

A collage of several skyscrapers with glass facades, viewed from a low angle looking up. The buildings are arranged in a staggered, overlapping pattern, creating a sense of depth and architectural complexity. The colors range from cool blues and greys to warmer yellows and oranges.

***ISG** Provider Lens™

2022

Cloud-native
Services and
Solutions 2022

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 800 clients, including more than 75 of the 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	4
Quadrants Research	5
Quadrants by Region	11
Schedule	12
Partial list of companies being invited for the survey	14
Contacts for this study	18
Quality & Consistency Review Team for this study	20

© 2022 Information Services Group, Inc. All rights reserved. Reproduction of this publication in any form without prior permission is strictly prohibited. Information contained in this report is based on the best available and reliable resources. Opinions expressed in this report reflect ISG's judgment at the time of this report and are subject to change without notice. ISG has no liability for omissions, errors or completeness of information in this report. ISG Research™ and ISG Provider Lens™ are trademarks of Information Services Group, Inc.

Definition

In recent years, the development of lightweight software containers and orchestration tools has revolutionized the enterprise IT market, liberating enterprises, large and small, from the constraints of a fixed, monolithic IT infrastructure. This cloud-native approach focuses on building applications that are highly modular, adaptable, fault-tolerant and better capable of delivering value to end users. By decoupling applications from the underlying infrastructure, container solutions offer major advantages over traditional on-premises applications, which include light-touch updating of applications, faster scaling of compute and other resources to accommodate peaks in demand, the freedom to work in web-based programming languages, easier development of new applications, and better integration with DevOps and continuous integration/continuous delivery CI/CD pipelines. Kubernetes, an open-source container orchestration system created by Google and maintained by a massive community of technologists, aids in this approach.

As cloud-native technologies become more prevalent, however, attention is increasingly on managing some of the attendant challenges such as the need for new ways of working between development and operations (DevOps). Enterprises, therefore, take a variety of approaches to adopting cloud-native technologies across their technology environments. Some choose to work with managed service providers and system integrators (SIs) that offer managed container services, backed by skilled employees who can help configure entire platforms for cloud-native applications, migrate legacy workloads to containers and build new applications for enterprises to run on the platform. Others opt to directly procure container management and orchestration capabilities, either by turning to independent software vendors (ISVs) for packaged Kubernetes distributions or by using the cloud-native offerings of hyperscalers as the foundation for their future. Increasingly, enterprises are also looking to the hyperscalers for cloud-native services and applications that span multiple clouds.

With the shift to containerization, cloud-native observability and security are becoming top concerns for enterprises. Cloud-native technologies trigger many unique security challenges. The distributed and dynamic nature of containers makes monitoring, incident resolution and compliance more difficult. Containers make much greater use of third-party software and components, which can introduce vulnerabilities. Identity and access/entitlement management are more difficult to manage in the multi-developer world. For these and other reasons, enterprises are increasingly turning to cloud-native security software providers, which have developed specialized solutions to map and protect the expanding attack surface in cloud-native environments.

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

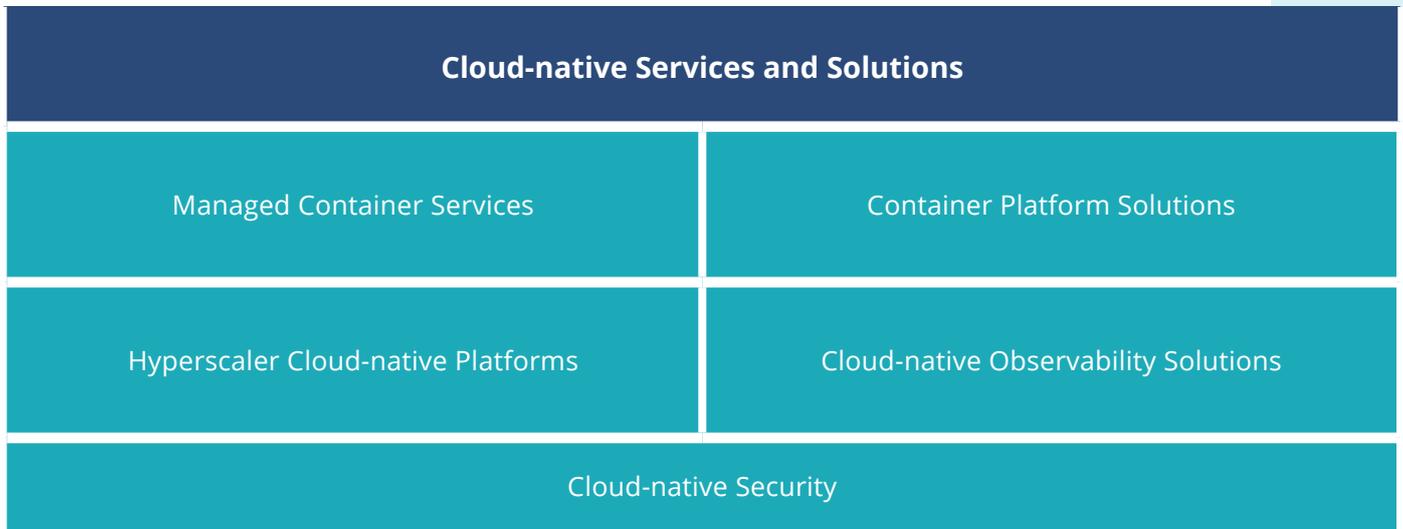
- Transparency on the strengths and weaknesses of relevant providers
- A differentiated positioning of providers by segments
- A view of the global services and solutions market with a focus on the U.S. and Europe

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 engagements.

Quadrant Research

As a part of this ISG Provider Lens™ quadrant study, we are focusing on the following five quadrants for Cloud-native Services & Solutions:

Simplified illustration



Source: ISG 2022

Managed Container Services

This quadrant analyzes service providers that offer a suite of capabilities to enterprises, assisting them with the creation and operation of modern container platforms, along with the development of applications atop these platforms. Such providers will typically provide a range of managed services, carefully calibrated to an enterprise's IT and business needs, and designed to maximize the business impact of a cloud-native posture for a client. Concurrently, service providers must be equipped with a structured methodology to help enterprises containerize existing applications across on-premises, hybrid or multicloud platforms. Also, service provider offerings should assist enterprises with setting up orchestration, service mesh, observability and security functionalities, backed by skilled employees in these fields. Providers should also be well versed in DevOps methodologies and site reliability engineering (SRE)/platform reliability engineering (PRE) practices, integrating flexibly with client teams to accelerate software release cycles, while managing the increased burden on operations functions.

Eligibility criteria

- Robust tooling that augments and streamlines the process of operating a container platform for an enterprise, with capabilities tailored to complex business environments
- Expertise in cloud-native operations such as tools and practices to derive the benefits of a cloud-native posture across infrastructure and applications. These include SRE, PRE, and tools to automate cloud-native operations and provisioning
- Strong local employee base with expertise in deploying and operating container platforms, along with building and supporting applications that run on these platforms
- A path to integrate legacy workloads with a modern container platform; the workloads are either running in separate virtual machines or on the container platform itself
- Strong understanding of local compliance and regulatory requirements
- Service structure that prioritizes business benefits for clients (for example, reduced total cost of ownership, improved customer service metrics or faster innovation cycles) from the use of cloud-native technologies
- Relevant certifications, for example the Cloud Native Computing Foundation's Kubernetes Certified Service Provider (KCSP) certification

Container Platform Solutions

This quadrant analyzes ISVs that offer proprietary enterprise software distributions of Kubernetes or other open-source orchestration platforms (for example, Cloud Foundry, Docker Swarm, OpenShift or Nomad). These container-based platform-as-a-service solutions should be based on the relevant upstream open source projects and provide additional capabilities necessary for enterprises to gain greater value from a cloud-native posture such as multi-cluster management, compliance management and patching. Platform orchestration should include an in-depth architecture to support control planes and organize and maintain Kubernetes clusters. Different solutions may allow varying levels of abstraction (for example, application layer as opposed to container layer), to ease or simplify the work of developers. The software should be able to run under an on-premises or a hybrid cloud model.

Eligibility criteria

- Unique capabilities that aid enterprises in developing and adopting Kubernetes, with special consideration for machine learning and edge computing use cases
- Technical support capabilities that assist enterprises with the adoption and management of platform solutions
- Support for on-premises, hybrid and multicloud operations
- Automation of node allocation and pod assignment to guarantee efficiency. Clear business benefits (for example, increased service reliability) tied to use of the Kubernetes platform solution
- Relevant certifications for platforms, such as the Cloud Native Computing Foundation's Certified Kubernetes Distribution

Hyperscaler Cloud-native Platforms

This quadrant analyses hyperscalers that offer a suite of services on platforms designed to help enterprises maximize the business benefits of a cloud-native posture across their IT environments. Many enterprises are looking to harness the benefits of modern containerized applications but — for reasons of cost, flexibility, regulation or environmental performance — want to do so across a hybrid or multicloud environment. Different hyperscalers answer this requirement in different ways. Some focus on extending their cloud-native services and capabilities to on-premises data centers, some are providing managed Kubernetes across different public clouds, and others are moving toward the next frontier of serverless and functions-as-a-service technologies. No matter the model adopted, hyperscalers typically offer additional services such as tools for migrating and modernizing applications from virtual machines into containers; automated configuration management, including policy and compliance monitoring across multiple environments; automated security updating; and support for cloud-native DevOps and integrated CI/CD pipelines.

Eligibility criteria

- Fully managed platforms that automate the deployment of Kubernetes clusters across multiple environments
- Provide flexibility to harness the cloud-native capabilities of the hyperscalers across other environments (for example, a hosted on-premises data center environment or another hyperscaler environment)
- Relevant additional services for supporting Kubernetes operations on the platforms, including multicluster management, managed service mesh, observability and security
- Integration with cloud platform services, with special consideration for machine learning, edge computing and hybrid cloud use scenarios
- Hyperscale cloud infrastructure with container services available from multiple data centers within relevant regions, along with robust enterprise support capabilities in these regions

Cloud-native Observability Solutions

This quadrant assesses software vendors that provide dedicated solutions for observability (logging, tracing and measurement) of containerized applications. Understanding the behavior of these applications can be more complex than a traditional monolith. Developers and operators must understand the behavior of each containerized app or service, including how they communicate with one another. Using standard monitoring tools that have been built without considering cloud-native applications could fail to provide the necessary information to enterprises. Hence, a paradigm shift from host-based monitoring to container and orchestrator-level monitoring is the new cloud-native standard to ensure availability and performance. Thus, enterprises need to opt for specialized capabilities.

Eligibility criteria

- Software with novel capabilities to help enterprises understand the inner workings and performance of their containerized application environments
- Dedicated tools meant for observability, specifically multi-container applications, with support for highly granular microservices architecture, as well as for applications that comprise 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 the software within their environment
- Strong connection between the solution's business model and enterprise outcomes (for example, financial and performance benefits).

Cloud-native Security Platforms

This quadrant assesses software providers that offer proprietary solutions for securing infrastructure and applications in a cloud-native environment, starting from application development all the way to production and run-time. Traditional monolithic security tools are unsuitable to the elastic, distributed and ephemeral nature of the cloud-native environment, where containerized applications are spread across multiple locations, both multicloud and hybrid, and are continually created and updated by multiple users and developers. Cloud-native security providers typically offer a unified platform, providing visibility of the orchestration and container network environment, with features such as scans for vulnerabilities and misconfigurations both during development and at run-time, topology maps, AI-enabled risk assessment, micro-segmentation of the container environment, auto-generation of network policies such as least-privilege access, regulatory compliance monitoring and validation, and identity and access management.

Eligibility criteria

- Unified platform, covering infrastructure and applications, capable of working across on-premises, multicloud and hybrid environments (impact on license management — in which environments they can be run and how that affects costs)
- Ability to integrate with third-party data sources and open source cloud-native security software such as Falco and Prometheus
- Unified visibility for DevSecOps, including intelligent container image screening integrated into CI/CD pipelines; ability to block unscanned or vulnerable images (for example, from public registries or containers with root access to the operating system)
- Use of machine learning for intelligent discovery of container topology and automated remediation
- Strong identity and access management features, including automated least-privilege management and network policies, password management and zero-trust boundaries
- Out-of-the box mapping to major regulatory compliance controls (for example, GDPR and HIPAA)
- Strong connection to delivery of business outcomes for enterprise customers (for example, scheduled and unscheduled downtime, reduction in false positives, improved service reliability and end-user satisfaction)
- Relevant certifications for cloud-native security, such as CNCF, GIAC and CCSP

Quadrants by Region

Quadrants	Global	U.S.	Europe
Managed Container Services	Overview	✓	✓
Container Platform Solutions	Overview	✓	✓
Hyperscaler Cloud-native Platforms	Overview	✓	✓
Cloud-native Observability Solutions	Overview	✓	✓
Cloud-native Security Platforms	Overview	✓	✓

Schedule

The research phase falls in the period **May 2022 to July 2022**. During this period, survey, evaluation, analysis and validation will take place. The results will be presented to the media in **August 2022**.

Milestones	Beginning	End
Launch	May 2, 2022	
Survey Phase	May 2, 2022	May 30, 2022
Sneak Preview	August 2022	
Press Release	September 2022	

Please refer to this [link](#) to view/download the ISG Provider Lens™ 2022 research agenda.

Access to Online Portal

You can view/download the questionnaire from [here](#) using the credentials you have already created or refer to instructions provided in the invitation email to generate a new password. We look forward to your participation!

ISG Star of Excellence™ – Call for nominations

The Star of Excellence is an independent recognition of excellent service delivery based on the concept of “Voice of the Customer.” The program is designed by ISG to collect client feedback about service providers’ success in demonstrating the highest standards of client service excellence and customer centricity.

The global survey is all about services that are associated with IPL studies. All ISG analysts will be continuously provided with information on the customer experience of all relevant service providers. This information comes on top of existing first-hand advisor feedback that IPL leverages in context of its practitioner-led consulting approach.



Providers are invited to [nominate](#) their clients to participate. Once the nomination has been submitted, ISG sends out a mail confirmation to both sides. It is self-evident that ISG anonymizes all customer data and does not share it with third parties.

It is our vision that the Star of Excellence will be recognized as the leading industry recognition for client service excellence and serve as the benchmark for measuring client sentiments.

To ensure your selected clients complete the feedback for your nominated engagement, please use the client nomination section on the Star of Excellence [website](#).

We have set up an email where you can direct any questions or provide comments. This email will be checked daily, please allow up to 24 hours for a reply. Here is the email address: Star@isg-one.com

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 being invited for the survey

Are you on the list, or do you see your company as relevant provider that is missing from the list?

Then feel free to contact us to ensure your active participation in the research phase.

*um	Arctiq	Checkov
2nd Watch	Aspen Mesh	Chef Inspec
Acaisoft	Aspire Systems	Chronosphere
Accenture	Aspiresys	Cinq ICT
Accurics	Aternity	Cisco
Acuvate	Atos	Citrix
Agilisys	AWS	Citynetwork
AgoraKube	Banzaicloud	Clair
Airlock	BeOpenIT	Claranet
Alerant	Birlasoft	Cloudboostr
Alert Logic	BJSS	Cloudera
Alibaba Cloud	Blue Matador	CloudHealth Technologies
All for One Group	Booz Allen Hamilton	Cloudical
Alterway	BoxBoat	CloudIQ
Altoros	Camptocamp	CloudMatos
Anchore	Cancom	CloudOps
Apolicy	Canonical	Cloudpassage
AppDynamics	Capgemini	Cloudreach
Appfleet	Capita	CloudYuga
AppNeta	Capsule8	Codefresh
AppOptics	Catchpoint	Coforge
Appvia	Centreon	Cognizant
Aqua Security	Checkmk	Component Soft

Partial list of companies being invited for the survey

Are you on the list, or do you see your company as relevant provider that is missing from the list?

Then feel free to contact us to ensure your active participation in the research phase.

Computacenter	Desktop Kubernetes	Fugue
Conoa	Desotech	Fujitsu
Container Solutions	Devoteam	Fullstaq
Containous	Diamanti	Genpact
Content+Cloud	DigitalOcean	Giant Swarm
Contino	DoiT	Google
Contrast Security	DXC Technology	Gradle Enterprise
Controlplane	Dynatrace	Gremlin
Cortex	Eficode	Guida
Cuemby	Elastisys	HashiCorp
Curiefense	Elastx	HCL
D2IQ	Engineer Better	Hexaware
Data Essential	Entigo	Hitachi Vantara
Datadog	Epsagon	Honeycomb
Datadrivers	Ericsson	HPE
DataStax	Fairwinds	Humio
Decipher Technology Studios	Fivetran	Hyve
Deepfence	Flant	IBM
Deepshore	Flexkube	IBM/Red Hat
Dell Technologies Consulting	Flowmill	Icinga
Deloitte	Fossa	Infinite
Dembach Goo Informatik	FossilID	infogain
Denodo	Fuga Cloud	Informatica

Partial list of companies being invited for the survey

Are you on the list, or do you see your company as relevant provider that is missing from the list?

Then feel free to contact us to ensure your active participation in the research phase.

InfraCloud	Nebulaworks	Red Kubes
Innovations ON	Netways	Redpill Linpro
Instana	New Relic	Redploy
Ionos	Noris network	Replex
Jaeger	Novetta	RX-M
Jelastic	NTT DATA	SAP
Jetstack	Nutanix	Scale Factory
Kamatera	OBSS	ScaleUP Technologies
Kasten	Occentus	Scaleway
kiratech	OCTO Technology	Servinga
Kong	Opsdis	SIGHUP
LeanIX	Oracle	SLK Software
Lightstep	Origoss Solutions	SmartStream
Litmus	Oteemo	Softax
Logz	OvHcloud	SoKUBE
Mantisnet	Persistent Systems	Sonata - Software
Microland	Platform9	SparkFabrik
Microsoft	PlusServer	Spectro Cloud
Mirantis	Prodyna	Splunk
Mobilise	Pulsant	Stackpath
Mphasis	Rackner	StackRox
MSys Technologies	Rackspace	Stackstate
Navitas	Rancher (SUSE)	Stakater

Partial list of companies being invited for the survey

Are you on the list, or do you see your company as relevant provider that is missing from the list?

Then feel free to contact us to ensure your active participation in the research phase.

Starburst	UKFast
Stark & Wayne	UST
Steadybit	ValueLabs
Storm Reply	Ventus Cloud
Sumo Logic	Virtuozzo
SUSE	VmWare
SVA	Vultr
Sysdig	Weaveworks
SysEleven	WhizUS
Talend	Wipro
TCS	x-cellent
Tech Mahindra	XenonStack
Translucent Computing	YLD
TietoEvry	Zabbix

Contacts for this study



Mark Purdy
Lead Analyst



Mirza Iqbal
Research Analyst



Ravi Ranjan
Project Manager

Do you need any further information?

If you have any questions, please contact us at isglens@isg-one.com.

ISG Provider Lens QCRT Program Description

ISG Provider Lens™ offers market assessments by incorporating practitioner insights, reflecting regional focus and conducting independent research. ISG ensures advisor involvement in each study to cover the appropriate market details aligned to the respective service lines/technology trends, service provider presence and enterprise context. In each region, ISG has expert thought leaders and respected advisors who know the provider portfolios and offerings as well as enterprise requirements and market trends. On average, three advisors participate as part of each study's Quality and Consistency Review Team (QCRT) that ensures each study reflects ISG advisors' experience in the field, which complements the primary and secondary research the analysts conduct. Advisors participate in each study as part of the QCRT group and contribute at different levels depending on their availability and expertise.

The QCRT advisors:

- Help define and validate quadrants and questionnaires
- Advise on service providers inclusion, participate in briefing calls
- Give their perspectives on service provider ratings and review report drafts

The ISG Provider Lens QCRT program helps round out the research process, supporting comprehensive research-focused studies.

Quality & Consistency Review Team for this study



Iain McLurcan
Director



Rakesh Parameshwara
Principal Consultant



Venkatesh Sangam
Senior Consultant

Do you need any further information?

If you have any questions, please contact us at isglens@isg-one.com.