CNAPP Buyer's Guide

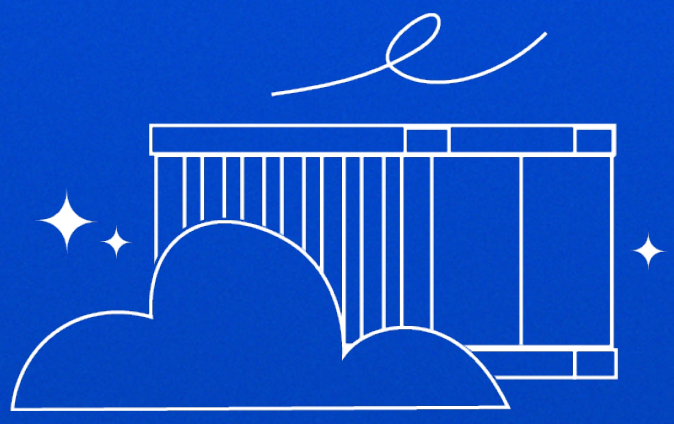


Table of Contents:

Introduction

The cloud enables organizations to innovate faster than they have ever been able to before. With the rapid growth of cloud environments and the dynamic nature of the cloud, there are constantly new security risks that organizations need to look out for.

It is challenging to manage cloud security manually, and organizations use a variety of security tools to secure their cloud environments, such as Cloud Security Posture Management (CSPM), Cloud Workload Protection Platform (CWPP), and others. Cloud-Native Application Protection Platforms (CNAPP) consolidate these different tooling into a single comprehensive and unified platform, that helps protect cloud-native applications by identifying risks across the different risk factors and correlating them to find toxic combinations.

Based on the 2023 CNAPP Market Guide, Gartner predicts that by 2026, 80% of enterprises will have consolidated security tooling for the life cycle protection of cloud-native applications to three or fewer vendors, down from an average of 10 in 2022. This guide is intended to help you choose a comprehensive and tightly integrated CNAPP that is the best fit for your organization by examining the key capabilities of a CNAPP and providing a Request for Proposal template for evaluating a CNAPP.

Challenges with cloud security

The cloud has introduced new types of security risks

Cloud environments are complex. The cloud allows organizations to add new resources on demand, from virtual machines to serverless functions to containers. There are constantly new types of services getting introduced to a dynamic and scalable environment. This makes it challenging to secure an environment that can grow and change in minutes. The cloud also simplifies actions, such as making it possible to expose a resource to the internet at the click of a button, resulting in further risks of misconfigurations. With so many different types of services and configurations, organizations need a solution to help them ensure they are staying secure as their environment changes. This complexity also introduces new types of attack paths on the cloud, which requires organizations to have a threat detection and response strategy in place that is built for cloud-native attacks.

Visibility gaps and blind spots

To gain visibility into this complex environment, organizations often use security tools that rely on agents to provide them with visibility into their workloads. Agent-based solutions result in blind spots in the environment, as resources that don't have the agent set up are simply not protected by the tool. These visibility gaps in the security posture can result in critical issues going unnoticed, and lead to a breach.

Siloed tooling and operational challenges

To set a security foundation on the cloud, organizations often use standalone security tools such as vulnerability management, data security posture management, Kubernetes security posture management, cloud security posture management, and others. Gartner talks about this approach to security in the CNAPP Market Guide 2023:

> **This lack of integration creates fragmented views of risk with insufficient context individually making it difficult to prioritize the actual risk.**

As described, using standalone tools creates siloes in security posture and operational challenges, as each tool requires unique expertise and process per tool. In addition, to understand risk criticality, organizations need to manually correlate risks across the different tools resulting in further operational overhead.

Alert fatigue

Siloed tools lack the context around each risk, for example, a vulnerability management solution can identify if a machine is vulnerable, but it is not aware if the machine is also exposed to the internet, or if it has high privileges. The lack of context results in the inability of the tools to identify which risks are more critical than others and leads to them creating a lot of noise and alert fatigue. This makes it hard for teams to identify the actual critical risks in their environment and prioritize them. Gartner also addressed this challenge as “fragmented tools create excessive alerts, wasting developers’ time and making remediation efforts confusing to target roles.“.

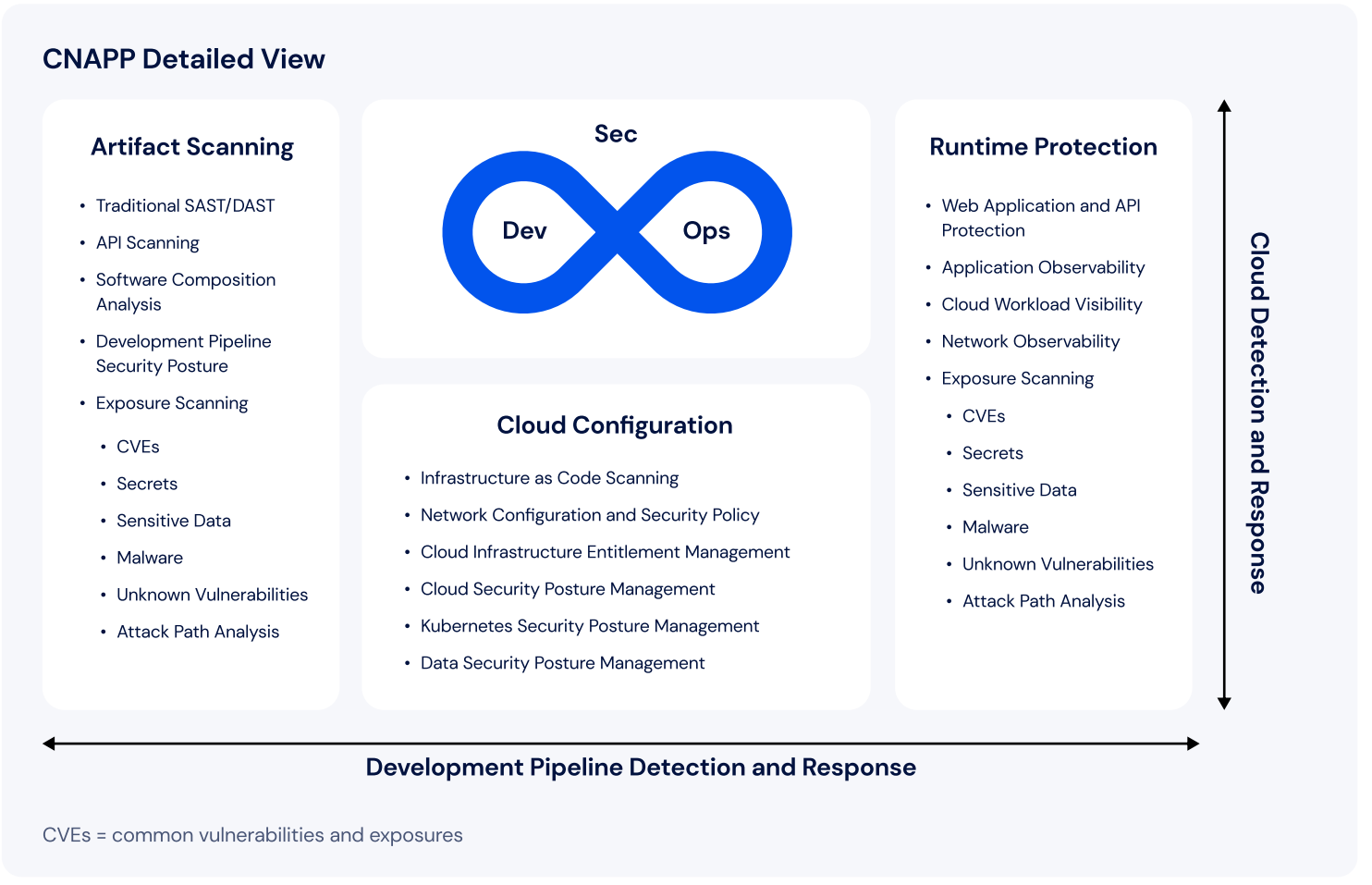
Gaps between the security team and developers

The security team is responsible for ensuring the security of the cloud environment, however, developers are the ones spinning up resources in the cloud. This results in security slowing down innovation, as described by Gartner “Security teams are perceived as slowing down modern DevOps style development. Security controls weren’t designed for the speed and scale of cloud-native applications and weren’t designed with the developer as the central customer (not security)”. In addition, developers often don’t have visibility into the risks related to their resources, and even when they do, they are unable to prioritize them successfully as they lack context and prioritization.

What is CNAPP and why organizations need it

As defined by Gartner, “Cloud-native application protection platforms (CNAPPs) are a unified and tightly integrated set of security and compliance capabilities designed to secure and protect cloud-native applications across development and production. CNAPPs consolidate a large number of previously siloed capabilities, including container scanning, cloud security posture management, infrastructure as code scanning, cloud infrastructure entitlement management, runtime cloud workload protection and runtime vulnerability/configuration scanning.”.

When evaluating a CNAPP solution, these are key capabilities you should look out for in a vendor:



Complete visibility into cloud environments

Visibility across all clouds

A CNAPP should provide complete visibility into your cloud environment, no matter what cloud your workloads run in, whether it is AWS, GCP, Azure, Alibaba, OCI, or other clouds you are in.

Visibility across all resources

A CNAPP should be comprehensive in its coverage and provide visibility into every resource in your environment, including virtual machines, serverless functions, containers, databases, managed services, and any other cloud service you use. A CNAPP should also normalize the different types of resources from the different clouds so you can have a consistent platform with consistent visibility spanning all clouds.

Visibility across all risk factors, from prevention to detection

CNAPP should provide cohesive visibility into all risk factors including vulnerabilities, network exposures, secrets, malware, identities, and sensitive data, as well as visibility into threats in real-time, to give you the full picture of your security posture.

Remove blind spots with agentless visibility

A CNAPP should ensure full coverage and no blind spots in the security posture by using an agentless approach to provide visibility into cloud environments, utilizing the Cloud Service Provider's (CSP) APIs to detect and scan for resources and workloads, rather than relying on agents that must be configured and maintained.

Holistic solution replacing point solutions

Unified approach to security

A CNAPP provides you with one platform, one process, and consistent controls across all environments. Based on Gartner's CNAPP Market Guide, when evaluating a CNAPP "All services should be fully integrated, not loosely coupled independent modules.". A fully integrated CNAPP replaces all point solutions with one single platform that covers all security aspects, removing the need for a unique process per tool and reducing operational overhead.

Unified risk engine

A CNAPP uses a unified risk engine to identify risks across CSPM, CWPP, CIEM, Kubernetes Security Posture Management (KSPM), Data Security Posture Management (DSPM), and IaC scanning. Gartner summarized this as:

> CNAPP offerings allow an organization to use a single integrated offering to identify risks across the entire life cycle and disparate elements of a cloud-native application.

Defense in depth strategy

A comprehensive CNAPP provides a complete defense in depth cloud security strategy. It starts from prevention, through agentless visibility and risk reduction, to the last line of defense being detection and protection from threats from inside the workload, through a lightweight agent. A CNAPP with defense in depth provides full end-to-end visibility into attacks, enabling faster, more efficient response.

Single pane of glass

A CNAPP does not only have visibility into all risk factors, but also correlates all risks to understand how risks combine to result in a toxic combination in an environment that can create an attack path. CNAPP models risks on a security graph to provide the complete context around risks. Garner also recommends that a CNAPP has a single front-end console with a unified back-end data model to reduce switching between multiple consoles.

Prioritized risks with context

Context

A fully integrated CNAPP can identify the context around risks and find attack paths in an environment, enabling organizations to understand the real criticality of risks in their environment. Using a security graph, CNAPP is also able to provide a deep understanding of relationships between all elements in the cloud environment.

Prioritization

A contextual CNAPP is able to prioritize risks based on criticality, and only surfaces the issues you should really pay attention to so your team can focus on the risks that matter. Gartner recommends that a CNAPP should have “Integrated advanced analytics that are combined with the graph to prioritize risks” Prioritization allows teams to spend less time responding to distracting noise, and more time remediating critical issues.

Bridge between development and security teams

Reduce time spent remediating issues in production

A CNAPP can integrate security checks into CI/CD pipelines to scan for risks during development. It enables you to apply unified security policies across production and the CI/CD pipeline to prevent issues from reaching production in the first place. In the CNAPP Market Guide, Gartner recommends to "Reduce complexity and improve the developer experience by choosing integrated CNAPP offerings that provide complete life cycle visibility and protection of cloud-native applications across development and staging and into runtime operation".

Enable developers to ship faster and more securely

CNAPP empowers developers with the context, prioritization, and specific remediation guidance they need to fix issues related to the resources they own. Context and prioritization enable developers to stay agile and move fast while staying secure. Gartner described this requirement as:

> Because security is often viewed as an obstacle to developers, it is absolutely critical to prioritize risks identified and provide sufficient context for the developer to remediate it.

Key components of CNAPP

A fully integrated CNAPP consolidates the following security tools into a single platform that covers and correlates all capabilities below:

Cloud Security Posture Management (CSPM)

A CSPM provides visibility into the configuration of cloud resources and continuous detection of resources. CSPM evaluates cloud resources against misconfiguration rules to identify resources that are not configured properly. It also helps ensure compliance by providing built-in and customized compliance standards and frameworks, and automatic remediation to remediate non-compliant resources. CSPM allows you to evaluate resources in development to prevent misconfigurations from reaching production.

Cloud Workload Protection Platform (CWPP)

CWPP provides visibility into cloud workloads and risk reduction without any agents across VMs, containers, and serverless functions. CWPP scans for vulnerabilities, secrets, malware, and secure configurations in workloads, and allows you to shift left to identify workload misconfigurations and vulnerablities in CI/CD pipelines. For the last line of defense, CWPP provides real-time detection of threats using a lightweight agent that is correlated and enriched with context from the agentless visibility and risk reduction.

Cloud Infrastructure Entitlement Management (CIEM)

CIEM helps manage entitlements in cloud environments, it provides guidance for least privilege permissions in the cloud and helps right-size access and entitlement in your environment. It also analyzes effective permissions for all principals and resources and identifies leaked secrets or credentials that could be used to access sensitive assets.

Kubernetes Security Posture Management (KSPM)

KSPM helps automate security and compliance for Kubernetes components. KSPM provides complete visibility into your containers, hosts, and clusters and has deep risk assessment across vulnerabilities, misconfigurations, permissions, secrets, and networking and correlates all risks to provide context and prioritization. KSPM also enables you to shift left to identify and prevent Kubernetes security issues in development.

Data Security Posture Management (DSPM)

DSPM protects your sensitive data on the cloud. It discovers all your sensitive data and provides visibility into where the data is located, across buckets, data, OS and non-OS volumes, and managed and hosted databases. DSPM correlates your sensitive data with underlying cloud context and other risk factors to understand how data assets are configured and used and how data moves within your environment. A fully integrated DSPM can identify attack paths to your sensitive data so your team can prioritize issues before they become breaches.

Cloud Detection and Response (CDR)

CDR allows you to detect, investigate, and respond to cloud threats by monitoring activity in your cloud environment and detecting any suspicious events. While you proactively remove attack paths in your environment through agentless risk reduction, you still want to ensure you can detect any threats in real time. A CDR identifies threats and suspicious behavior in real time such as remote code execution, malware, crypto-mining, lateral movement, privilege escalation, and container escape. It provides you with end-to-end visibility, automatically correlating threats across real-time signals, cloud activity, and audit logs, to uncover attacker movement in your cloud so you can respond rapidly andlimit the impact of a potential incident.

Importance of having agentless visibility and risk reduction

Full coverage removing blind spots

Agent-based solutions only protect a workload if they are deployed on it. This can result in blind spots in the security posture, leading to vulnerable resources that can go unnoticed and result in risks getting exploited. CNAPP provides agentless visibility and risk reduction and automatically detects new cloud workloads and protects them without the need to configure agents, providing full coverage and removes any blind spots in the security posture.

Faster deployment

Agent-based solutions for visibility and risk-reduction can take time to set up and configure to protect your entire cloud environment. Agentless CNAPP enables organizations to protect their entire environment in minutes, by using the cloud provider's APIs to scan for resources. Agentless scanning also allows for a much easier and seamless onboarding to the platform and automatically protects your environment as it grows without the need to configure anything.

Improves operational efficiency

Agents have high TCO, require ongoing maintenance, and impact the performance of the workload, resulting in operational challenges that slow down innovation. This operational overhead was also described by Gartner, “With modern cloud-native applications, it can be difficult if not impossible to use a traditional host-OS-based agent approach. In some cases, the DevOps product teams won’t accept them, and in other cases, the value of runtime visibility into ephemeral workloads is not offset by the operational overhead of deploying and managing agents”. A CNAPP with agentless visibility and risk reduction reduces operational costs and removes the burden of having to configure and maintain agents.

Importance of a fully integrated CNAPP

Unified risk engine

A CNAPP should be the one platform that covers all risk factors across vulnerabilities, network exposures, secrets, malware, identities, and sensitive data, as well as real-time threat detection. With a unified risk engine, the platform can provide the real criticality of risks by understanding how risks combine to create an attack path in your environment. The platform automatically correlates all risks, across prevention to detection, and removes the need for manual correlation, enabling organizations to focus on remediating critical risks instead. Based on the Gartner report:

> All services should be fully integrated, not loosely coupled independent modules. Integration should include the front-end console, unified policy across multiple points of inspection and a unified back-end data model.

Graph-based context

A CNAPP should provide a graph-based context around risks. The node-and-edge structure is a best practice for graphs, making it much more intuitive to define queries that represent risks. Having a graph-based view also makes it easy for anyone at any skill level to understand relationships between resources and context around risk, so they can respond to issues faster. Gartner described this as a key characteristic for a CNAPP:

> Deep understanding of relationships between the elements of an application (VMs, containers, service functions and storage), security posture, permissions and connectivity, typically enabled by underlying graph database technology.

Prioritization

A CNAPP that has a fully integrated set of features can prioritize risks better, by correlating all risks and identifying toxic combinations and their real criticality. A CNAPP should provide a single queue of prioritized risks to allow teams to focus on the most important issues and spend less time on distracting noise.

Shift-left

Once risks were identified and prioritized in production, a CNAPP should enable organizations to shift left to scale security across the development lifecycle. By providing integration with CI/CD pipelines, a CNAPP allows organizations to identify risks early on in development and ensure they don't reach production from the first place. This results in fewer issues the security team has to remediate in production and allows them to focus on broader initiatives. Gartner also discusses this, "By integrating security testing throughout the life cycle and directly into the developer's toolset versus one large test prior to production, CNAPP offerings enable fixing problems earlier and speeding application deployment. "

Contextualized detection and response

Cloud-native development introduces unique attack vectors that are challenging to identify before and after exposure. To have an effective detection and response strategy, defenders need to be aware of the attack paths in their environment so they can better understand the blast radius of an attack. Before exposure, a CNAPP should provide the ability to proactively remove attack paths in an environment through contextual risk reduction. After exposure, the CNAPP should enable defenders to detect threats in real-time based on cloud events and runtime signals and allow them to limit blast radius based on cloud context. Correlating runtime signals and cloud events with cloud and infrastructure risks allows defenders to respond rapidly to threats and limit the impact of a potential incident.

Request for proposal (RFP)

Inventory	
What Code technologies do you provide visibility into? (Frameworks, Libraries, Software Build Systems, Collaboration Software, Scripting Languages, etc.)	
What CI/CD tools do you provide visibility into?	
What Compute Platforms do you provide visibility into? (Cloud Subscriptions, Container Services, Serverless, Virtual Machines, Operating Systems, Networking, etc.)	
What Application and Data Platforms do you provide visibility into?	
What Security and Identity tools do you provide visibility into?	

Can you identity all Cloud services including those not supported for risk assessment?
Describe the visibility you provide into Workloads across VMs, Containers, and Serverless Functions.
Demonstrate level of visibility into managed Kubernetes across EKS, AKS,GKE, and OKE.
Demonstrate visibility into non-public Kubernetes API endpoints via private endpoints.
Do you generate resource mapping relationships? Explain what relationships you map.
Can you easily flag unwanted technologies in our environment?

Governance and Secure Config
Demonstrate support for compliance frameworks [SPECIFIC FRAMEWORKS].
Demonstrate support for OS and applications compliance benchmarks [SPECIFIC BENCHMARKS].
Demonstrate support for custom compliance frameworks.
Demonstrate support for OS and applications compliance benchmarks [SPECIFIC FRAMEWORKS].
Ability to create compliance reports based on account/subscription.
Demonstrate ability to compare compliance posture across multiple frameworks in one view.
Do you provide the ability to apply compliance frameworks to any level of operation (cloud provider, account, grouping of resources)?
Do you provide the ability to disable/enable or create policy exceptions as required?
Demonstrate ability to prove compliance via reporting with timestamps.
Do you provide a library of security policies?
Do you provide the ability to build custom security policies?
Do you provide a library of host configuration policies?
Do you provide ability to build custom host configuration rules?
Demonstrate ability to detect weak authentication of assets (e.g., VMs with password enabled SSH authentication that are publicly exposed).
Demonstrate ability to detect high risk configuration findings.

Risk Assessment	
Demonstrate ability to monitor and report on the most critical attack vectors across network, identity, vulnerabilities, secrets and configuration analysis.	
Demonstrate ability to prioritize security issues according to the environmental layout (e.g., External exposure, assumed privileges, business impact).	
Demonstrate ability to detect vulnerabilities on VM's, Containers, and Functions.	
Do you have the ability to detect vulnerabilities on powered off VM's?	
Demonstrate detection of weak authentication methods on VM's, Containers, and Functions.	
Demonstrate ability to detect exposed secrets on VM's, Containers, and Functions.	
Do you provide the ability detect end of life version of defined software packages?	
How do you generate automated risk scoring to prioritize resource risk?	
Demonstrate ability to detect systems that require restart.	
How do you manage the detection of multiple occurrences of the same misconfiguration on a resource?	
Demonstrate ability to detect API services without authentication set.	
Demonstrate ability to query functionality for custom searching.	
Do you provide the ability to customize and export query results?	
Demonstrate ability to provide complete audit trail of all user activities within platform.	
Do you scan for malware across cloud environments?	

Vulnerability and Patch Management	
Demonstrate ability to detect vulnerabilities in container images.	
Demonstrate ability to detect vulnerabilities in currently running containers.	
Demonstrate ability to detect vulnerabilities in container images without repository access	
Demonstrate ability to detect vulnerabilities in container images hosted in a container registry	
Do you provide the ability to scan private container registry?	
Demonstrate ability to detect vulnerabilities in container images in self-deployed docker/Kubernetes	
Demonstrate ability to detect vulnerabilities in VMs	
Demonstrate ability to detect vulnerabilities in Functions	
Demonstrate ability to detect library-based vulnerabilities in VMs and containers (e.g., Python, Java).	
Detail the level of context provided for vulnerabilities.	
Provide examples of advanced queries on vulnerabilities.	
Demonstrate ability to determine if a detected vulnerability is active on a workload	
Demonstrate ability to detect vulnerabilities on publicly exposed resources.	
Demonstrate ability to detect vulnerabilities on highly privileged resources.	
Demonstrate ability to detect vulnerabilities on critical risk assets.	
Demonstrate ability to detect unpatched OS on compute nodes and instance groups.	
Demonstrate ability to detect unpatched OS on compute nodes and instance groups.	

Demonstrate ability to detect publicly exposed unpatched VMs and containers.	
Demonstrate ability to detect publicly exposed containers running on a compute node with unpatched kernel	
Demonstrate ability to detect end-of-life Hosted technologies running on public facing compute instance	
Demonstrate ability to detect highly privileged unpatched assets and assets with critical risk.	
Provide list of threat and vulnerability databases you source information from.	

Exposure Analysis

Demonstrate ability to provide network reachability map of resources and workloads.	
Demonstrate ability to detect publicly exposed resources and containers.	
Demonstrate ability to detect Kubernetes clusters with publicly exposed APIs.	
Demonstrate ability to detect ingress rules on any port and destination.	
Do you provide built-in intelligence that is able to identify known suspicious IPs connecting to workloads?	
Demonstrate ability to detect poorly separated network traffic.	
Demonstrate ability to detect resources accessible from other subscriptions.	
Demonstrate ability to detect geo-location traffic from unrecognized regions.	
Demonstrate ability to detect resources accessible from other Vnets.	
Demonstrate ability to detect all resources exposed publicly behind load-balancers.	
Demonstrate ability to provide intuitive visual interface to analyze & investigate network traffic in either north-south or east-west directions.	

CIEM	
Demonstrate ability to detect who has access to specific resources.	
Demonstrate ability to detect users/roles with elevated permissions on resources.	
Demonstrate ability to detect over-privileged permissions on containers.	
Demonstrate ability to detect over-privileged permissions on serverless workloads.	
Demonstrate ability to detect exposed secrets on VMs, containers, and functions.	
Demonstrate ability to detect exposed secrets on public and private buckets	
Demonstrate ability to detect secrets (certificates, access/ encryption keys, cleartext data, etc.)	
Demonstrate ability to detect lateral and cross-account movement via compromised access keys or stolen permissions.	
Demonstrate ability to identify cloud services that can access data.	
Demonstrate ability to find inactive admin users and groups.	
Demonstrate ability to find exposed SSH private keys.	
Demonstrate ability to detect weak password for local users in managed and self-managed Databases	
Demonstrate ability to detect exposed private keys of domain certificates	
Demonstrate ability to find resources using service accounts with admin permissions.	
Demonstrate ability to find certificates nearing expiration and exposed certificates.	
Demonstrate ability to find cleartext cloud keys allowing high privileges.	
Demonstrate ability to find attack path to high value assets.	

CDR	
Demonstrate ability to collect Cloud Audit logs from any supported Cloud Providers.	
Do you provide the ability to explore who did what on where and when?	
Demonstrate ability to correlate resources with events.	
Demonstrate ability to detect and alert on architecture configuration changes.	
Demonstrate ability to detect and alert on Failed API activities or Failed Resource access.	
Do you provide any mechanism or capability to validate external exposure?	
Demonstrate ability to view what an attacker will see from the outside.	
Demonstrate ability to detect and alert on misconfigured APIs	
Demonstrate ability to detect secret and sensitive data in HTTP response of externally exposed resources	
Do you provide the ability to add custom threats feeds?	
Demonstrate ability to find any instance of a specific file via its custom hash.	
Do you provide the ability to monitor unwanted changes in important files at the OS level?	

Real-time Threat Detection	
Are you able to generate a process tree that includes the vulnerable elements when a threat is detected?	
Are you able to merge vulnerability context with other risk factors (e.g., cloud identity, network exposure, configuration exposure, data findings) to enable comprehensive detection of potentially toxic combinations ?	
Demonstrate ability to detect the execution of a crypto miner	
Demonstrate ability to detect container escape	
Demonstrate ability to detect remote shell attacks e.g., webshell, reverse-shell)	
Demonstrate ability to detect container drifts (execution of processes that are not part of the original image)	
Demonstrate ability to detect malicious/suspicious network activity – lateral movement	
Demonstrate ability to detect privileges escalation	
Demonstrate ability to identify and flag any processes or files associated with known malicious software based on an established database of malware signatures.	
Demonstrate ability to prioritize unusual runtime behavior on a container when its risk is heightened due to toxic combinations such as having access to a Kubernetes service account.	
Are you able to prioritize running vulnerabilities when their risk is amplified due to compounding factors such as network exposure?	

Security Automation	
List the ticketing platform(s) you support.	
Provide details on workflow actions for notifications.	
Demonstrate ability to generate rule sets based on conditions and criteria.	
Demonstrate ability to send notifications with context on risk (can be customized to enrich if required).	
List what SIEM tools are supported.	
List what SOAR tools are supported and remediation playbooks available.	
Do you support auto-remediation? Provide examples and details.	
List what vulnerability management and response tools are supported.	
Demonstrate ability to obtain recommendations against misconfigurations and to execute auto-corrective actions.	
Demonstrate ability to generate management policies for CSPs (AWS SCP, Azure Policy) for preventive control.	

DevSecOps	
Demonstrate ability to integrate controls as part of a deployment pipeline to validate infrastructure-as-code (IaC) is compliant with defined policies.	
Demonstrate ability to validate IaC templates are compliant before enterprise use.	
Demonstrate ability to scan VM images (e.g., AMI) and container images for vulnerabilities and exposure.	
Demonstrate ability to scan container images for exposed secrets in the CI/CD pipeline.	
Demonstrate ability to scan virtual machine images for exposed secrets in the CI/CD pipeline.	
Demonstrate ability to block misconfiguration or unauthorized container image before they are deployed on the kubernetes cluster.	
List what CI/CD tools you integrate with.	
List customer references who have successfully implemented a DevSecOps strategy using your product.	

DSPM	
Demonstrate ability to identify sensitive data (PII, PCI, PHI and secrets)	
Do you provide the ability to scan public and private cloud storages (AWS S3, Azure Blob Storage and GCP Cloud Storage)?	
Do you provide the ability to scan managed and self-hosted SQL databases?	
Do you provide the ability to scan managed and self-hosted No-SQL databases and identify sensitive data?	
Do you provide the ability to scan workload OS and non-OS disks and identify sensitive data?	
Do you provide ability to scan data warehouses?	
Do you provide the ability to ingest classified tags from external sources like BigID or Macie?	
Demonstrate ability to detect unintentionally moved or copied between environments, regions, or clouds	
Demonstrate ability to detect and alert on externally exposed workloads (VM, container, Serverless) with possible lateral movement to sensitive data	
Demonstrate ability to detect and alert on externally exposed cloud storage with sensitive data	
Demonstrate ability to create custom classifiers	
Demonstrate ability to assess data compliance posture against industry compliance frameworks (I.e PCI DSS, HIPAA, NIST)	
Demonstrate ability to detect suspicious and unwanted behavior on sensitive data based on cloud events in near-real time	
Demonstrate ability to detect unused data	
Demonstrate ability to detect cross-boundary data access such as outside of organization, cross-subscriptions, and cross-regions	
Do you have the ability to generate a data findings report?	

General Operability	
Describe your deployment architecture. Are agents or additional deployments required? Do you support Outpost?	
Describe how services are integrated to each other	
Do you provide a single security policy across all artifacts?	
Does your solution rely on a unified back-end data model?	
Does your solution provide relationship graph based analytics?	
What SAML integrations and MFA do you support?	
Do you support role-based access control (RBAC) for business units?	
Do you provide the ability to have different views depending on the team or Business Unit that is connected to the UI?	
Do you provide the ability to create multiple tenant inside the same organization?	
Demonstrate programmatic access capabilities via API.	
Describe your approach to dashboard visibility on risks & trending metrics.	
Demonstrate ability to generate reports in PDF & CSV formats.	
Demonstrate ability to generate executive vs. technical reports.	
Demonstrate custom reporting capabilities.	
Demonstrate ability to provide scheduling and emailing of reports.	

Demonstrate ability to rapidly incorporate zero-day risks in platform for prompt detection of exposed resources.	
Describe ability to deliver custom changes to meet customer needs and include customer references.	
Describe support for operational simplicity for fast adoption (self-guided training) and documentation.	
List support for region/ sovereign clouds (e.g., AWS, Azure China)	
What percentage of your users are non-security practitioners uses your solution as an average?	

About Wiz

Wiz secures everything organizations build and run in the cloud. Founded in 2020, Wiz is the fastest-growing software company in the world, scaling from $1M to $100M ARR in 18 months. Wiz enables hundreds of organizations worldwide, including 35 percent of the Fortune 100, to rapidly identify and remove critical risks in cloud environments. Its customers include Salesforce, Slack, Mars, BMW, Avery Dennison, Priceline, Cushman & Wakefield, DocuSign, Plaid, and Agoda, among others. Wiz is backed by Sequoia, Index Ventures, Insight Partners, Salesforce, Blackstone, Advent, Greenoaks, Lightspeed and Aglaé. Visit https://www.wiz.io/ for more information.