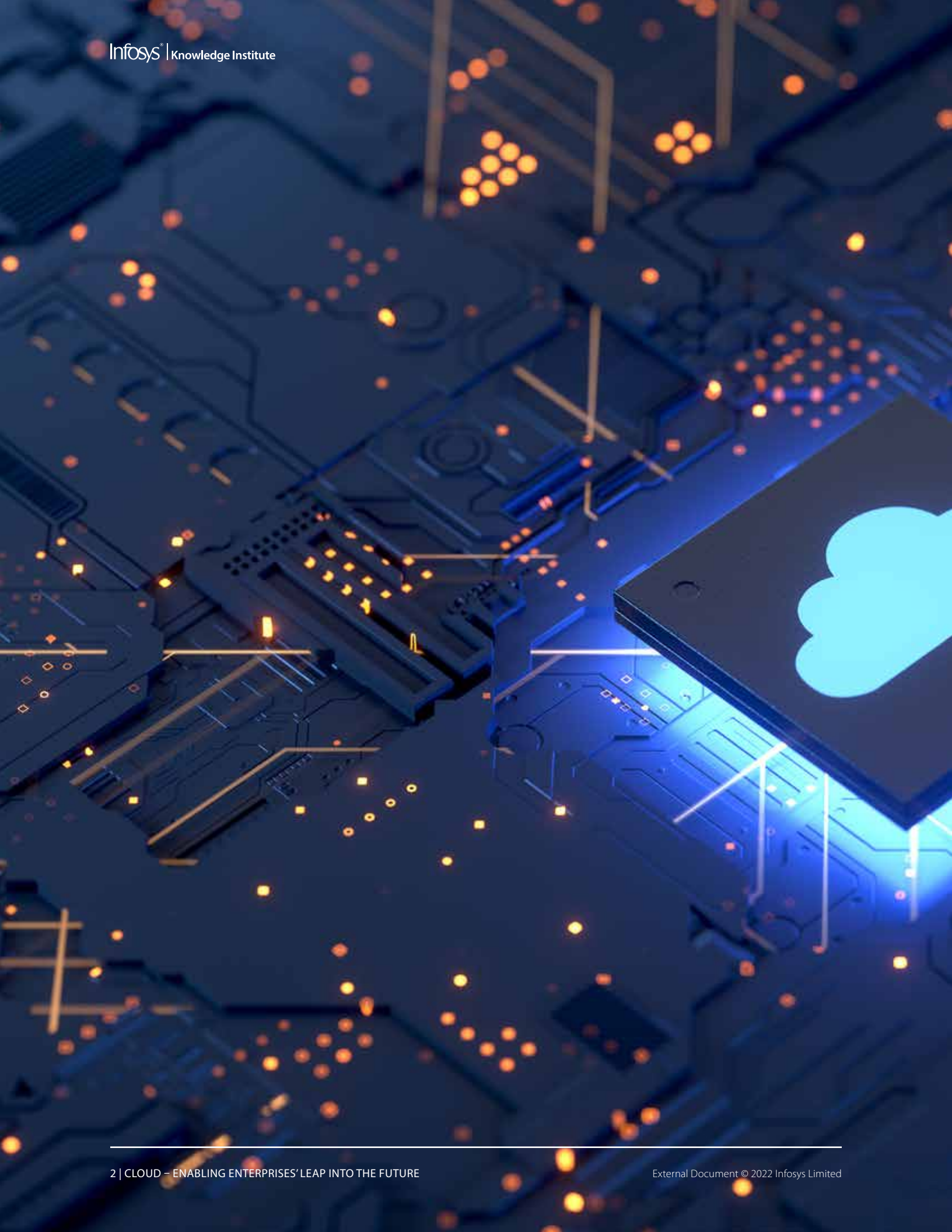
Infosys®
Navigate your next

CLOUD – ENABLING ENTERPRISES' LEAP INTO THE FUTURE

Infosys® | Knowledge Institute



Contents

Cloud-native technologies helped businesses smoothly navigate the pandemic with speed, agility, and innovation. Cloud has become the key to developing solutions quickly and at scale. Growing demand for immersive experiences, responsiveness, and intelligent decisioning at the point of consumption extends the cloud continuum to the edge.

Enterprises are adopting a hybrid multicloud approach to build business capabilities. They use a combination of public clouds, software as a service (SaaS), and private clouds based on specific needs. However, businesses must strike a balance between existing and new investments to enhance business capabilities and optimize the cloud setup.

The services from cloud technology providers (across public cloud and SaaS) are maturing fast. Providers are offering industry cloud solutions capable of efficiently solving business problems. Typical boundaries within enterprises are collapsing with agile ways of working. Hyperautomation is further enhancing delivery speed across business functions.

A recent **Infosys study** found that enterprises that have shifted more than 60% of their workloads to cloud could meaningfully improve their bottom line. The exceptional performers use hybrid multicloud more often for consolidating and surfacing enterprise data, increasing speed of application deployment, and closely collaborating across the partnership ecosystem.

Evolution in the cloud continuum

Horizon 1 (H1): In the first phase, the cloud was mainly utilized as infrastructure as a service (IaaS). Enterprises extended their data center model, including processes and tools, to the cloud, leveraging infrastructure programmability. This enabled them to start new projects faster, but they still considered cloud as a cost lever. During the following phase, SaaS became mainstream in user productivity, collaboration, and business support functions.

Horizon 2 (H2): Enterprises move toward a cloud-first approach and invest in harnessing the power of hybrid cloud and automation to gain agility, efficiency, and scalability. This cloud-native transformation model starts with containers and serverless technology, integrated security, and embedded governance. This rides on the backbone of "as a code" for every aspect of the software engineering and delivery lifecycle.

Here, SaaS adoption for core business functions and a strong application programming interface (API)-based integration platform digitally connect all stages of business processes.

Horizon 3 (H3): Enterprises are increasingly evolving their cloud adoption approach to align with the global-scale system and exploring opportunities. The cloud continuum will encompass the edge for newer use cases such as gaming, metaverse, process automation, and autonomous operations. In a perimeterless topology, a "zero-trust" security model helps manage distributed systems, powered by artificial intelligence (AI)-backed security operations. Here, industry cloud will take the center stage by partnering with industry consortia and technology vendors and create an open platform for innovation and interoperability.

Let us explore capabilities and trends across each of the following subdomains:

Platform as a service

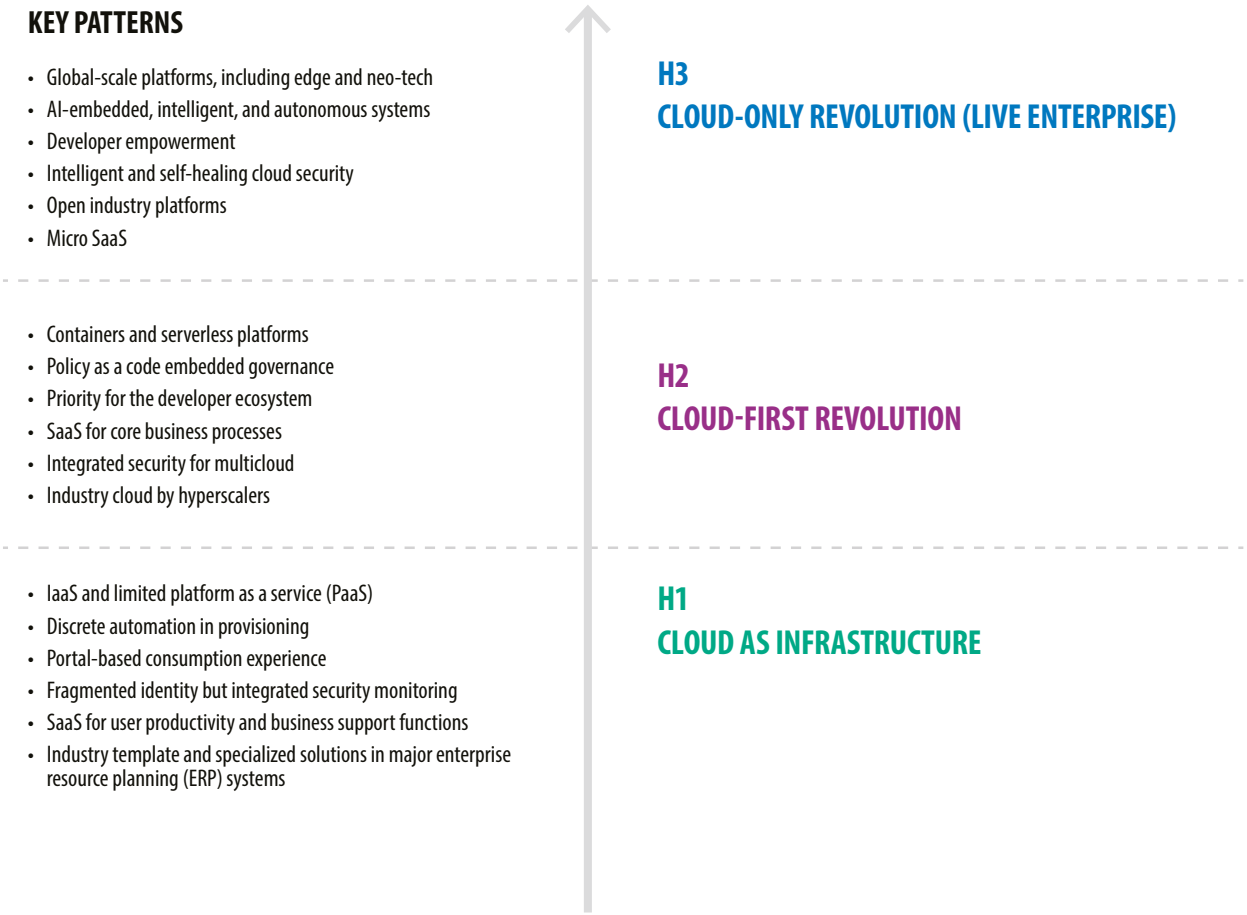
Migration, management, and operations

Software as a service

Cloud security

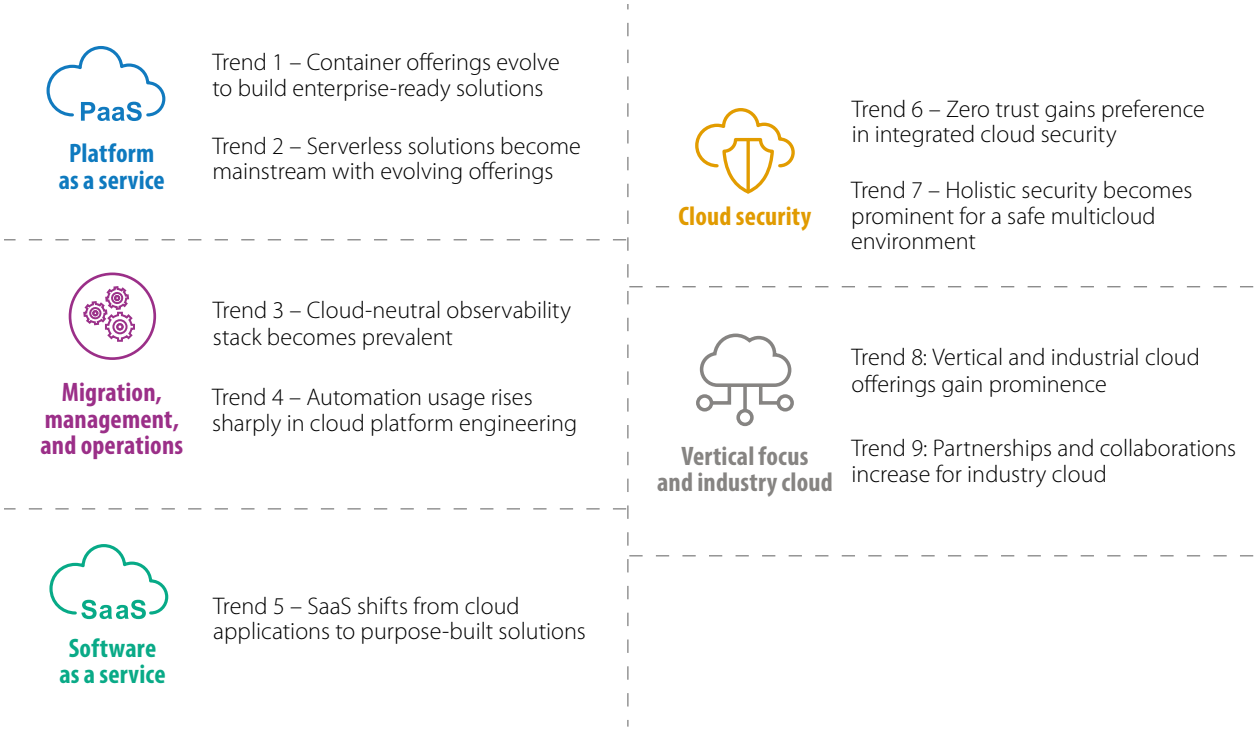
Vertical focus and industry cloud

Figure 1. Adapting to market dynamics: the three horizons



Source: Infosys

Figure 2. Key trends across cloud subdomains



Source: Infosys

PLATFORM AS A SERVICE

Managed PaaS providers continue to expand their offerings. This allows enterprises to leverage on-demand infrastructure and software environments to enhance their business capabilities. Managed PaaS for application runtimes, databases, containers, and integration services is widely accepted. Container ecosystems have further evolved, bundling serverless, application, and microservices constructs like service mesh and deeper integration with other cloud services (including security). Developer and operational tools such as AWS Proton and Azure DevOps focus on managing and releasing into PaaS environments. Big data processing solutions have seen an uptick, with ubiquitous storage on the cloud and managed services for distributed processing such as Databricks, AWS Glue, Azure Data Factory, BigQuery, and Azure Synapse becoming mature. PaaS offerings such as Azure Machine Learning, Google AutoML, and AWS SageMaker further democratize machine learning (ML) and internet of things (IoT) spaces, allowing easy onboarding and experimentation for new initiatives. Open source continues to see attention from hyperscalers and enterprises to build portability and cloud readiness into applications. Edge computing services like Anthos, Outposts, and Azure Arc and storage migration services support hybrid workloads. Hyperscalers innovate in specialty compute options, cognitive services, self-service ML, industry cloud, blockchain services, and connected ecosystems.

Trend 1 – Container offerings evolve to build enterprise-ready solutions

Using containers for building scalable and portable microservices has become the de facto standard across all digital platforms. Kubernetes emerged as a standard for orchestration and management of container deployments. Every hyperscaler already had its version of managed Kubernetes, allowing customers to deploy containers at scale. This past year has seen further evolution of these offerings to make them enterprise-ready and a complete stack for building applications. As more applications are deployed onto Kubernetes clusters,

more sophisticated requirements for connectivity, observability, and security lead to extended offerings of service mesh components such as Istio, Open Service Mesh, and Dapr.

Deployment pipelines are more automated, with secrets management and container image scanning built in. Serverless versions of container services such as AWS ECS Fargate, Azure Container Apps, and Google Cloud Run have been added to run one-of batch kinds of workloads. Event-driven pod execution and on-demand scaling have been added with the integration of KEDA, Knative, and Virtual Kubelet frameworks. Ingress services have been integrated with the cloud provider's load balancer (e.g., AWS Elastic Load Balancing) and gateway services (e.g., Azure Application Gateway). Enterprise-supported offerings such as Red Hat OpenShift are now available in a managed services model across cloud providers.

These solutions address the complexity of administering and managing Kubernetes-based solutions, making adoption easier for enterprises. IT teams can focus completely on building business applications and less on cluster management, software upgrades, certificate management, and other complexities around Kubernetes.

In collaboration with Infosys, a U.S.-based specialty auto parts provider built Next-Generation Auto Repair Assistant Platform. It was developed using container technologies on AWS with ECS Fargate, along with Amazon's Simple Storage Service (S3), API Gateway, and DynamoDB. The platform helps car owners book services at registered garage workshops with the integration of Google Maps and geolocation. It leverages an AWS ECS Fargate cluster for its API back end, which completely removes any provisioning requirement and scales to workload, optimizing hosting costs.

Trend 2 – Serverless solutions become mainstream with evolving offerings

Function as a service (FaaS) is a serverless way to execute modular pieces of code on the edge of computer systems. FaaS lets developers write and update a piece of code on the fly that can be executed in response to an event, such as a user clicking on an element in a web application. Offerings such as AWS Lambda, Azure Functions, and Google Cloud Functions support several programming languages and even container images. Newer serverless offerings have emerged, including containers, messaging middleware, big data processing, workflow orchestration, and low-code (LC) platforms. In fact, serverless and LC together significantly increase the speed of application delivery. From the developer's perspective, there is no server and no need for extensive programming to create business logic. The developer tooling, software development kits (SDKs) and support for DevOps, observability, and debugging have also improved. Hyperscaler solutions continue to address challenges around provisioning scale, integration with other cloud services, and security.

Enterprises should view the space as an opportunity to streamline API, microservice, and event-driven application implementation. Serverless solutions will continue to drive down application costs and evolve to better suit varying workload requirements.

A leading engine manufacturer in North America partnered with Infosys to modernize its legacy approval system with a centralized, one-stop, and on-the-go approval solution. It utilized serverless technologies, including API Gateway, Lambda, Step Function, SES, SNS, Aurora serverless, S3, and Azure AD, to track and act upon asset requests from multiple heterogeneous systems in near real time. This resulted in significant licensing costs savings on the legacy database and forms software. It helped build a pay-per-use model for an application with a highly variable load.

MIGRATION, MANAGEMENT, AND OPERATIONS

Shifting to the cloud involves numerous difficulties. Many firms spend too much, too soon, on cloud, without performing enough research on their specific requirements. And that leads to cloud burnout. Also, the sheer number of cloud solutions often thwarts cloud migration, and many organizations revert to adopting cloud in pockets, running up the cost. This is where good migration, management, and operations tools come to the fore, with automation and embedded governance becoming the key to cloud success. In recent years, enterprises have shifted from single to multicloud setups, X as a code, and policy-driven strategies. In addition, the focus on governance and compliance has resulted in specialized solutions for embedded governance from cloud vendors. Automated management of cloud systems will become mainstream in the coming years. The focus will significantly increase on intelligent workload-centric orchestration, enhanced developer empowerment, and integrated monitoring. We expect intelligent and synergized orchestration, involving the integration of enterprise workloads orchestration and network orchestration, to become popular. Likewise, solutions will emerge to enhance developer productivity through automatic service deployments using reusable templates, unified AI platforms to build and scale ML models faster, and an integrated observability platform for a unified and real-time view of services, resources, software, etc.

Trend 3 – Cloud-neutral observability stack becomes prevalent

Enterprises are increasingly adopting multicloud environments. This gives them access to on-premises clouds and multicloud vendors to avoid vendor lock-in, add capacity, and leverage unique capabilities such as surfacing enterprise data for ML use cases. In fact, top performers in the recent cloud research by the Infosys Knowledge Institute use more than three cloud vendors, with a bias toward hybrid multicloud. This, however, leads to some challenges in observability, including vendor-specific tools, lack of all information in one place, high monitoring costs, multiple standards, etc. To monitor such complex systems, enterprises need a single pane of glass to monitor various cloud components, including applications, services, infrastructure, microservices, etc., cutting across multicloud vendors/multiclusters/multiregional deployments. Enterprises are adopting cloud-native

and third-party tools like the Elastic Observability suite, Datadog multicloud monitoring suite, and LogicMonitor multicloud monitoring tool, etc., to reduce complexities in multicloud environments. These tools measure the health of application performance and behavior using vast amounts of collected telemetry data such as metrics, logs, and incidents. This lets those developing applications understand what's wrong with a system, what's slow or broken, why an issue occurred, and how it will affect the whole cloud ecosystem.

A large multinational financial advisory service company is working with Infosys to implement an observability toolset and a site reliability engineering model that provides convergence of metrics, logs, traces, and AI-powered insights in a multicloud environment. Similarly, Infosys is helping a technology company implement a cloud-neutral observability stack for multicloud operations.

Trend 4 – Automation usage rises sharply in cloud platform engineering

Automation is increasingly contributing to improved developer productivity. Multicloud vendors offer a multitude of technologies, platforms, and tools to help developers in their day-to-day tasks. Currently, developers need end-to-end frameworks and tools to manage all services and related resources such as infrastructure, deployments, pipelines, etc., in an integrated fashion. One way to achieve this is to have an integrated developer portal for a unified view of services, resources, software, etc. Developers also need a fully managed application delivery service that can automate the deployment of all types of cloud-native workloads such as containers, serverless, etc. This is done through standard and automated service templates across multicloud environments. Developers and data scientists working on AI and ML models also need a unified AI platform to build and scale ML models faster. Enterprises are looking for ready-to-use frameworks or tools that can enhance developer productivity. Some examples include AWS Proton, Google Vertex for unified AI, and Backstage. Google Vertex is out in front, with the ability to use the same dataset for different models, significantly reducing costs and errors. The model training pipeline is also automated, with a series of containerized steps that helps with generalization, reproducibility, and auditability.

A large Japanese auto company is working with Infosys to build a cloud services consumption platform for its U.S. business unit. Developers can use this platform to develop applications on the cloud and provide services across the application engineering lifecycle, eliminating the friction with the platform team. This enables the company to embrace agile with the DevSecOps model, which increases speed to market and developer productivity.

SOFTWARE AS A SERVICE

Enterprises accelerate their SaaS cloud journey to deploy vertical-specific solutions and access collective capabilities. Micro SaaS vertical services and extensions with deep industry insights bring specialized knowledge and industry best practices to specific business flows. The information across data islands is integrated through APIs and converted into timely advice and action through ML and AI. Further, low-code, no-code (LCNC) platforms enable business teams to respond faster and become agile, aiding the development ecosystem for faster adoption and rapid development. LCNC also helps the wider workforce become tech savvy, with users who have minimal coding expertise building departmental systems, providing a boon to enterprise productivity.

Trend 5 – SaaS shifts from cloud applications to purpose-built solutions

SaaS companies are transforming themselves from providers of cloud applications to providers of purpose-built industry cloud solutions through organic and inorganic expansions. The user interface layer, the data model, and the declarative/customer business logics of these products have all been tailored to suit the needs of various industries such as communications, utility, health, insurance, media, and public cloud.

Foundational and metadata constructs are available to design for the business needs of specific functions such as sales, orders, pricing, and product catalog.

Industry data model-based extension and LCNC platforms bring in cross-industry synergies. SaaS providers are also creating industry process-based libraries, consisting of accelerators to swiftly track the development and design of their platforms.

Businesses should adopt industry clouds and LCNC solutions for their core functions. This requires senior leadership sponsorship and identification of a core execution team with clear ownership and responsibilities across IT, third parties, and business owners. Businesses must ensure data security and privacy and have these covered as part of their SaaS solutions. They should continually monitor the spend on SaaS licenses and embark on cost takeout and license optimization/automation initiatives. Businesses should leverage SaaS solutions in the best possible way through continuous training and the enablement of user groups.

A large telecom player wanted to transform its B2B operations and commercial 5G offerings. Transformation objectives included the unification of look and feel across all channels for all partners/users, digitization of quote and order management, and process standardization and simplification. The company applied the design thinking approach to create role-based personas, and an intuitive user experience to provide a 360-degree view of the customer portfolio. The solution creates and baselines platforms for accelerated product/service rollouts (including 5G). The solution is developed on the Salesforce Industries-Vlocity platform, providing differentiation while allowing partners to create quotes, place and track orders, and change or disconnect the existing services.

CLOUD SECURITY

Increased use of cloud resources has increased cloud security risks, with malicious actors taking advantage of misconfigurations and vulnerabilities. This requires developing a strong cloud ecosystem, adopting zero-trust principles, and addressing supply chain vulnerabilities. Cloud security has transformed from a siloed, control-based, and reactive process to a more holistic and continuous process of strengthening the security posture throughout the lifecycle. Thus, the adoption of secure-by-design principles is now essential for cloud transformation. Here, security is no longer considered as a bolt-on aspect of the overall cloud framework. Instead of viewing security as merely a technology issue, security by design considers all systems, processes, and people, right from the start. As the threat landscape increases due to massive digitization across industries and the integration of IoT and operational technology with IT, the people and process elements are now more important than ever. Properly devised cloud security can reduce costs and aid organizations in increasing customer and employee satisfaction through enhanced confidence in the systems that make life rewarding and enjoyable.

Trend 6 – Zero trust gains preference in integrated cloud security

Enterprises are increasingly adopting the zero-trust approach to make a next-generation, cyber-resilient cloud environment. This approach follows the principles of "least privilege," "assume breach," "verify explicitly," and multiple security controls. Important controls include the following:

- Cloud security policies or guardrails on cloud resources at various layers. These include root, subscriptions, accounts, management groups, resource groups, and staging environments, to have better security and governance.
- Attribute-based access control (ABAC) model that uses attributes, rather than roles, to grant user access. It can control access on a more detailed level and it helps maintain dynamic control of conditional access policies after the completion of first-factor authentication. Conditional access isn't intended to be an organization's first line of defense for scenarios like denial of service (DoS) attacks, but it can use signals from these events to determine access.

- Microsegmentation for creating network zones in cloud environments to isolate workloads from one another and secure them individually against protection of east-west traffic. It reduces the network attack surface, improves breach compliance, and strengthens regulatory compliance.

An American multinational food company wanted to migrate its applications to Google Cloud Platform (GCP) with the utmost security. Infosys was selected as its cloud infrastructure and security partner. The company followed the zero-trust security architecture to implement end-to-end cloud security solutions for better cyber resilience and error-free cyber protection. The entire service included setting up cloud guardrails, access controls, network segmentation, data protection, and security logging.

Trend 7 – Holistic security becomes prominent for a safe multicloud environment

Companies are using multiple clouds to meet business continuity and disaster management requirements. This enables them to use the best-suited cloud services based on specific requirements. While cloud adoption has intensified, it is crucial to strategically work on minimizing associated cyber risks. Integrated cloud security platforms help organizations establish secure environments while working with multiple clouds. These platforms consist of various functionalities such as cloud security posture management (CSPM), cloud workload protection platform (CWPP), cloud infrastructure entitlement management (CIEM), vulnerability management, etc. This enables businesses to perform the following:

- A shift-left approach to security, which ensures real-time management of cloud assets, inventory, cloud security posture, and vulnerability.
- Unified threat management for multicloud assets, including, virtual machines (VMs), PaaS components, containers, and functions.
- Periodic reviews of identity to ensure reconciliation.
- Cloud microsegmentation to create network zones in cloud environments; this helps in isolating workloads based on their functionality and cyber criticality.

There is a caveat, though. Holistic security requires a highly talented workforce, but security experts are in short supply. Seven out of 10 software developers are expected to write secure code, but less than half receive adequate training. And the shortfall of security workers is projected to be 1.8 million this year alone. Even more, firms will have to do six things well to contend with the current climate for cybercrime. First, a security architecture review process should be set up for all systems that firms develop or procure from third parties. Second, they must also conduct threat modeling for complex projects. Third, every person in the organization must undergo security awareness training, particularly in multicloud authentication environments. Fourth, only security-tested, legally vetted open-source components should be used by development teams. Fifth, DevSecOps should be used in software deployment, fusing business, development, testing, infrastructure deployment, and operations. And sixth, and perhaps most important, the C-suite must be involved in the definition of "holistic secure-by-design" in the firm; to this end, the function of the chief information security officer should be empowered to make big decisions quickly.

A U.S.-based global technology company, which develops conversational commerce software, established an integrated cloud security platform. The platform can protect all cloud assets in the multicloud environment, identify misconfigurations, and secure containers and VMs to provide a compliance score. The solution has fortified the company's multicloud platform against cybersecurity risks while ensuring that it meets regulatory requirements.

VERTICAL FOCUS AND INDUSTRY CLOUD

Industry cloud offers customized cloud computing to meet industry-specific business, operational, legal, regulatory, and security considerations. Analyst findings reveal that industry cloud will drive the next generation of business-centric services. Over the past few years, cloud services have matured from IaaS, PaaS, and containers as a service (CaaS) to comprehensive business solutions. These innovative solutions adhere to industry-specific regulations such as Fast Health Interoperability Resources (FHIR).

Organizations are increasingly investing in industry cloud to stay ahead of the competition, resulting in an open marketplace for industry-specific innovations. Traditional cloud service providers (CSPs) like Azure, GCP, and AWS, and others like SAP and ServiceNow, leverage industry cloud to build end-to-end cloud solutions. For instance, in financial services, Azure provides specialized cloud applications and systems that are tailored to banking firms — addressing their needs in a stringent and evolving regulatory environment. Industry cloud offerings for health care providers include personalized experience use cases, along with medical management, member acquisition, value-based care, and telemedicine/home health. These applications create a seamless and unified customer experience across all channels, along with enabling data mining, for an end-to-end view of each health care member.

Trend 8: Vertical and industrial cloud offerings gain prominence

According to IDC, the health care sector spent the most on industry cloud, followed by the public and finance sectors. Industry cloud consolidates industry-specific services, tools, data, and analytics, and brings AI/ML to bear for intelligent business operations. It provides end-to-end integrated solutions with all the regulatory compliance needs of the vertical.

Industry cloud enables rapid deployment of innovative industry-specific solutions at a reduced cost. For example, multiple organizations have adopted health care cloud services like Azure FHIR and GCP Healthcare API. The health cloud also provides various connectors and accelerators for data transformations like Azure IoT Connector to connect high-frequency data streams from devices by transforming telemetry into FHIR Observations.

A North American healthcare organization wanted to achieve full compliance for its patient access, provider, and pharmacy directory. The company, in partnership with Infosys, developed a solution for FHIR implementation and integration. The solution aided the organization in scaling operations quickly while adhering to stringent timelines. The FHIR-compliant data models/lakes enable the company to make data available for any future implementations of interoperability applications.

Trend 9: Partnerships and collaborations increase for industry cloud

Industry cloud providers (such as hyperscalers) and SaaS providers (Salesforce, SAP, and ServiceNow) collaborate with business and core product vendors and system integrators for industry cloud implementations.

Organizations are also partnering to develop industrial cloud platforms that provide community-driven cloud-based marketplace solutions. For example, in collaboration with AWS and integration partner Siemens, Volkswagen has built its Digital Production Platform for the Volkswagen factories. This open platform enables partners to create their own software in the marketplace. Similarly, Microsoft partnered with BMW to build BMW's Open Manufacturing Platform.

Industry-specific traditional core product vendors and hyperscalers are collaborating to increase the business value of cloud. For example, AWS is working closely with Epic for a cost-effective deployment of Epic environments on AWS. Notably, Epic is a U.S.-based electronic medical record company handling the database of more than 250 million patients.

Glossary

Abbreviation/Acronym	Full term-form
ABAC	Attribute based access control
AI	Artificial intelligence
API	Application programming interface
AWS	Amazon Web Services
CAAS	Containers as a service
CIEM	Cloud infrastructure entitlement management
CSP	Cloud service providers
CSPM	Cloud security posture management
CWPP	Cloud workload protection platform
DOS	Denial of service
ERP	Enterprise resource planning
FAAS	Function as a service
FHIR	Fast Health Interoperability Resources
GCP	Google Cloud Platform
IAAS	Infrastructure as a service
IOT	Internet of things
LCNC	Low code - no code
ML	Machine learning
PAAS	Platform as a service
SAAS	Software as a service
SDK	Software development kit
VM	Virtual machines
XR	Extended reality

Advisory Council

Mohammed Rafee Tarafdar

SVP and Chief Technology Officer

Narry (Narsimha M)

EVP and Head Global Services – Independent Validation Solutions

Shaji Mathew

EVP and Service Offering Head – Health, Insurance & Life Sciences

Satish HC

EVP, Head Global Services – Data and Analytics

Vishal Salvi

SVP – Chief Information Security Officer, ISG

Gautam Khanna

VP – IP Deployment and Commercialization

Saju Sankarankutty

VP – Unit Technology Officer

Pradeep Yadlapati

VP – Delivery Head

Contributors

Amit Junankar

Anjali Yadav

Avinash Dongre

Darshan Singh

Deepak Palasamudram

Dinesh Nagabushanam

Harry Keir Hughes

Madhanraj Jeyapragasam

Muralidharan Srinivasan

Ramkumar Krishnamurthy Dargha

Saurav Kanti Chandra

Senthil Kumar Shanmugam

Shambhulingayya Aralelemath

Vijayaraghavan Varadharajan

Vijith Vayanippetta

Viral Thakkar

Producers

Ramesh N

Infosys Knowledge Institute
ramesh_n03@infosys.com

Abhinav Shrivastava

Infosys Knowledge Institute
abhinav.s08@infosys.com

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision-making on critical business and technology issues.

To view our research, visit Infosys Knowledge Institute at infosys.com/IKI or email us at iki@infosys.com.

For more information, contact askus@infosys.com