ISG Provider Lens™

2020

Cloud Native – Container Services 2020

imagine your future®

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 700 clients, including more than 75 of world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, visit www.isg-one.com.

Table of Contents

Definition

In the past decade, new patterns and technologies have emerged for the development, deployment and operation of modern applications that take advantage of the capabilities available in cloud infrastructure environments. This cloud native approach focuses on building applications that are highly modular, adaptable, fault-tolerant and better capable of delivering value to end users.

In particular, Kubernetes, the open source container orchestration software originally released by Google, has become the foundation of the stack underpinning these applications. It provides software features that enable easier management of multi-container applications, including automatic scaling, management of container failures and routing network traffic.

While Kubernetes solves many problems in application development and operation, it also creates a host of new, complex issues that enterprises need to contend with. Shifting away from monolithic architectures means that monitoring, security and networking become significant challenges. New software and services have emerged to mitigate these issues, but that means enterprises must not only figure out how to adopt Kubernetes, but also how to secure their cloud native applications, how to best use service mesh to manage multi-container environments and how to monitor those applications and the increasingly complex fabric of connections and logic.

Service mesh helps technology teams manage the communications and connections between different containerized applications within an overall technical estate. Given the hype around this technology, ISG notes that enterprise interest around it far outweighs its current utility for most businesses. Service providers must be able to provide a clear business case and value for implementing service mesh, beyond its current trendiness.

Cloud native security offerings are necessary to protect an attack surface that is considerably different from what enterprises are traditionally used to managing. This added layer of security complexity often requires dedicated software and services. Past incidents have shown that even the most technically capable enterprises can be caught out by their Kubernetes clusters' security needs.

The ISG Provider Lens™ study offers the following to IT decision makers:

- Transparency on the strengths and weaknesses of relevant providers
- A differentiated positioning of providers by segments
- A view of the global services market with a focus on the U.S.

Our study serves as the basis for important decision-making for positioning, key relationships and go-to-market considerations. ISG advisors and enterprise clients also use information from these reports to evaluate their current vendor relationships and potential new engagements.

Quadrant Research

As part of this ISG Provider Lens™ quadrant study, we are introducing the following four quadrants on Cloud Native - Container Services 2020:

Cloud Native – Container Services 2020	
Managed Kubernetes	Managed Service Mesh
Managed Cloud Native Security	Cloud Native Observability Solutions

Source: ISG 2020

Managed Kubernetes

This category analyzes service and solution providers that offer deployment and operation of Kubernetes, above and beyond what is provided in the upstream open source project. The offerings evaluated in this quadrant will help enterprises adopt and deploy Kubernetes within an environment of their choice and in a highly automated manner. The offerings highlighted for this quadrant will provide enterprises with the capabilities that they need, including application deployments and patching, compliance and access management and cluster health monitoring.

(Note: This quadrant replaces the Managed Containers-as-a-Service quadrant from last year’s Private/Hybrid Cloud study.)

Eligibility Criteria:

- Robust tooling that augments and streamlines the process of operating Kubernetes within an enterprise, with features tailored to complex business environments
- A path to migration for bringing legacy workloads under management by Kubernetes
- Support for a broad variety of workloads and application development patterns
- Ability to offer Kubernetes-specific services and support, either through first-party professional services or partnerships with other providers
- Relevant certifications for Kubernetes, including the Cloud Native Computing Foundation’s Kubernetes Certified Service Provider and Certified Kubernetes Distribution.

Managed Service Mesh

This category is focused on service and solution providers that offer software and services necessary to help enterprises adopt and manage service mesh technology to aid in management of a cloud native application estate. Service mesh technology enables easier composition of microservices into a single application, and success in this category requires further streamlining of this process for the benefit of enterprises.

Managed service mesh providers must have robust capabilities to help enterprises adopt, integrate and troubleshoot the mesh(es) in their environment. These capabilities should be focused on deriving benefits from service mesh to allow developers to spend more time writing code and less time contemplating the connections between different parts of a cloud native environment. The offerings evaluated should provide benefits around routing, resilience, security and observability.

Eligibility Criteria:

- Support for at least one open source service mesh (Envoy, Linkerd, Istio, Consul, etc.)
- Support for multiple environments under a hybrid cloud model
- Ability to streamline set-up and operation of service mesh in the context of an enterprise
- Services, software and guidance that improve routing, resilience, security and observability of cloud native applications managed by the service mesh
- Ability to offer robust enterprise services to aid the configuration and operation of the service mesh(es), either through first-party professional services or through partnerships with other service providers
- A clear point of view about when it is right for clients to deploy service mesh in their environments, and the ability to provide thoughtful, structured guidance for deployment.

Managed Cloud Native Security

This category is focused on software and service providers managing security of cloud native applications, either as part of a broader containers-as-a-service offering, or as a standalone add-on to an enterprise's application architecture. Success in this area requires dedicated understanding of cloud native applications and the inherent security challenges. Specifically, these offerings should address securing the Kubernetes cluster, containers within that cluster and communication within and without that cluster environment.

Because enterprises often adopt cloud native development approaches as part of a broader DevOps or DevSecOps transformation, it is necessary for the offerings considered here to integrate well with highly automated software development tool chains and processes.

Eligibility Criteria:

- Security capabilities specific to container-rich application environments and inherent complexities
- Consistent support of multiple environments, both on-premises and in the cloud
- Integration with a variety of security tooling that may already exist within a client environment
- Resources to educate enterprises on best practices for security in a cloud native environment, and ability to guide implementation of these practices.

Cloud Native Observability Solutions

This category is focused on software vendors that provide dedicated solutions for observability of cloud native applications. Understanding the behavior of these applications has the potential to be far more complex than doing the same for a traditional monolith. Developers and operators must understand not only how each containerized app or service behaves, but also how they communicate with one another. Using standard monitoring tools that have not been built with cloud native applications in mind could fail to provide necessary information to enterprises. Thus, enterprises need to opt for specialized capabilities.

Eligibility Criteria:

- Software that provides novel capabilities to help enterprises understand the inner workings and performance of their cloud native application environments
- Dedicated tooling meant for observability, specifically multi-container applications, with support for highly granular microservices architecture as well as for applications composed of a smaller number of complex services
- Capability to work across multiple infrastructure environments under a hybrid cloud model
- Resources to help enterprises understand and implement this software within their environment.

Quadrants by Region

Quadrants	Global	U.S.
Managed Kubernetes	Overview	√
Managed Service Mesh	Overview	√
Managed Cloud Native Security	Overview	√
Cloud Native Observability Solutions	Overview	√

Schedule

The research phase falls in the period **April 2020 to August 2020**. During this period, survey, evaluation, analysis and validation will take place. The results will be presented to the media in **August 2020.**

Milestones	Beginning	End
Launch	April 15, 2020	
Survey Phase	April 15, 2020	May 11, 2020
Sneak Preview	June 16, 2020	
Press release	Aug 24, 2020	

Please refer to this link to view/download the ISG Provider Lens™ 2020 research agenda.

Research production disclaimer:

ISG collects data for the purposes of writing research and creating provider/vendor profiles. The profiles and supporting data are used by ISG advisors to make recommendations and inform their clients of the experience and qualifications of any applicable provider/vendor for outsourcing work identified by the clients. This data is collected as part of the ISG FutureSource process and the Candidate Provider Qualification (CPQ) process. ISG may choose to only utilize this collected data pertaining to certain countries or regions for the education and purposes of its advisors and not to produce ISG Provider Lens™ reports. These decisions will be made based on the level and completeness of information received directly from providers/vendors and the availability of experienced analysts for those countries or regions. Submitted information may also be used for individual research projects or for briefing notes that will be written by the lead analysts.

Partial list of companies invited for the survey

Are you in the list? Do you see yourself as a relevant provider but missing from the list? Contact us to become an active participant in the research phase.

2nd Watch

Acaisoft

Accenture

Alcide

Altoros

Anchore

Apprenda (Atos)

Appvia

Aqua

Amazon Web Services (AWS)

Banzai Cloud

Booz Allen Hamilton

BoxBoat

Canonical

Capgemini

Check Point Software Technologies

Chef

CloudOps

Cognizant

Container Solutions

Containous

Contino

CoreHive Computing

D2IQ

Darumatic

Datassential

Datica

Dell Technologies Consulting

Deloitte

Diamanti

DoiT International

DXC

Decipher Technology Studios

Dynatrace

Elastisys

Entigo

Epsagon

Fairwinds

Flant

Fujitsu

Fullstaq

Giant Swarm

Google Cloud

Grape Up

Gravitational

HashiCorp

HCL

Honeycomb

IBM Cloud

InfraCloud Technologies

Kong

Kublr

LightStep

Logz.io

MayaData

Microsoft

Mirantis

MSys Technologies

Navitas Business Consulting

Nebulaworks

NEC

NeuVector

New Context

New Relic

NIIT Technologies

Nirmata

NTT Data

Oteemo

Palo Alto Networks

Pivotal

Platform9

Portworx

Rackner

Rackspace

Rancher Labs

RX-M

SAIC

Samsung SDS

Solo.io

Snyk

Splunk

StackPointCloud

StackRox

Stark & Wayne

SUSE

Sumo Logic

Synopsys

Sysdig

TCS

Tech Mahindra

Tigera

Vmware

Weaveworks

Wipro

YLD

Contacts for this study

Blair Hanley Frank

Lead Analyst and Regional Analyst
for Global and U.S.

Dhananjay Koli

Global Project Manager

Do you need any further information?

If you have any questions, please do not hesitate to contact us at isglens@isg-one.com.