The bridge to possible

Cisco Cloud Experience

Bridge all clouds to deliver the experience you desire

March 2021

Contents

Cisco focuses on application experience by seamlessly supporting its customers' application development and delivery requirements with hybrid, multicloud, app-centric infrastructure.

We do this with agile and secure operations across XaaS, on-premises, and private and public cloud platforms, providing consistent security across the required layers with full observability and control of application behavior and performance, wherever those applications reside.

The future of work and applications in multicloud

The disruption to lives and business caused by the global pandemic has shown how much we all rely, as consumers and workers, on services and applications that are delivered from the cloud. This has accelerated new approaches to working and living, with significant implications and responsibilities for technology platform providers.

Throughout, Cisco® has supported its own workforce and that of its partners and customers with a range of products, services, and capabilities which have helped deliver a degree of continuity to the lives of people everywhere.

Cisco, as a global enterprise, is at the forefront of multicloud services adoption, as a consumer, SaaS provider, and, most importantly, enabler of the multicloud journey for our customers and partners. We have developed a wide range of capabilities, services, and partnerships to deliver cloud-agnostic, cloud-native software solutions. These solutions enable and optimize your multicloud, hybrid, and edge deployments, with end-to-end secure connectivity, assurance, and visibility.

From our own experience, and in conversations with our customers and partners, we have observed five key needs in a hybrid, multicloud, multi-app environment:

- Enabling continuity for and powering a distributed workforce with business resiliency.
- Fast innovation with an observable, cloud native, application-centric technology stack to provide insights that drive the application experience.
- Seamless and consistent security, visibility, governance, and control across endpoints, network, cloud, and application environments.
- Easy and secure connecting of distributed users, devices, and applications with heterogenous cloud and on-premises resources.
- Establishing a cloud operating model with a uniform approach to building and deploying modern applications and consuming services across multicloud.

Cisco is a unique position to address these needs, as discussed below.

Cisco's multicloud capabilities

Our multicloud service and product capabilities continue to grow and evolve. Today, we are addressing the key needs discussed above by:

- Enabling full-stack, multi-vendor, seamless application and user experience observability, across connectivity, compute, storage, and security, integrated with the deployment, orchestration, and behavior of the applications and microservices that deliver the experience.

- Providing an open and modular framework that integrates with best-of-breed tools across the application delivery lifecycle to scale, monitor, and automate application delivery performance.
- Delivering automation plus actionable and measurable insights with an AI- and ML-based closed-loop operational model to proactively identify and resolve issues, so that business objectives and SLAs can be automatically met.
- Automating Secure Access Service Edge (SASE) across domains, reducing cost and complexity, and enabling NetOps and SecOps, together, to deliver a scalable, secure, and seamless connectivity experience with full visibility across all network and security domains.
- Consistently integrating software-defined networking (SDN) solutions natively with cloud provider networks and CoLo partners across the Internet for full automation and visibility of experience, for all users, regardless of location, as well as for all applications, regardless of where those applications are deployed.
- Securing the business across the broadening and evolving attack surface that multicloud inevitably introduces, with an integrated and open zero-trust security architecture of unrivalled breadth and depth, unified under the SecureX operations platform.
- Reducing security fragmentation across multiple layers, on-premises and in the cloud, with a unified approach to identity-based access control and workload security, with cloud-based services for remote workers and advanced threat detection.
- Helping our customers define an agile, consistent, automated, and scalable cloud-native operating model that simplifies and unifies development, security, and delivery across the full stack.
- Supporting full-stack observability across the varying forms of traditional and modern application architectures, including multicloud services agnostic to the infrastructure, with real-time, actionable insights leading to automated or manual actions.
- Centralizing management, operations, and visibility for the multicloud, with a seamless deployment and operating model across XaaS, on-premises, and private and public cloud, focused on the application experience, at scale.
- Enabling hybrid infrastructure-as-code (IaC) with unified integration and deployment across multicloud platforms, regardless of where workloads sit, while continually optimizing based on the insights provided by full-stack observability.
- Hybridizing the capabilities that support the workforce wherever they may be and whatever tools they may be using, with secure and reliable access to corporate resources, wherever and however those resources are deployed.
- Expanding on our unique position as a company that, for decades, has used a remote work model for many employees, to help our customers and partners understand, implement, and deliver the complete, best-of-breed solutions we continue to perfect with our global workforce.
- Digitizing our business and our way of thinking and working as a very large global enterprise, so that we can truly test and optimize the secure, holistic digitization and collaboration platforms and solutions we deliver for our customers and ourselves.
- Making the workplace trusted, safe, and secure with capabilities to analyze the movement of people and help ensure that social distancing and utilization policies keep the workforce healthy.

In the rest of this white paper, we provide further insight and details about Cisco's contribution to the multicloud journey of our customers and partners.

What is multicloud?

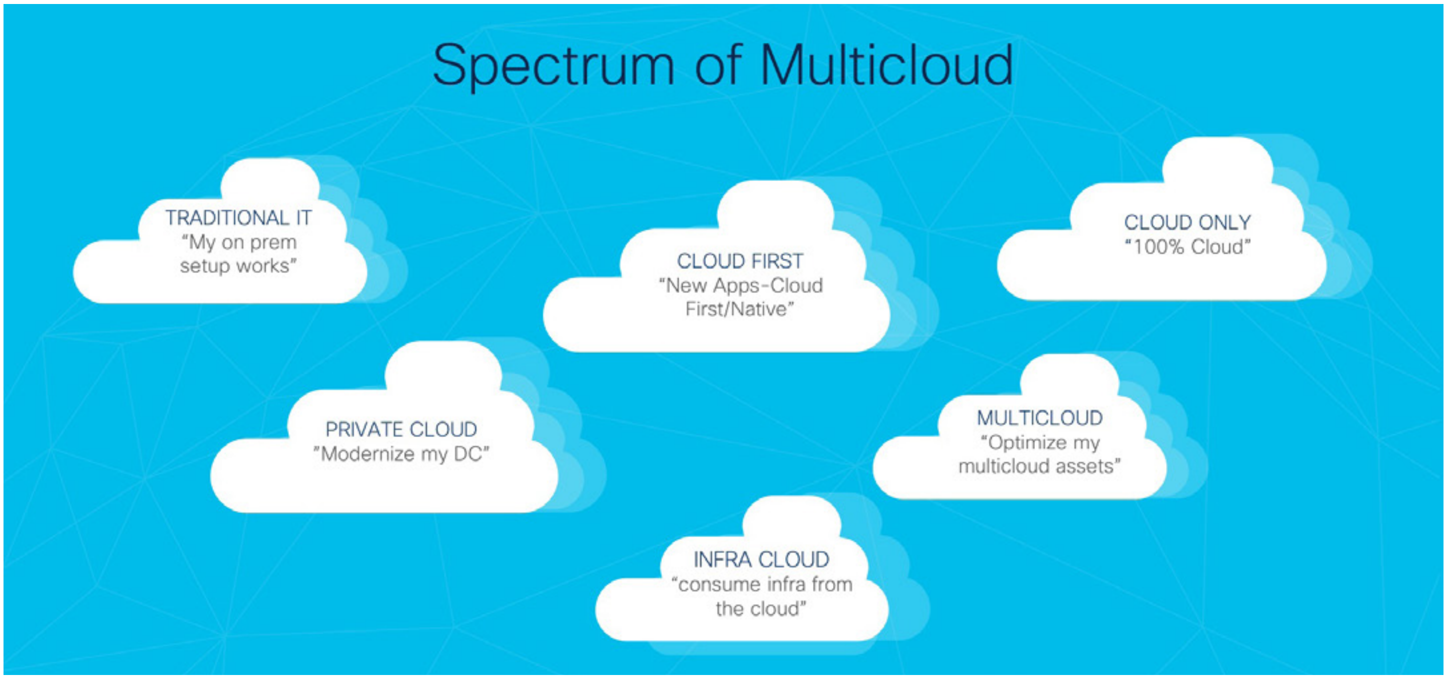

Figure 1.
The Spectrum of Multicloud

Multicloud[1] is the use of services from multiple cloud platforms, including private on-premises and co-located data centers, SaaS, IaaS, PaaS, edge compute, and public cloud providers, including AWS, Azure, GCP, IBM, and potentially others[2]. Under different circumstances, a given form of cloud service will better optimize the application experience, at a given cost point, for reasons related to connectivity, automation capabilities, service type and availability, price point, location, regulatory constraints, privacy, security, and so on.

Thus arises “multicloud,” which is simply the reality today. IDC, in their Cloud Pulse 1Q20 Survey[3], reported that 97% of surveyed enterprises are using multiple public cloud services and private clouds. All the available tools can, and will, be used to deliver the applications that underpin the modern enterprise, in different ways, depending on a wide variety of circumstances. This is, in effect, the multivendor IT purchasing strategy for the cloud era.

As the adoption of multicloud has increased, so has the potential for evolution to cloud-native operating models and the transformation in IT capabilities delivered by such an evolution. That transformation, in turn, helps enable agility and responsiveness for the business. Hence, the rationale for multicloud is evolving from IT economics to business advantage—it is what multicloud does for the business that really matters.

What enables multicloud?

Some aspects of cloud services are homogeneous, such as Kubernetes (K8s) and Docker-based containers for virtualization and microservices. Others include Linux as a base operating system, a wide range of open-source tools and code libraries that run on Linux, IaC automation based on tools such as Ansible and Terraform, and so on.

These commonalities help decouple application code from infrastructure and enable “cloud-native” approaches. Importantly, these commonalities accelerate application delivery and, with infrastructure services that are commoditized, to a degree, also increase efficiency and agility and can drive down cost.

[1] A distinction can be made between “Hybrid” cloud and “Multicloud”, where Multicloud indicates use of multiple public cloud platforms, and hybrid indicates a mix of public and private cloud platforms. For simplicity, we use the term “Multicloud” to mean both.

[2] See the glossary at the end of this document for an explanation of these acronyms and terms.

[3] IDC, Cloud Pulse 1Q20 Survey, 2020

These aspects of commonality are, essentially, what enable multicloud. As different cloud platforms support these common elements and the automated deployment of applications based on them, these basic capabilities become the norm, a standard across infrastructure environments. This enables applications to be deployed, executed, and/or moved between locations or providers without disruption and with relative ease.

Even so, there are still many aspects of cloud services and their integration with the edge that are not common, nor easy. These include:

- Secure access to different cloud providers.
- Identity and Access Management (IAM), security and policy constructs, definitions, and control.
- Deployment pipelines and IaC automation across all platforms and providers.
- Application visibility, monitoring, and experience analysis.
- Cost and usage analysis and optimization across not only multiple SaaS and IaaS providers, but also on-premises and private cloud and the CoLo interconnects and connectivity providers between them.
- Integration of all this, and more, in a cloud-native operations model.

Above and beyond these considerations, there is also the need to consider the overall business readiness and ability to take advantage of these new capabilities. Furthermore, business resiliency, continuity, and compliancy must be rethought in the multicloud landscape. These are all aspects of multicloud complexity where Cisco is adding significant value with advisory and platform offerings.

Multicloud requires that an organization combine multiple cloud systems together with common operations and deployment capabilities. We offer a cloud-agnostic approach to securely and easily deploy and use applications from multiple forms of cloud–on-premises, XaaS, public, and private–in a simple, integrated, and seamless fashion.

Cisco, as a platform-neutral vendor and provider of services, can help with the complexities of continuity, insights, security, connectivity, and cloud-native operations for the best application experience in multicloud.

The economics of cloud

Cloud services are underpinned by these key concepts:

- Virtualization and containerization, which minimize the RAM/CPU/OS infrastructure required to run application code, reducing CapEx at the compute infrastructure layer.
- Automation-based on APIs, with IT tasks implemented as code-calling APIs representing the functions of a given IT service, thereby delivering efficiency, scale, reliability, and consistency and reducing OpEx in providing "infrastructure-as-code" (IaC).
- XaaS, where X is practically any IT service, including networking, that is managed and consumed via an API as an optimized service.
- Providers that focus on the optimization of services, reducing cost and improving reliability and resiliency, at scale.
- Usage-based charging models, so that consumers do not need to make fixed investments in CapEx and OpEx.

Today, there are multiple competing cloud service providers. In addition, IT service delivery and consumption is merging traditional, on-premises delivery models with the cloud. There are clear economic benefits to being able to seamlessly and securely integrate your traditional, on-premises application deployment practices with multiple cloud service providers.

A multicloud strategy is the rational approach from an economic perspective. Helping you determine how to make your strategy work in practice so you can reap the key benefits of an agile, cloud-native operations model that enhances the responsiveness of the business–that is where Cisco comes in.

Market trends

Our experience of evolving towards a digitized enterprise has foreshadowed that of many of our customers and partners. As a global technology company, we are on the forefront of many trends that we expect our customers will also have to face. The experiences of 2020/2021 have accelerated many of these changes that have been evident for some time.

In their "Worldwide Cloud 2021 Predictions,"[5] IDC predicts that, by 2023, that over half of enterprises will adopt cloud-centric operating models, and that, during 2022, over half of enterprise applications will be redeveloped to become cloud-native. At the same time, many software vendors and providers, including Cisco, will be rearchitecting their offerings or building new ones with similar goals of becoming multicloud-capable, or as IDC puts it, adopting automated "connected cloud" architectures.

The motivations that IDC identifies behind this shift to cloud-native applications are, not surprisingly, core to our multicloud vision. The primary drive comes from the need to increase the agility of delivering IT value to the business while controlling costs, with an operations model that enables the collaboration to support continuous improvement.

These motivations are also accompanied by a need to increase business resiliency, scale digital ecosystems, and enable the business to innovate and respond rapidly to new opportunities.

The trend to as-a-Service (aaS) offerings is seen across all layers. Applications will be distributed, deployed, and accessed in and from multiple locations. This is no longer the traditional model. Instead, this is a dynamic and constantly optimized mesh of microservices and/or web services with many different forms of endpoints and connectivity types. One of the many implications is that the security perimeter will also move to the cloud. Gartner calls this Secure Access Service Edge (SASE)[5]. Gartner describes SASE as a concept that:

> …combines network security functions (such as SWG, CASB, FWaaS, and ZTNA), with WAN capabilities (i.e., SD-WAN)[6] to support the dynamic secure access needs of organizations. These capabilities are delivered primarily as a service (aaS) and based upon the identity of the entity, real time context, and security/compliance policies.

We at Cisco have a strong understanding of the direction of travel of these intertwined trends. We have been, and are, making significant investments on many fronts to ensure that we can continue to deliver the best application experience in multicloud as these trends become more prominent and achieve mainstream adoption.

Five enablers of Cisco's multicloud approach

Our approach to multicloud is rooted in direct feedback from customers and partners, and is strictly aligned with those demands and needs. Our approach is also well informed by our experience as a global enterprise and SaaS provider delivering and using multicloud capabilities. On the forefront of cloud enablement and adoption for many years, we've gained a deep understanding of what works, and how to deliver that, as a consumer and provider of multicloud services and infrastructure.

The Cisco approach is based on the five enablers depicted in Figure 2. Also illustrated are some of the key use cases that we see mapping to these enablers. We shall describe these use cases, and how they are supported by our portfolio of products and services, in future white papers. The key element that ties all this together is the comprehensive Cloud Advisory Services, Multicloud Foundation Service, and Business Critical Services for Multicloud that we offer. All this, and more, can be discussed in detail with your Cisco account team.

[4] IDC, Worldwide Cloud 2021 Predictions, 2020

[5] Gartner, 2019

[6] SWG – Secure Web Gateway; CASB – Cloud Access Security Broker; FWaaS – Firewall as a service; ZTNA – Zero Trust Network Access; SDWAN – Software-Defined Wide Area Network.

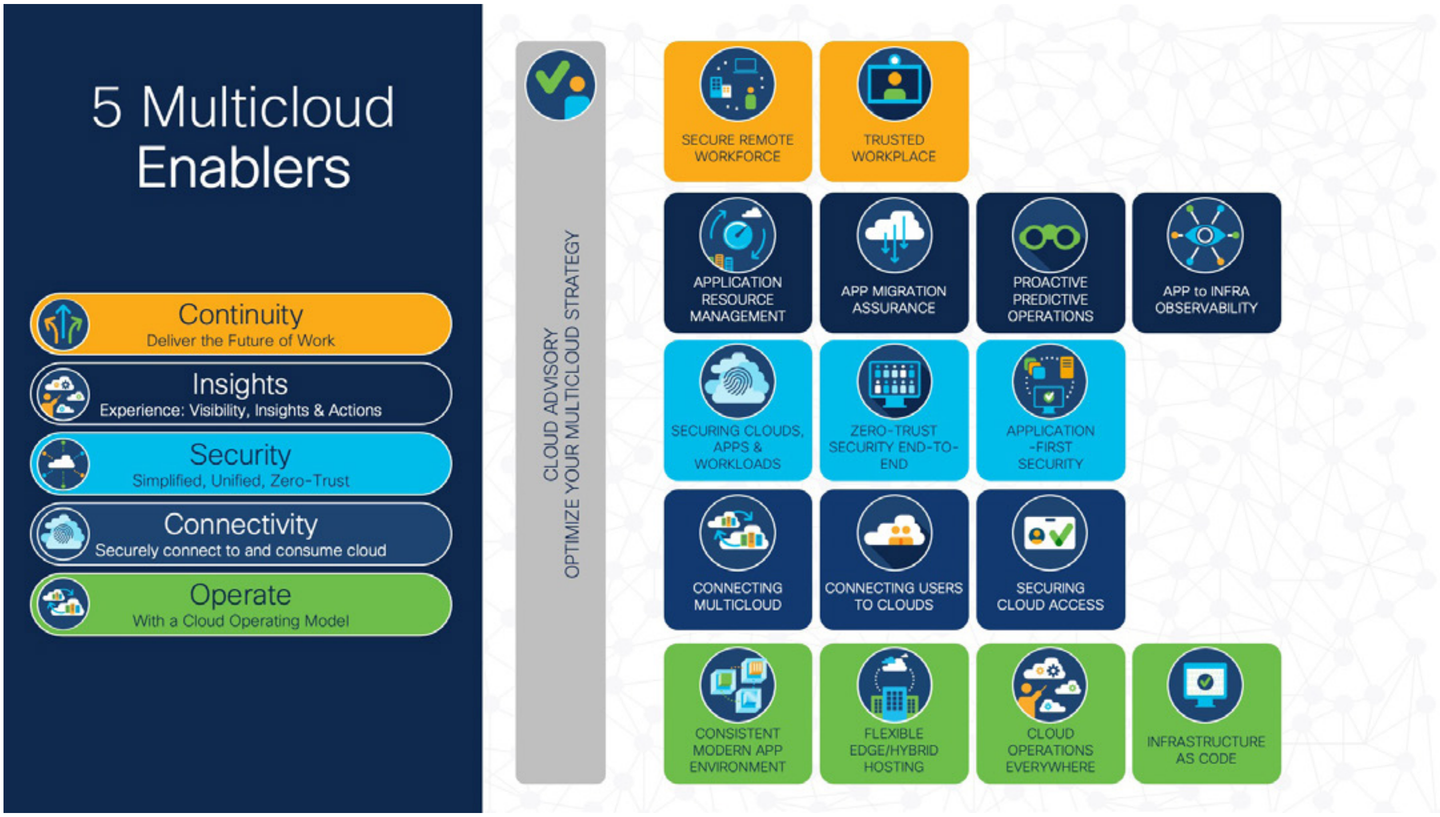
5 Multicloud Enablers
Continuity
Deliver the Future of Work
Insights
Experience: Visibility, Insights & Actions
Security
Simplified, Unified, Zero-Trust
Connectivity
Securely connect to and consume cloud
Operate
With a Cloud Operating Model
CLOUD ADVISORY
OPTIMIZE YOUR MULTICLOUD STRATEGY
SECURE REMOTE WORKFORCE
TRUSTED WORKPLACE
APPLICATION RESOURCE MANAGEMENT
APP MIGRATION ASSURANCE
PROACTIVE PREDICTIVE OPERATIONS
APP to INFRA OBSERVABILITY
SECURING CLOUDS, APPS & WORKLOADS
ZERO-TRUST SECURITY END-TO-END
APPLICATION -FIRST SECURITY
CONNECTING MULTICLOUD
CONNECTING USERS TO CLOUDS
SECURING CLOUD ACCESS
CONSISTENT MODERN APP ENVIRONMENT
FLEXIBLE EDGE/HYBRID HOSTING
CLOUD OPERATIONS EVERYWHERE
INFRASTRUCTURE AS CODE

Figure 2.
The Five Enablers of the Cisco Multicloud Framework

The context for the Cisco enablers for multicloud is rooted in an application experience-centric approach. Like our customers, Cisco operates through a rich ecosystem of applications and services we consistently and securely deliver to our workforce, partners, and customers, regardless of location.

This is all about supporting the agile delivery of the applications on which an enterprise depends, with a consistent, secure, and unified operations model across the whole of the technology infrastructure stack. The way in which we think about that is explained below.

Continuity – Deliver the future of work

We deliver the services and capabilities to empower a distributed workforce with seamless and secure collaboration supported by flexible and secure access to applications. We thus underpin the business resiliency and continuity required for the future of work.

The connected experience that we enable for the global workforce delivers a safe and trusted workplace for all staff, regardless of location, from home to cafe, park bench, or office desk. We offer technology in the workplace for safe social distancing, comprehensive tools for distributed teams, and simple and consistent access to applications for all the people working for your enterprise, thus ensuring business continuity and resiliency.

Visibility, insights, and action across multicloud – Deliver a seamless application experience

Cisco’s modern, cloud-native, application platform supports visibility from the application all the way down and through multiple infrastructure environments, revealing actionable insights with AI-powered analytics. Closed-loop automation proactively identifies and resolves issues to avoid service outages and help ensure that SLAs and business objectives are met. With extensible platforms and open APIs, we support a wide ecosystem of Cisco and third-party systems and tools.

Developers and users benefit from our fully observable, cloud-native, application-centric stack, which supports innovative multicloud application delivery, faster and more efficiently than any other.

Security and compliance – Simplified, unified, multi-layered, zero-trust, threat intel

The Cisco integrated and open platform for zero-trust security and breach defense, combined with the unrivaled breadth and depth of our security portfolio, unifies visibility and operations for greater simplicity and efficiency in multicloud.

Our security platform enables seamless governance and control across user and customer endpoints, network, cloud, and application environments, with embedded real-time threat intelligence enabling efficient security operations for incident management and risk avoidance.

Connectivity – Modernize and automate across domains

Multicloud application delivery necessitates networking architectures focused on securely connecting users to applications, regardless of location and access type, with fully integrated performance and experience telemetry to provide actionable feedback. Such visibility across public and private networks ensures that issues are quickly and easily identified and resolved and SLAs are fully measurable and met.

Full automation and visibility of all aspects of connectivity management is provided by SDN solutions that integrate natively with CoLo partners and cloud provider networks. These SDN solutions enable secure connectivity and optimized performance between users located anywhere (office, home, cafes, or traveling) and applications located in private data centers, public clouds, SaaS, or on the edge. The flexibility enabled by such end-to-end connectivity solutions is key to the seamless and secure delivery of multicloud capabilities to any location required by today's modern, distributed organization.

The Cisco capabilities for connectivity simplify and secure distributed users, applications, and heterogeneous cloud and on-premises resources, thereby improving issue management, SLAs, and operational efficiency with multiple levels of consumption flexibility.

Operations – Accelerate with a consistent, integrated cloud operating model

With the combination of our cloud-delivered management and optimization solutions and a comprehensive suite of service offerings, we support the operational intelligence, consistency, and automation required to securely deliver legacy, cloud-native, and edge-native applications in all forms of multicloud.

We are doing this today with many examples of infrastructure-as-code (IaC) integration across our portfolio. Our IaC focus is supported by SaaS-delivered models for end-to-end automation and insights. We continue to expand these capabilities with services offers supporting these approaches throughout the lifecycle of application delivery and operations.

Our experience as a global SaaS provider and consumer has given us a deep understanding of how to deliver rightsized services for a wide variety of consumption needs. Alongside that is a deep appreciation for operational efficiency and the corresponding usage and cost optimization such efficiency can bring.

With a range of solutions for all permutations of hybrid, on-premises, edge, and cloud-based deployments, along with partnerships with a variety of cloud and CoLo providers, we help enterprises establish a simplified, cost-efficient, and unified cloud operating model that integrates and enhances collaboration across development, operations, and security teams.

With the Cisco cloud operating model, you can deploy anywhere and manage heterogeneous environments and applications with optimized and secure consumption of services, regardless of location.

Summary

The application experience in a multicloud world is central to our vision. Our goal is to remove the complexity in delivering an optimal, consistent, and secure user and application experience across all multicloud domains, private and public.

We do this with full-stack observability, actionable insights, and native and fully automated integration with cloud stacks, regardless of type and location, based on an open, modular, and extensible cross-platform multicloud architecture, with security embedded in the core of our technology.

We continue with our goal of building an open and extensible platform that supports the creation of value-add services and capabilities. The extensibility of our platform underpins the vital role of the Cisco partner ecosystem in further enriching the cloud experience for all.

To learn more, see:

- Watch this video from Liz Centoni, VP of Strategy, Emerging Technologies & Incubation, on how Cisco is "Helping our Customers Harness the Power of the Cloud."
- Visit CX Services for Cloud to learn how Cisco CX Cloud Advisory Services, Multicloud Foundation Service, and Business Critical Services for Multicloud provide expertise and support for your multicloud journey.

Glossary

This glossary addresses some terms used in this document, for the purposes of aiding understanding. This is not a complete treatment of all multicloud terminology. Some Cisco product links are supplied here also, where considered useful for the purposes of clarity, but this is by no means intended to be a complete treatment of all applicable Cisco products.

aaS/XaaS (IT capability provided as a Service)	Some IT capability, X, provided as a service (XaaS). Some benefits are: ▪ The provider manages the design, implementation, deployment, upgrades, resiliency, scalability, and overall delivery of the service and the infrastructure that supports it. ▪ There are very low barriers to entry, so that services can be quickly adopted and dropped in response to business demand, without the penalty of inefficiently utilized CapEx. ▪ The service charge is an IT OpEx cost (pay-as-you-go), whereas the CapEx and the service infrastructure is the responsibility of the provider. ▪ Costs are commensurate to usage and hence more easily controlled with respect to business demand and outcomes. Such services are typically implemented as "microservices," which are accessed via REST APIs. This architectural style supports composition of service components into systems. Access to and management of aaS assets is via a web GUI and/or APIs, such that Infrastructure-as-code (IaC) techniques can be used for automation, e.g., Ansible and Terraform. The provider can be any entity capable of implementing an aaS "cloud-native" architecture. The cloud-native architecture concept is well-documented and supported by open-source software and a rich ecosystem of services such as training and consultancy. The provider can be an internal IT department or any of many third-party companies using and supporting the same open-source platforms.

	Service access control, integrated with corporate IAM, can be mapped to specific users and business activities, enabling consistent policy controls across services, wherever they are delivered from.
Ansible	An infrastructure automation tool, used to implement processes for instantiating and configuring IT service components, such as VMs on an IaaS platform. Supports the consistent execution of processes defined in YAML "playbooks" at scale, across multiple targets. Because the Ansible artefacts (playbooks) are text-based, they can be stored in a source code management (SCM) system, such as GitHub. This allows for software development like processes to be applied to infrastructure automation, i.e., Infrastructure-as-code (see IaC below). https://www.ansible.com
AWS (Amazon Web Services)	Provider of IaaS and PaaS. https://aws.amazon.com
Azure	Microsoft IaaS and PaaS. https://azure.microsoft.com/en-gb/
Co-located data center	"A colocation center (CoLo)...is a type of data center where equipment, space, and bandwidth are available for rental to retail customers. Colocation facilities provide space, power, cooling, and physical security for the server, storage, and networking equipment of other firms and also connect them to a variety of telecommunications and network service providers with a minimum of cost and complexity." https://en.wikipedia.org/wiki/Colocation_centre
Containers (Docker)	A (Docker) container is a means to create a package of code for an application and its dependencies, such that the application can run on different platforms which support the Docker environment. In the context of aaS, microservices are typically packaged within Linux containers orchestrated by Kubernetes (K8s). https://www.docker.com https://www.cisco.com/c/en/us/products/cloud-systems-management/container-platform/index.html

DevOps	The underlying principle of DevOps is that the application development and operations teams should work closely together, ideally within the context of a toolchain that automates the stages of development, test, deployment, monitoring, and issue handling. DevOps is closely aligned with IaC, continuous integration and deployment (CI/CD), and Agile software development practices. https://en.wikipedia.org/wiki/DevOps https://en.wikipedia.org/wiki/CI/CD
Edge compute	Edge compute is the idea that it can be more efficient to process data at the edge of a network, close to the endpoints that originate that data, or to provide virtualized access services, such as at the network edge. This could be for reasons related to low latency response, reduction of the amount of unprocessed data being transported, efficiency of resource utilization, and so on. The generic label for this is multi-access edge computing (MEC), or Mobile Edge Computing for mobile networks specifically. From an application experience perspective, it is important to be able to utilize, at the edge, the same operations model, processes, and tools used for any other compute node in the system. https://en.wikipedia.org/wiki/Mobile_edge_computing
IaaS (Infrastructure-as-a-Service)	Infrastructure components provided aaS, located in data centers operated by a provider, typically accessed over the public Internet. IaaS provides a base platform for the deployment of workloads, typically with containers and Kubernetes (K8s).
IaC (Infrastructure-as-Code)	Given the ability to automate aaS via APIs, the implementation of the automation is typically via Python code, Ansible playbooks, and similar. These automation artefacts are programming code that define how the services are consumed. As such, they can be subject to the same code management and software development regimes as any other body of code. This means that infrastructure automation can be subject to all of the quality and consistency benefits, CI/CD, traceability, automated testing, compliance checking, and so on, that could be applied to any coding project. https://en.wikipedia.org/wiki/Infrastructure_as_code
IAM (Identity and Access Management)	IAM is the means to control access to IT resources so that only those explicitly authorized to access given resources can do so. IAM is an essential foundation to a secure multicloud environment. https://en.wikipedia.org/wiki/Identity_management

IBM (Cloud)	IBM IaaS and PaaS. https://www.ibm.com/cloud
Intersight	Cisco Intersight™ is a software-as-a-service (SaaS) infrastructure lifecycle management platform that delivers simplified configuration, deployment, maintenance, and support. https://www.cisco.com/c/en/us/products/servers-unified-computing/intersight/index.html
GCP (Google Cloud Platform)	Google IaaS and PaaS. https://cloud.google.com/gcp
Kubernetes (K8s)	Kubernetes is an open-source system for automating deployment, scaling, and management of containerized applications. https://kubernetes.io
Microservices	A microservices architecture is characterized by processes implementing fine-grained services, typically exposed via REST APIs and which can be composed into systems. The processes are often container-based, and the instantiation of the services often managed with Kubernetes. Microservices managed in this way are intrinsically well suited for deployment into IaaS environments, and as such, are the basis of a cloud-native architecture. https://en.wikipedia.org/wiki/Microservices
PaaS (Platform-as-a-Service)	PaaS is a layer of value-add services, typically for application development, deployment, monitoring, and general lifecycle management. The use of IaC with IaaS and PaaS is very closely associated with DevOps practices.
Private on-premises data center	A data center infrastructure housed within an environment owned by a given enterprise is distinguished from other forms of data center, with the implication that the private data center is more secure, given that access is restricted to those authorized by the enterprise. Thus, circumstances can arise where very sensitive IT assets are only deployed in a private data center, in contrast to using public IaaS. For many intents and

	purposes, the underlying technology can be identical, allowing for hybrid deployments where some IT assets are privately deployed but also accessible to other assets in public IaaS. IAM, VPNs, firewalls, and similar are key technologies needed to underpin the security of such an arrangement.
REST API	Representational state transfer (REST) APIs is a generic term for APIs accessed over HTTP(S), typically transporting data encoded in JSON or XML. REST APIs have the advantage that they support distributed systems, communicating over HTTP, which is a well-understood protocol from a security management perspective. REST APIs are another element of a cloud-native applications architecture, alongside microservices. https://en.wikipedia.org/wiki/Representational_state_transfer
SaaS (Software-as-a-Service)	End-user applications provided "aaS" over the public Internet, with the underlying software systems and infrastructure owned and managed by the provider.
SAML (Security Assertion Markup Language)	Used in the context of Single-Sign-On (SSO) for exchanging authentication and authorization data between an identity provider, typically an IAM system, and a service provider (some form of SaaS). The SAML protocol exchanges XML documents that contain security assertions used by the aaS for access control decisions. https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language
Terraform	An open-source IaC software tool for cloud services, based on declarative configuration files. https://www.terraform.io

Authors

Nathan Sowatskey, Principal Engineer, Cisco Customer Experience

Ashley Novak, Principal Engineer, Cisco Customer Experience

Dave Zacks, Director, Cisco Customer Experience

Carlos Pereira, Chief Architect, Cisco Strategy, Emerging Technologies and Incubation