If applicable, please respond with Y/N and explanation. Otherwise please just include response.

Vendor Feature & Functions Evaluation Questionnaire	Yes/No

Vendor Address & phone number — -

Vendor Point of contact(s) name, phone, & email — -

Brief profile (years in business; growth via mergers and acquisitions; funding; number of employees; biggest customer wins; and customer wins in the healthcare sector).

Please describe core team and what assets/experience they provide

Please provide an overview of your company's growth over the past 5 years (including mergers and acquisitions).

Describe your company's value proposition
Briefly describe your business model.

Briefly describe your near and longer-term vision and roadmap.

How do you differentiate yourself from your competition?

Who do you view as your key competitors?

List major customers, specifically large academic medical centers who use container Orchestration tools

Please provide 2 or more customer references.

Describe your typical implementation plan and timeline (e.g. how long from initiation to go-live)?
Describe the vendor and customer team effort required to stand up your platform (e.g. team makeup, estimated hours of effort, estimated timeline post contract signing etc.)

What is the support model offered as part of the tool?

Does your company offer professional services or partner with other service providers to support solution deployment?

Can your solution assist in forensic analysis and investigations in the event of a security breach?

Describe your service and support options including phone, web support, proactive support, reporting, etc.

1. How does your container management solution ensure secure access control and authentication for users and containers?

2. Can you explain the security measures in place to protect container communications and network traffic?

3. Is there support for Role-Based Access Control (RBAC) to define and enforce permissions and roles within the container environment?

4. How does your platform handle the security of container images, including image scanning for vulnerabilities and patch management?

5. What tools or features are provided for the secure management of sensitive data (secrets) within containers?

6. Can you elaborate on how your solution enforces security policies and compliance requirements for containerized applications?

7. What auditing and monitoring capabilities are available to track and respond to security incidents and compliance violations?

8. Does your platform offer runtime protection and intrusion detection to identify and mitigate security threats while containers are running?

9. Do you store patient data in your system in a HIPAA-compliant way? Describe how your store data.

10. Can the container registry be managed and scanned with InsightVM

11. were your containers solutions pen tested by a third party?

12. does your container support code-signing?

( ) ( )   0   / 0   0

1. How does your container management platform handle container orchestration and scheduling across clusters within its architectural design?
2. What architectural measures are in place to ensure high availability and fault tolerance for containerized applications?

3. Can your system provide architectural support for managing containers across diverse environments, including multi-cloud and on-premises setups?
4. How is scalability and elasticity achieved within the architecture to accommodate the growth of container workloads?
5. Does your solution adopt a microservices architecture, and if so, how does it leverage this approach in its design?

6. What architectural options are available for integrating with external services, tools, and platforms, and how extensible is the overall architecture?
7. Could you provide insights into the security architecture that underpins the protection of containerized applications and data?
8. Does your platform offer well-documented APIs and a developer-friendly architecture to promote ease of use and integration?
9.Explain how your solution supports and integrates with GitOps practices for Kubernetes

1. Does your container management platform support multi-cloud deployments, allowing seamless container operation across various cloud providers?

2. How does your solution integrate with major cloud providers (e.g., AWS, Azure, GCP) to leverage native cloud services and resources within its architecture?

3. Can your platform automatically scale container workloads in response to fluctuations in demand when deployed in a cloud environment?
4. What features or tools are available to assist organizations in managing and optimizing container-related costs in the cloud?
5. How does your platform handle cloud-native networking and load balancing for containers running in cloud environments?

Explanation/Response

-
-