

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

Vendor Feature & Functions Evaluation Questionnaire		Yes/No
Contact Information		
	<i>Vendor Address & phone number</i>	-
	<i>Vendor Point of contact(s) name, phone, & email</i>	-
Size, Growth, & Vision		
	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.	
Implementation, Professional Services, & Support		
	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.	
Storage features		
	1. How does your system handle storage provisioning, including both automatic setup and categorization by performance?	

	2. Can you describe your approach to ensuring data availability and redundancy, as well as data security, especially when data is at rest?	
	3. Does your platform support persistent storage, and how is it integrated with applications?	
	4. What mechanisms are in place for data backup and restoration, and how are backups managed?	
	5. How does your system facilitate the adjustment of storage sizes without data loss, and what tools are available for storage monitoring and tracking performance?	
	6. Can your solution seamlessly integrate with external storage systems or cloud-based storage solutions, and how does data access and migration work with external storage?	
	7. How does your platform handle multi-tenancy and access control for storage resources, and can different users or teams have their segregated storage spaces?	
	8. Can data be migrated between clusters or environments, and how is data integrity maintained during migration processes?	
	9. Is your platform compatible with both Dell EMC CSI and NetApp Astra storage technologies?	
Backup features		
	1. How does your container management platform handle backups, including scheduling, automation, and retention policies?	
	2. Can you explain how data consistency is maintained during backups, especially for applications with databases?	
	3. What storage options are available for storing backups, and does your platform integrate with external storage solutions or cloud providers?	
	4. Does your solution support incremental backups, and how are they managed to minimize data transfer and storage?	
	5. What encryption standards and protocols are supported for securing backup data both in transit and at rest?	
	6. Can backups be tested and verified for data integrity and successful restores, and what mechanisms are in place for disaster recovery using backups?	
	7. Is there support for cross-cluster or cross-environment backup and restore, and how is data consistency ensured during these processes?	
	8. How does your platform provide monitoring, alerts, access control, reporting, and auditing for backup-related activities?	

	9. Can you provide details on Kubernetes' native support or integration capabilities for NetBackup, including any features or functionalities that facilitate backup and recovery operations within Kubernetes environments?	
Regulatory & Security Compliance		
	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 you 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?	
Networking features		
	1. How does your container management platform handle network configuration, segmentation, and policy management for containerized applications?	
	2. Can you explain how your system enables service discovery, load balancing, and network segmentation within container clusters?	
	3. What mechanisms are available for implementing network policies and access control to secure container communications?	
	4. How does your platform ensure secure communication between containers within the same cluster?	
	5. What options are provided for containers to connect with external services or resources, and how is external connectivity managed?	
	6. Does your system support network isolation for multi-tenant environments or applications, and how is this achieved?	

	7. Is there built-in support for networking across multiple clusters or environments, and how are network connections established between them?	
	8. What network monitoring and troubleshooting tools or features are available to manage and optimize network performance and address network-related issues?	
	9. Can you describe the level of integration your Kubernetes solution offers with Infoblox?	
Architecture features		
	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	
Cloud features		
	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?	

	6. What security measures and best practices are integrated into your platform to ensure the security of containerized applications when running in the cloud?	
	7. Does your system provide integration with cloud billing and reporting services, offering visibility into container-related costs for financial management?	
	8. How does your platform assist organizations in maintaining compliance and governance standards when deploying containers in the cloud?	

Hardware Compute features

	1. What hardware infrastructure, including server and CPU architectures, is supported by your container management platform?	
	2. How does your system optimize resource utilization to efficiently use available hardware resources?	
	3. Are there features or tools to leverage GPUs and hardware acceleration for containerized workloads, and how is this managed?	
	4. Does your platform support bare metal deployments, and what considerations and benefits are associated with this option?	
	5. How does your system ensure hardware resource isolation and fairness among containers sharing the same physical hardware?	
	6. Can you explain the fault tolerance mechanisms and hardware failover capabilities for containerized applications?	
	7. Does your platform integrate with hardware monitoring and management tools to provide insights into the health and status of underlying hardware?	
	8. Is there support for custom hardware integrations or specialized hardware requirements for specific workloads, and how is this accommodated?	
	9. How does your solution handle the deployment of Kubernetes clusters on VMware vSphere or other VMware products?	

Monitoring features

	1. How does your container management platform monitor the health and performance of containers and clusters?	
	2. What performance metrics and insights are available to monitor containerized applications and resource utilization?	
	3. Can you describe the system's approach to logging, log aggregation, and accessibility for analysis and troubleshooting?	

	4. Does your platform include alerting and real-time notification mechanisms for identifying performance anomalies and issues?	
	5. How is resource utilization, including CPU and memory, tracked and reported for containers and clusters?	
	6. Are there integrations with external monitoring and observability tools or platforms to enhance monitoring capabilities?	
	7. Can users define custom metrics and create dashboards to visualize container and application performance data?	
	8. What tools or features are available for monitoring the overall health and performance of container clusters and their applications?	

