigurations, provide remediations, and monitor compliance.

Why it is worth watching: Netskope CSPM combines API-enabled controls with real-time inline protection to assess public cloud deployments for risks, threats, and compliance issues such as insecure data.

Skyhigh Security

Skyhigh Security was founded in 2011 and has its headquarters in Plano, Texas. It offers Skyhigh Security Cloud-Native Application Protection Platform (CNAPP) which includes CSPM and CWPP capabilities. It provides comprehensive discovery and risk-based prioritization, and Shift Left to detect and correct misconfigurations.

Why it is worth watching: Skyhigh Security CSPM extends to data protection by using the same DLP, malware detection and threat protection policies in Skyhigh CASB.

Sophos

Sophos is a cybersecurity company that was founded in 1985 with its headquarters in Abingdon in the UK. It offers Sophos Intercept X for Servers which includes a range of capabilities including Cloud Native Security, Extended Detection and Response and Cloud Security Posture Management.

Why worth watching: This is a mature security solutions vendor and its CSPM capabilities cover Amazon Web Services, Microsoft Azure, and Google Cloud workloads in addition to other critical cloud services such as serverless functions, databases, and S3 buckets.

Symantec

Symantec is a cyber security solutions vendor that was founded in 1982. In 2019 Symantec was acquired by Broadcom and the Symantec brand name is used for Broadcom cybersecurity products. Symantec Cloud Workload Assurance is a Cloud Security Posture Management solution for public cloud IaaS platforms, including AWS and Microsoft Azure.

Why it is worth watching: Symantec Cloud Workload Assurance integrates with other Symantec products such as Symantec CloudSOC, CASB and Symantec Cloud Workload Protection to deliver a unified view into cloud security and compliance posture.

Trend Micro

Trend Micro is a global cybersecurity company that was founded in 1988 and has its headquarters in Irving, Texas, USA. As part of the Trend One unified cybersecurity platform, Trend Cloud One™ delivers application security capabilities across all major cloud providers and integrates with commonly used DevOps tools.

Why is it worth watching: Trend Cloud One Conformity provides visibility and monitoring of cloud infrastructure, compliance scans against a wide range of security and compliance frameworks as well as CI/CD integration.

Zscaler

Zscaler is a cloud security company that was founded in 2007 and has its headquarters in San Jose, California. Zscaler offers Posture Control, which is a cloud native application protection platform, this includes built in CSPM policies covering cloud infrastructure and native applications deployed across multi cloud environments.

Why worth watching: as well as identifying and remediating risks and from misconfigurations in IaaS, and PaaS Zscaler Cloud Security Posture Management also covers those in SaaS.

Methodology

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market which you should consider for product decisions. It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report does not provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements against product features, i.e., a complete assessment.

Types of Leadership

We look at four types of leaders:

- Product Leaders: Product Leaders identify the leading-edge products in the particular market. These products deliver most of the capabilities we expect from products in that market segment. They are mature.

- Market Leaders: Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack of global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- Innovation Leaders: Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- Overall Leaders: Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas, but they become Overall Leaders by being above average in all areas.

For every area, we distinguish between three levels of products:

- Leaders: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.
- Challengers: This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- Followers: This group contains vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, and other sources.

Product rating

KuppingerCole Analysts AG as an analyst company regularly evaluates products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview of our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Deployment
- Interoperability

- Usability

Security is primarily a measure of the degree of security within the product/service. This is a key requirement. We look for evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer, including authentication measures, access controls, and use of encryption. The rating includes our assessment of security vulnerabilities, the way the vendor deals with them, and some selected security features of the product/service.

Functionality is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

Deployment is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree to which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logical and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly, and ineffective IT infrastructure.

Vendor rating

We also rate vendors on the following characteristics:

- Innovativeness
- Market position
- Financial strength
- Ecosystem

Innovativeness is measured as the capability to add technical capabilities in a direction which aligns with the KuppingerCole understanding of the market segment(s). Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors because innovative vendors are more likely to remain leading-edge. Vendors must support technical standardization initiatives. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

Market position measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active. Therefore, being weak in one segment does not lead to a very low overall rating. This factor considers the vendor's presence in major markets.

Financial strength: even while KuppingerCole does not consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor.

Rating scale for products and vendors

For vendors and product feature areas, we use a separate rating with five different levels, beyond the Leadership rating in the various categories. These levels are:

Strong positive	Outstanding support for the subject area, e.g., product functionality, or outstanding position of the company for financial stability.
Positive	Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative

	entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.
Neutral	Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for are not met, while others are well served. For Market Position, it could indicate a regional-only presence.
Weak	Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.
Critical	Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets such as Germany, Russia, or the US.

However, there might be vendors which do not appear in a Leadership Compass document due to various reasons:

- Limited market visibility: There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- Declined to participate: Vendors might decide to not participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the market segment.
- Lack of information supply: Products of vendors which do not provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- Borderline classification: Some products might have only a small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The target is to provide a comprehensive view of the products in a market segment. KuppingerCole will provide regular updates on their Leadership Compass documents.

We provide a quick overview about vendors not covered and their offerings in chapter Vendors to Watch. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

Related Research

Leadership Compass - SASE Integration Suites | KuppingerCole

Leadership Compass: Security Orchestration Automation and Response (SOAR) (kuppingercole.com)

Leadership Compass - Cloud Backup for Ransomware Protection | KuppingerCole

Leadership Compass - Security Orchestration Automation and Response (SOAR) (kuppingercole.com)

Leadership Compass - Privileged Access Management | KuppingerCole

Leadership Compass - CIEM & Dynamic Resource Entitlement & Access Management (DREAM) platforms (kuppingercole.com)

Leadership Compass - Identity Governance and Administration 2022 | KuppingerCole

Leadership Compass - Container Security | KuppingerCole

Copyright

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 customers@kuppingercole.com.