Cloud native application protection platform (CNAPP)

Request for proposal

Includes:

- Cloud Security Posture Management
- Cloud Workload Protection
- Cloud Infrastructure Entitlement Management
- Vulnerability Management
- Container Security
- Cloud Detection and Response
- IaC Scanning
- Data Security Posture Management

Table of Contents

Issuing company profile

Please provide the following information about the company issuing the RFP.

Company background

Describe the background of the company that is re- questing proposals for Cloud Native Application Pro-tection Platforms (CNAPP), including: Cloud Security Posture Management (CSPM), Cloud Workload Protection (CWPP), Cloud Infrastructure Entitlement Management (CIEM).

Project overview and objectives

The purpose of this RFP is to gather technical, delivery, and pricing information for Cloud Native Application Protection Platforms (CNAPP) services. Specifically, [COMPANY NAME] seeks to acquire Cloud Native Application Protection Platforms (CNAPP) technologies for…X, Y, Z.

Project owners

The individuals responsible for participating in this RFP include:

a. Product Owner(s):

b. Product Users / Implementer(s):

c. Other Stakeholders:

Supporting cloud environments

List the Cloud Service Providers (CSP) where [COMPANY NAME] has resources deployed (typically AWS, Azure, and/or GCP), including private cloud and on-premises container environments (like Openshift).

Also, provide information on existing remediation workflows for cloud alerts.

Schedule & submission instructions

Please provide the following information about the company issuing the RFP.

Schedule of events

Detail in the following table the anticipated schedule of events:

TASK	DATE
RFP distribution	xx/xx/xx
Deadline for vendor questions	xx/xx/xx
Answers for vendor questions	xx/xx/xx
Deadline for RFP submission	xx/xx/xx
Vendor notification of short-listed vendors	xx/xx/xx
Vendor presentations	xx/xx/xx
Vendor evaluations, POC etc.	xx/xx/xx
Vendor selection	xx/xx/xx
Project commencement	xx/xx/xx
Project completion	xx/xx/xx

RFP cost

All costs incurred in the preparation and submission of responses to the RFP shall be the responsibility of the vendor.

Late proposals

Proposals received after the due date will not be considered unless special considerations have been agreed to in advance of the due date. Regardless of the method used for delivery, vendors shall be wholly responsible for the timely delivery of submitted proposals.

Proposal delivery

Each submitted proposal shall consist of one Master with [INSERT NUMBER] paper copies, and one (1) electronic copy using the following format(s): Microsoft Word, Microsoft Excel, and/or Adobe PDF. Electronic cop ies will be submitted via email. Clearly label and index proposals with appropriate section and subsection numbers as referred to herein. Number each page individually and provide a table of contents. Please send all questions and final proposal to:

[Contact Name]

[Contact Email]

[COMPANY NAME]

Company Address

City, State Zip

Selection process

Describe any important details of the above Schedule of Events and outline the decision-making process for the purchase of a Cloud Infrastructure Security solution.

SECTION A

Vendor profiles

REFERENCE NO.	REQUIREMENT	VENDOR RESPONSE
A-1	How long has your company been in business and how long has your product been generally available for purchase?	
A-2	Describe the vision and direction for your company.	
A-3	Provide company Information: 1. Number of employees? 2. Number of existing clients? 3. Financials?	
A-4	Provide company ownership and funding information	
A-5	What is the largest scale cloud environment you're actively protecting?	
A-6	What is the largest AWS environment you're protecting?	
A-7	What is the largest Azure environment you're protecting?	
A-8	What is the largest Google Cloud Platform environment you're protecting?	
A-9	What is the largest Oracle Cloud Infrastructure environment you're protecting?	
A-10	Detail the breakdown of your customer base by business vertical, indicating the number of installations in each particular vertical.	
A-11	Please describe where your product fits in terms of market competition and explain what your product does better than others in the market.	
A-12	Please provide a high-level overview of your product's roadmap over the next 12 months.	
A-13	Are you active in standards organizations? If so, which?	
A-14	Do you maintain alliances with other information technology vendors? If so, which ones?	
A-15	Please indicate how many companies can resell your solution.	

SECTION B

Resource and workload inventory (Visibility)

REFERENCE NO.	REQUIREMENT	VENDOR RESPONSE
B-1	What Code technologies do you provide visibility into? (Frameworks, Libraries, Software Build Systems, Collaboration Software, Scripting Languages, etc.)?	
B-2	What CI/CD tools do you provide visibility into?	
B-3	What Compute Platforms do you provide visibility into? (Cloud Subscriptions, Container Services, Serverless, Virtual Machines, Operating Systems, Networking)	
B-4	What Application and Data Platforms do you provide visibility into?	
B-5	What Security and Identity tools do you provide visibility into?	
B-6	Can you identity all Cloud services including those not supported for risk assessment?	
B-7	Describe the visibility you provide into Workloads across VMs, Containers, and Serverless Functions.	
B-8	Demonstrate level of visibility into managed Kubernetes across EKS, AKS, and GKE.	
B-9	Demonstrate visibility into non-public Kubernetes API endpoints via private endpoints.	
B-10	Do you generate resource mapping relationships? Explain what relationships you map.	
B-11	Can you easily flag unwanted technologies in our environment?	

SECTION C

Governance and Compliance

REFERENCE NO.	REQUIREMENT	VENDOR RESPONSE
C-1	Demonstrate support for compliance frameworks [SPECIFIC FRAMEWORKS].	
C-2	Demonstrate support for OS and applications compliance benchmarks [SPECIFIC BENCHMARKS].	
C-3	Demonstrate support for custom compliance frameworks.	
C-4	Demonstrate support for OS and applications compliance benchmarks [SPECIFIC FRAMEWORKS].	
C-5	Ability to create compliance reports based on account/ subscription.	
C-6	Demonstrate ability to compare compliance posture across multiple frameworks in one view.	
C-7	Do you provide the ability to apply compliance frameworks to any level of operation (cloud provider, account, grouping of resources)?	
C-8	Do you provide the ability to disable/enable or create policy exceptions as required?	
C-9	Demonstrate ability to prove compliance via reporting with timestamps.	
C-10	Do you provide a library of security policies?	
C-11	Do you provide the ability to build custom security policies?	
C-12	Do you provide a library of host configuration policies?	
C-13	Do you provide ability to build custom host configuration rules?	
C-14	Demonstrate ability to detect weak authentication of assets (e.g., VMs with password enabled SSH authentication that are publicly exposed).	
C-15	Demonstrate ability to detect high risk configuration findings.	

SECTION D

Risk assessment

REFERENCE NO.	REQUIREMENT	VENDOR RESPONSE
D-1	Demonstrate ability to monitor and report on the most critical attack vectors across network, identity, vulnerabilities, secrets and configuration analysis.	
D-2	Demonstrate ability to prioritize security issues according to the environmental layout (e.g., External exposure, assumed privileges, business impact).	
D-3	Demonstrate ability to detect vulnerabilities on VM's, Containers, and Functions	
D-4	Do you have the ability to detect vulnerabilities on powered off VM's?	
D-5	Demonstrate detection of weak authentication methods on VM's, Containers, and Functions.	
D-6	Demonstrate ability to detect exposed secrets on VM's, Containers, and Functions	
D-7	Do you provide the ability detect end of life version of defined software packages?	
D-8	How do you generate automated risk scoring to prioritize resource risk?	
D-9	Demonstrate ability to detect systems that require restart.	
D-10	How do you manage the detection of multiple occurrences of the same misconfiguration on a resource?	
D-11	Demonstrate ability to detect API services without authentication set.	
D-12	Demonstrate ability to query functionality for custom searching.	
D-13	Do you provide the ability to customize and export query results?	
D-14	Demonstrate ability to provide complete audit trail of all user activities within platform.	
D-15	Do you scan for malware across cloud environments?	

SECTION E

Workload vulnerability and patch management

REFERENCE NO.	REQUIREMENT	VENDOR RESPONSE
E-1	Demonstrate ability to detect vulnerabilities in container images.	
E-2	Demonstrate ability to detect vulnerabilities in currently running containers.	
E-3	Demonstrate ability to detect vulnerabilities in container images without repository access	
E-4	Demonstrate ability to detect vulnerabilities in container images hosted in a container registry	
E-5	Do you provide the ability to scan private container registry?	
E-6	Demonstrate ability to detect vulnerabilities in container images in self-deployed docker/Kubernetes	
E-7	Demonstrate ability to detect vulnerabilities in VMs	
E-8	Demonstrate ability to detect vulnerabilities in Functions	
E-9	Demonstrate ability to detect library-based vulnerabilities in VMs and containers (e.g., Python, Java).	
E-10	Detail the level of context provided for vulnerabilities.	
E-11	Provide examples of advanced queries on vulnerabilities.	
E-12	Demonstrate ability to detect vulnerabilities on publicly exposed resources.	
E-13	Demonstrate ability to detect vulnerabilities on highly privileged resources.	
E-14	Demonstrate ability to detect vulnerabilities on critical risk assets.	
E-15	Demonstrate ability to detect unpatched OS on compute nodes and instance groups.	
E-16	Demonstrate ability to detect unpatched Kubernetes clusters.	
E-17	Demonstrate ability to detect publicly exposed unpatched VMs and containers.	
E-18	Demonstrate ability to detect publicly exposed containers running on a compute node with unpatched kernel	
E-19	Demonstrate ability to detect end-of-life Hosted technologies running on public facing compute instance	
E-20	Demonstrate ability to detect highly privileged unpatched assets and assets with critical risk.	
E-21	Provide list of threat and vulnerability databases you source information from	

SECTION F

Exposure analysis

REFERENCE NO.	REQUIREMENT	VENDOR RESPONSE
F-1	Demonstrate ability to provide network reachability map of resources and workloads.	
F-2	Demonstrate ability to detect publicly exposed resources and containers.	
F-3	Demonstrate ability to detect Kubernetes clusters with publicly exposed APIs.	
F-4	Demonstrate ability to detect ingress rules on any port and destination.	
F-5	Do you provide built-in intelligence that is able to identify known suspicious IPs connecting to workloads?	
F-6	Demonstrate ability to detect poorly separated network traffic.	
F-7	Demonstrate ability to detect resources accessible from other subscriptions.	
F-8	Demonstrate ability to detect geo-location traffic from unrecognized regions	
F-9	Demonstrate ability to detect resources accessible from other Vnets.	
F-10	Demonstrate ability to detect all resources exposed publicly behind load-balancers.	
F-11	Demonstrate ability to provide intuitive visual interface to analyze & investigate network traffic in either north-south or east-west directions.	

SECTION G

IAM, secrets, and entitlement management (CIEM)

REFERENCE NO.	REQUIREMENT	VENDOR RESPONSE
G-1	Demonstrate ability to capture IAM activity for users & roles (create, modify, delete).	
G-2	Demonstrate ability to detect overly permissive access.	
G-3	Do you recommend permission sets based on utilization?	
G-4	Demonstrate ability to detect who has access to specific resources.	
G-5	Demonstrate ability to detect users/roles with elevated permissions on resources.	
G-6	Demonstrate ability to detect over-privileged permissions on containers.	
G-7	Demonstrate ability to detect over-privileged permissions on serverless workloads.	
G-8	Demonstrate ability to detect exposed secrets on VMs, containers, and functions.	
G-9	Demonstrate ability to detect exposed secrets on public and private buckets	
G-10	Demonstrate ability to detect secrets (certificates, access/encryption keys, cleartext data, etc.).	
G-11	Demonstrate ability to detect lateral and cross-account movement via compromised access keys or stolen permissions.	
G-12	Demonstrate ability to identify cloud services that can access data.	
G-13	Demonstrate ability to find inactive admin users and groups.	
G-14	Demonstrate ability to find exposed SSH private keys.	
G-15	Demonstrate ability to detect exposed private keys of domain certificates	
G-16	Demonstrate ability to find resources using service accounts with admin permissions.	
G-17	Demonstrate ability to find certificates nearing expiration and exposed certificates.	
G-18	Demonstrate ability to find cleartext cloud keys allowing high privileges.	
G-19	Demonstrate ability to find attack path to high value assets.	

SECTION H

Cloud Detection and Response

REFERENCE NO.	REQUIREMENT	VENDOR RESPONSE
H-1	Demonstrate ability to collect Cloud Audit logs from any supported Cloud Providers.	
H-2	Do you provide the ability to explore who did what on where and when?	
H-3	Demonstrate ability to correlate resources with events.	
H-4	Demonstrate ability to detect and alert on architecture configuration changes.	
H-5	Demonstrate ability to detect and alert on Failed API activities or Failed Resource access.	
H-6	Do you provide any mechanism or capability to validate external exposure?	
H-7	Demonstrate ability to view what an attacker will see from the outside.	
H-8	Demonstrate ability to detect and alert on misconfigured APIs	
H-9	Demonstrate ability to detect secret and sensitive data in HTTP response of externally exposed resources	
H-10	Do you provide the ability to add custom threats feeds?	
H-11	Demonstrate ability to find any instance of a specific file via its custom hash.	

SECTION I

Security automation

REFERENCE NO.	REQUIREMENT	VENDOR RESPONSE
I-1	List the ticketing platform(s) you support.	
I-2	Provide details on workflow actions for notifications.	
I-3	Demonstrate ability to generate rule sets based on conditions and criteria.	
I-4	Demonstrate ability to send notifications with context on risk (can be customized to enrich if required).	
I-5	List what SIEM tools are supported.	
I-6	List what SOAR tools are supported and remediation playbooks available.	
I-7	Do you support auto-remediation? Provide examples and details.	
I-8	List what vulnerability management and response tools are supported.	
I-9	Demonstrate ability to obtain recommendations against misconfigurations and to execute auto-corrective actions.	
I-10	Demonstrate ability to generate management policies for CSPs (AWS SCP, Azure Policy) for preventive control.	

SECTION J

CI/CD Pipeline integrations (DevSecOps Enablement)

REFERENCE NO.	REQUIREMENT	VENDOR RESPONSE
J-1	Demonstrate ability to integrate controls as part of a deployment pipeline to validate infrastructure-as-code (IaC) is compliant with defined policies.	
J-2	Demonstrate ability to validate IaC templates are compliant before enterprise use.	
J-3	Demonstrate ability to scan VM images (e.g., AMI) and container images for vulnerabilities and exposure.	
J-4	Demonstrate ability to scan container images for exposed secrets in the CI/CD pipeline.	
J-5	Demonstrate ability to scan virtual machine images for exposed secrets in the CI/CD pipeline.	
J-6	List what CI/CD tools you integrate with.	
J-7	List customer references who have successfully implemented a DevSecOps strategy using your product.	

SECTION K

Data Security Posture Management

REFERENCE NO.	REQUIREMENT	VENDOR RESPONSE
K-1	Demonstrate ability to identify sensitive data (PII, PCI, PHI and secrets)	
K-2	Do you provide the ability to scan public and private cloud storages (AWS S3, Azure Blob Storage and GCP Cloud Storage)?	
K-3	Do you provide the ability to scan managed and self-hosted SQL databases?	
K-4	Do you provide the ability to scan managed and self-hosted No-SQL databases and identify sensitive data?	
K-5	Do you provide the ability to scan workload OS and Data disks and identify sensitive data?	
K-6	Do you provide the ability to ingest classified tags from external sources like BigID or Macie?	
K-7	Demonstrate ability to detect unintentionally moved or copied between environments, regions, or clouds	
K-8	Demonstrate ability to detect and alert on externally exposed workloads (VM, container, Serverless) with possible lateral movement to sensitive data	
K-9	Demonstrate ability to detect and alert on externally exposed cloud storage with sensitive data	
K-10	Demonstrate ability to create custom classifiers	

SECTION L

General Operability and Adoptability

REFERENCE NO.	REQUIREMENT	VENDOR RESPONSE
L-1	Describe your deployment architecture. Are agents or additional deployments required? Do you support Outpost?	
L-2	What SAML integrations and MFA do you support?	
L-3	Do you support role-based access control (RBAC) for business units?	
L-4	Do you provide the ability to have different views depending on the team or Business Unit that is connected to the UI?	
L-5	Do you provide the ability to create multiple tenants inside the same organization?	
L-6	Demonstrate programmatic access capabilities via API.	
L-7	Describe your approach to dashboard visibility on risks & trending metrics.	
L-8	Demonstrate ability to generate reports in PDF & CSV formats.	
L-9	Demonstrate ability to generate executive vs. technical reports.	
L-10	Demonstrate custom reporting capabilities.	
L-11	Demonstrate ability to provide scheduling and emailing of reports.	
L-12	Demonstrate ability to rapidly incorporate zero-day risks in platform for prompt detection of exposed resources.	
L-13	Describe ability to deliver custom changes to meet customer needs and include customer references.	
L-14	Describe support for operational simplicity for fast adoption (self-guided training) and documentation.	
L-15	List support for region/ sovereign clouds (e.g., AWS, Azure China).	

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 30 percent of the Fortune 500, 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 and Aglaé. Visit https://www.wiz.io/ for more information.