Request for Proposal: Cloud-Native Application Protection Platform (CNAPP)

Table of Contents

1. Overview

We are seeking proposals for a comprehensive Cloud-Native Application Protection Platform (CNAPP) to safeguard our cloud-native applications throughout their entire lifecycle. The solution should provide integrated security functions, offering comprehensive visibility, consistent policy enforcement, and robust protection across our diverse cloud environments.

2. Key Components

The proposed solution must include the following key components:

2.1. Cloud Security Posture Management (CSPM)

2.2. Cloud Workload Protection Platform (CWPP)

2.3. Cloud Infrastructure Entitlement Management (CIEM)

2.4. DevSecOps Integration

2.5. Runtime Protection

3. Functional Requirements

3.1. Unified Visibility

Tip: A robust unified visibility solution is crucial for maintaining comprehensive security oversight. Look for solutions that provide real-time monitoring capabilities and can integrate data from multiple sources into a single, coherent view. Consider the depth of visibility across different cloud services and the ability to customize views based on different stakeholder needs.

Requirement	Sub-Requirement	Y/N	Notes
Unified Visibility	Centralized view of security across all cloud resources and services		
	Visibility into configurations		
	Visibility into assets		
	Visibility into permissions		
	Visibility into code		
	Visibility into workloads		

3.2. Automated Compliance

Tip: Automated compliance capabilities should reduce manual oversight while ensuring continuous regulatory adherence. Evaluate solutions based on their ability to automatically detect, report, and remediate compliance violations across multiple regulatory frameworks.

Requirement	Sub-Requirement	Y/N	Notes
Automated Compliance	Continuous assessment of compliance with industry standards		
	Continuous enforcement of compliance with industry standards		

	Streamlined adherence to regulatory requirements through monitoring		
	Streamlined adherence to regulatory requirements through reporting		

3.3. Threat Detection and Response

Tip: Advanced threat detection and response capabilities should leverage both traditional and AI-enhanced methods. Look for solutions that can detect threats in real-time and provide actionable response recommendations.

Requirement	Sub-Requirement	Y/N	Notes
Threat Detection and Response	Real-time identification of threats across application lifecycle		
	Real-time mitigation of threats across application lifecycle		
	AI-enhanced threat detection using advanced analytics		
	AI-enhanced threat detection using predictive analysis		
	Smart Cloud Detection & Response (CDR) implementation		
	Real-time threat detection with intent analysis		

3.4. Policy Management

Tip: Effective policy management requires both consistency and intelligence. Evaluate solutions based on their ability to maintain uniform security policies across diverse environments while leveraging AI to optimize and adapt policies based on emerging threats and organizational needs.

Requirement	Sub-Requirement	Y/N	Notes
Policy Management	Consistent definition of security policies across environments		

	Consistent enforcement of security policies across environments		
	AI-enhanced policy management capabilities		
	Intelligent policy recommendations		

3.5. Scalability

Tip: Scalability is essential for growing organizations. Look for solutions that can seamlessly scale with your infrastructure while maintaining performance. Consider both horizontal and vertical scaling capabilities, as well as the ability to handle sudden spikes in workload.

Requirement	Sub-Requirement	Y/N	Notes
Scalability	Ability to adapt to dynamic cloud environments		
	Support for growing workloads		
	Performance maintenance at scale		

3.6. Integration Capabilities

Tip: Integration capabilities are crucial for creating a cohesive security ecosystem. Evaluate solutions based on their ability to integrate with your existing toolchain and the ease of implementing new integrations.

Requirement	Sub-Requirement	Y/N	Notes
Integration Capabilities	Seamless integration with existing development tools		
	Seamless integration with security tools		
	Seamless integration with cloud management tools		
	Easy integration with SecOps ecosystems for real-time alerting		

3.7. Multi-Cloud Security Coverage

Tip: Comprehensive multi-cloud security is essential in today's diverse cloud environments. Look for solutions that provide consistent security controls across all major cloud providers while maintaining awareness of provider-specific nuances.

Requirement	Sub-Requirement	Y/N	Notes
Multi-Cloud Security Coverage	Visibility across IaaS environments		
	Visibility across PaaS environments		
	Visibility across serverless environments		
	Support for AWS		
	Support for Azure		
	Support for Google Cloud		

3.8. Infrastructure as Code (IaC) Scanning

Tip: IaC scanning capabilities should detect security issues early in the development lifecycle. Look for solutions that integrate with your development workflow and provide actionable remediation guidance.

Requirement	Sub-Requirement	Y/N	Notes
Infrastructure as Code Scanning	Detection of security vulnerabilities in infrastructure code before deployment		
	Support for multiple IaC frameworks		
	Pre-deployment validation		
	Security best practices enforcement		

3.9. Container and Kubernetes Scanning

Tip: Container security requires comprehensive scanning throughout the container lifecycle. Evaluate solutions based on their ability to scan container

images, detect runtime vulnerabilities, and provide Kubernetes-specific security controls.

Requirement	Sub-Requirement	Y/N	Notes
Container and Kubernetes Scanning	Identification of vulnerabilities within containerized applications		
	Runtime container security monitoring		
	Kubernetes cluster security assessment		
	Container image scanning		

3.10. Data Protection

Tip: Data protection capabilities should cover data at rest and in motion. Look for solutions that provide comprehensive data security controls, including classification, encryption, and access monitoring.

Requirement	Sub-Requirement	Y/N	Notes
Data Protection	Monitoring of data for potential exfiltration		
	Data classification capabilities		
	Data inspection capabilities		
	Prevention of data exfiltration		

3.11. Risk Prioritization

Tip: Effective risk prioritization helps focus security efforts on the most critical threats. Look for solutions that use AI to analyze risks in context of your environment and business impact.

Requirement	Sub-Requirement	Y/N	Notes
Risk Prioritization	AI-powered analysis of risks		
	AI-powered prioritization of risks		