The enterprise cloud market: A competitive overview

June 7, 2015
A Principled Technologies research report commissioned by Cisco Systems, Inc.

Principled Technologies®

TABLE OF CONTENTS

This Principled Technologies research report, commissioned by Cisco Systems, Inc., reflects publicly available information and lists all sources in footnote citations.

EXECUTIVE SUMMARY

As enterprises continue to adopt cloud technology, the portfolios of cloud service providers are growing to meet demands. In a survey from November 2014, IDG reported 69 percent of all respondents have at least one application or portion of infrastructure in the cloud, with more planning on utilizing the cloud in the future.[1] These businesses have reached a critical point: They understand how to make the cloud work for them and see the value of cloud computing. However, they face problems from balancing IT agility with security—as having strength in either area has traditionally meant giving it up in the other—and from integrating their existing IT infrastructures into new private and public cloud deployments.

In addition, the convergence of data from external sources—including public clouds, market data, social networks, and mobile devices—increases the volume of data a business must understand. The focus on centralized data stores as a single source of enterprise truth (data at rest) is shifting now to a focus on data processing and analysis at the edge (data in motion). The former was useful from an operational perspective, but the latter is becoming critical for real-time analysis of growing volumes of data at the point of capture on edge devices (e.g. mobile devices).

Getting more business value in the current competitive environment requires a different approach to business architecture. Existing cloud technology providers seek to improve business architecture by using their technology and business approaches to analyze and secure data in the context of data convergence. These approaches aim to allow cloud infrastructure to be pervasive regardless of location, device types, applications, and workloads.

There is no uniform answer when choosing the right cloud environment for a business—what works for one may not work for another. Cloud service providers, with varying levels of cloud market share, combine different approaches into unique cloud offerings.

Starting at the beginning, the base architectural approaches for building a cloud differ. Some are *device-centric* (sometimes referred to as *infrastructure-centric*), focusing on intelligent devices and how those devices access and use the cloud. Some are *network-centric*, focusing on network fabric intelligence. Finally, others are *application-centric*, focusing on cloud infrastructure intelligence and designed to provide fast and responsive IT solutions by making it easier to write, update, and deploy applications on cloud infrastructure.

[1] www.idgenterprise.com/report/idg-enterprise-cloud-computing-study-2014

In addition, cloud solutions can be vendor agnostic, vendor specific, or proprietary. The number of compatible technologies, platforms, and vendors for any given cloud solution dictates the level of flexibility and cloud customization that organizations using that solution can have.

Security remains a top priority for every part of the infrastructure, and to a lesser extent, so does networking, cloud management, and workload mobility. For cloud service providers, complete end-to-end cloud security involves securing the datacenter, the network, and remote devices, including mobile devices and other edge devices for the Internet of Things (IoT). *Datacenter security* can range from physical datacenter access and installation security, to data security of stored information, to datacenter access control and monitoring. Cloud providers implement *network security* with an intelligent network fabric that restricts data flow through the network based on defined security and application policies. Such policy-defined restrictions can make it easier to implement automation and secure data in motion between clouds, from cloud to on-premises IT, or from cloud to end devices. Cloud service providers may approach network security either via add-on solutions or as integrated, preventative measures. Finally, cloud service providers can implement *remote device security* inside the device, by the network – securing the device's access to a cloud – or by a combination of both. Some cloud service providers offer a combination of these approaches, designed to achieve stronger end-to-end security.

At the same time, as traditional IT and on-premises, hosted private, and public clouds become increasingly interconnected, it is critical to consider the manageability of a hybrid IT infrastructure and the ease with which compute resources, workloads, and applications move freely on that infrastructure. Different cloud service providers have different ways of accomplishing this, with varying scope and success.

Within this context, we have chosen to review Amazon Web Services (AWS), the Cisco cloud portfolio, and VMware cloud offerings focusing on vCloud Air. All three cloud portfolios include a large array of cloud-based services that span consulting, support, applications, storage, compute, and many more features discussed in this paper. Figure 1 provides a general overview of the key differences between AWS, Cisco cloud offerings, and VMware vCloud Air based on publicly available material.

Competitive profile

Overall cloud approach		
Amazon Web Services	Cisco	VMware vCloud Air
Infrastructure-centric, software-based public cloud service provider	Application-centric view of workload deployment, combining policy-based network intelligence and resource management with a network-centric hybrid cloud architecture	Infrastructure-centric hybrid cloud implementation with a vendor-locked (VMware-based) approach to software-defined infrastructure and management tools
Broad spectrum of services based on proprietary cloud infrastructure	Partner-centric, allowing a choice of cloud providers and platforms to create multivendor cloud solutions	Deployments are oriented to clients that are already completely VMware-based or willing to use only VMware technologies
Doesn't disclose the hardware that powers its public cloud solution or provide any hardware integration tools to the user	Open-cloud solutions that can use existing hardware, software, and other infrastructure or Cisco infrastructure if desired	Offers cloud solutions that can use existing hardware, software, and other infrastructure, as long as the cloud infrastructure is all VMware
Data security focused and compliant with many security certifications; no clear approach to network or device security	Policy-based, end-to-end data and network security	End-to-end hybrid cloud security similar to Cisco but covering only VMware products, such as vCloud Air; like AWS, compliant with many security certifications
VM management via dashboard or automation software, e.g. for analytics, with no automation for workload mobility into and out of AWS	Unified management of hybrid cloud solutions and application provisioning with complete workload mobility across component clouds	VM mobility across VMware clouds
Amazon's partner network consulting services provide pre-sales and implementation support for AWS-based public cloud solutions	Cisco's Intercloud Providers and Cisco Powered partner programs have hundreds of partners, Cisco-powered datacenters, and cloud service providers, in addition to cloud service provider infrastructure, cloud consulting and professional services, and flexible availability zones	Very large partner network providing cloud service provider infrastructure, cloud consulting and professional services, and flexible availability zones

Figure 1: An overview of key differences between AWS, Cisco, and VMware cloud offerings.

APPROACH TO PROVIDING CLOUD SOLUTIONS

Business needs and emerging technologies, such as the Internet of Things, are directing the development of cloud-based offerings. Cloud service providers and developers must respond to business needs to stay relevant, especially as the cloud market begins to shift toward more hybrid-centric and application-centric patterns. Based on the need for security, ease of use, and integration, cloud providers and vendors aim to develop software and hardware solutions that provide these services in the best ways possible. Below are high-level descriptions of the approach each vendor uses to market, develop, and provide their cloud products.

The AWS approach

Founded in 2006, AWS provides public cloud solutions ranging from entry-level small clouds to larger enterprise clouds, which aim to minimize capital expenditures, improve scalability, and respond quicker to changing business needs.[2] By providing a cost calculator, AWS allows all users to estimate initial cost before they sign up for services.[3]

Amazon provides only public cloud solutions. However, they do provide tools to help integrate such solutions into customers' on-premises solutions, e.g. a VMware vCenter AWS plugin.[4] Amazon does not disclose the hardware on which AWS provides services, and it offers only virtual infrastructure for its public cloud offerings.

For security, AWS offers a hardware-based, on-premises cryptography solution built by AWS partners. It also offers secure, VPN-like connections for customers to manage and secure data transfers to and from AWS. This feature requires payment and doesn't provide endpoint security for hybrid cloud deployments.[5]

Other key features:[6]

- Migrating VMs and workloads to AWS requires users to export and import VMs in certain formats
- Limited migration functionality into and out of AWS with no documented automation
- No Software-as-a-Service (SaaS) or Application-as-a-Service (AaaS) solutions, but the Amazon marketplace provides a location where third-party vendors can sell software validated by Amazon to run on AWS
- Users must pay for all AWS components to use the service

The Cisco approach

To provide cloud services, Cisco uses a partner-centric model: the Intercloud, a globally connected network of clouds built by Cisco and its partners. With a heavy focus on Cisco Application Centric Infrastructure (ACI), Cisco intends to meet many needs in cloud IT today, as cloud services evolve from Infrastructure-as-a-Service (IaaS) to SaaS and beyond it to Anything-as-a-Service (AaaS).

Cisco ACI encompasses a software-defined network solution and policies that manage workloads, networks, storage, servers, security, and other parts of infrastructure. ACI makes the application the focus of the infrastructure by decoupling application needs from network resources. The ACI ecosystem is built on a fabric

[2] aws.amazon.com/products/?nc2=h_ql_ent_atl
[3] calculator.s3.amazonaws.com/index.html
[4] aws.amazon.com/ec2/vcenter-portal/
[5] aws.amazon.com/vpc/
[6] aws.amazon.com/marketplace

component (either a Cisco Nexus 9000 series switch or a Cisco Application Virtual Switch) and the Cisco Application Policy Infrastructure Controller (APIC). Workloads and services that utilize ACI are built on open APIs. Cisco also curates the Cisco Developer Network for ACI, which provides documentation and other resources required for development of services that use the ACI fabric.[7]

Cisco, widely known for high-end networking and switching components, manufactures many cloud-ready hardware solutions. The Cisco Unified Computing System (UCS) portfolio includes the following cloud-ready hardware:[8]

- Rack servers, modular servers, blade servers, and chassis
- Fabric interconnects and expanders
- Server adapters, such as GPUs
- Flash storage
- Cisco-branded I/O, racks, and power components

Software components, such as Cisco UCS Director and Cisco UCS Manager, manage UCS hardware components. Cisco UCS management software suites include many cloud-oriented tools.

Cisco Nexus switches also include cloud-ready features. For example, the Nexus 9000 series switches can operate in the standard NX-OS network operating system mode or operate in ACI mode for full ACI compatibility,[9] allowing applications to request infrastructure components regardless of their location. As part of the Cisco networking portfolio, Cisco also provides software-defined networking functionality through ACI.[10]

Cisco aims to provide end-to-end security for the cloud and supports their security focus with many of their current technologies. Along with other Cisco security solutions, Cisco uses ACI to provide network and application-level security when deployed in an environment.[11] With Cisco Cloud Web Security (CWS), Cisco provides security in a SaaS model that protects users wherever they are.[12] (For a list of supported devices, see the Cisco Cloud Security section.) By using Cisco Identity Services Engine (ISE), administrators can utilize networking and network access policies to facilitate security, including in bring-your-own-device (BYOD) situations, where corporate users connect their personal mobile devices to the enterprise network.

[7] www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html

[8] www.cisco.com/c/en/us/products/servers-unified-computing/product-listing.html

[9] www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html

[10] www.cisco.com/web/solutions/trends/sdn/index.html

[11] www.cisco.com/c/en/us/solutions/enterprise-networks/application-centric-infrastructure-security/index.html

[12] www.cisco.com/c/en/us/products/security/cloud-web-security/index.html

The VMware vCloud approach

VMware continues to be the largest developer of hypervisors in the market.[13] By focusing mainly on software-defined networking, compute, and storage, VMware's products are largely hardware agnostic. The VMware portfolio includes products that span network virtualization, security, management, and cloud services. In addition, VMware has begun working with hardware vendors to create prepackaged solutions for on-premises private clouds.

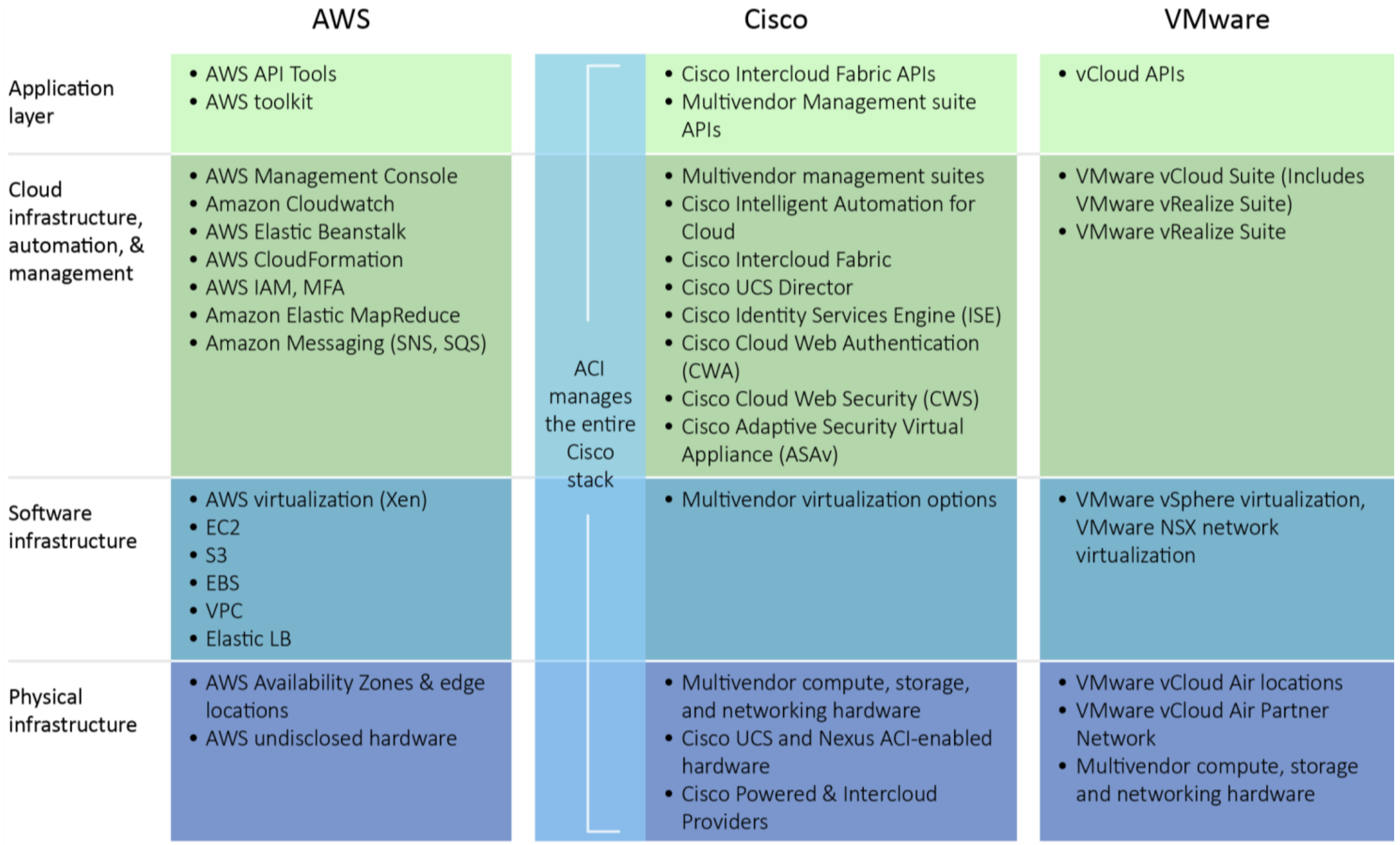
VMware's public cloud offering is called vCloud Air, implemented on VMware proprietary software-based hybrid cloud technologies. For the hybrid cloud, VMware has designed vRealize, a cloud management platform.[14] VMware technology is also used throughout cloud solutions e.g. for hypervisors and cloud automation tools) to implement private and public cloud infrastructure. In the datacenter, VMware offers their hypervisor solution, VMware vSphere, to cover virtualization needs. To manage the hypervisors and virtual machines, VMware provides vCenter Server, which includes a single dashboard for all machines running VMware solutions. VMware offers VMware vCloud Suite to create a private cloud on-premises. The vCloud Suite provides cloud-focused services such as disaster recovery, usage metering, cloud automation, and performance/operational management.

Based on VMware hypervisors, vCloud Air and other VMware products use the same support model through a single point of contact. Thanks to compatibility, customers can easily integrate vCloud Air and vCloud Suite to create a VMware-only hybrid cloud solution managed from a single location.[15] VMware leverages their installed base of vSphere hypervisors to create hybrid cloud environments, as vCloud Air can integrate with vSphere installs, with the addition of only vCloud Suite.[16] VMware products can also support integration with other public cloud providers, such as Microsoft Azure and Amazon Web Services.[17]

VMware claims that EVO:RAIL, announced in 2014, provides a hyper-converged VMware software and hardware appliance, which is available through EVO OEM partners and is intended to be simple to configure, set up, and integrate into a production environment. Starting with configurations as small as four nodes in a 2U footprint, EVO:RAIL is marketed as a software-defined datacenter solution.[18]

[13] www.enterprisetech.com/2014/07/08/vmware-microsoft-rule-x86-server-virtualization/
[14] www.vmware.com/products/vrealize-suite
[15] vcloud.vmware.com/uk/explore-vcloud-air/what-is-vcloud-air
[16] www.vmware.com/files/pdf/products/vCloud/VMware-vCloud-Suite-Datasheet.pdf
[17] www.vmware.com/files/pdf/products/vCloud/VMware-vCloud-Suite-Datasheet.pdf
[18] blogs.vmware.com/tribalknowledge/2014/08/vmworld-2014-vmware-evorail-building-block-software-defined-data-center.html

Working with vCloud Suite, but offered as an add-on, VMware NSX provides network virtualization components intended to simplify datacenter functions while also providing security in the hybrid cloud model.[19] By using NSX to logically separate networks and other components, users can utilize NSX capabilities to create their own secure solutions.



	AWS		Cisco	VMware
Application layer	• AWS API Tools • AWS toolkit	ACI manages the entire Cisco stack	• Cisco Intercloud Fabric APIs • Multivendor Management suite APIs	• vCloud APIs
Cloud infrastructure, automation, & management	• AWS Management Console • Amazon Cloudwatch • AWS Elastic Beanstalk • AWS CloudFormation • AWS IAM, MFA • Amazon Elastic MapReduce • Amazon Messaging (SNS, SQS)		• Multivendor management suites • Cisco Intelligent Automation for Cloud • Cisco Intercloud Fabric • Cisco UCS Director • Cisco Identity Services Engine (ISE) • Cisco Cloud Web Authentication (CWA) • Cisco Cloud Web Security (CWS) • Cisco Adaptive Security Virtual Appliance (ASAv)	• VMware vCloud Suite (Includes VMware vRealize Suite) • VMware vRealize Suite
Software infrastructure	• AWS virtualization (Xen) • EC2 • S3 • EBS • VPC • Elastic LB		• Multivendor virtualization options	• VMware vSphere virtualization, VMware NSX network virtualization
Physical infrastructure	• AWS Availability Zones & edge locations • AWS undisclosed hardware		• Multivendor compute, storage, and networking hardware • Cisco UCS and Nexus ACI-enabled hardware • Cisco Powered & Intercloud Providers	• VMware vCloud Air locations • VMware vCloud Air Partner Network • Multivendor compute, storage and networking hardware

Figure 2: A sample diagram of components for AWS, Cisco, and VMware cloud offerings.

COMPETITIVE CLOUD FEATURES

Each of the three competitors we reviewed has its own approach to implementing key features. In general, the features of each cloud offering we present are determined by the approach that each cloud service provider takes. For example, let's consider security, a key aspect of cloud implementations. AWS has a software-centric approach to cloud, and due to the nature of their offering, their main concern is data residing in the public cloud. Implementing security for AWS then means implementing security for stored data, i.e. for data at rest. Securing a cloud connection

[19] www.vmware.com/products/nsx

from on-premises IT to AWS requires users to implement security and can come at an additional cost.

Cisco’s view of cloud is network-centric. For Cisco, intelligence in the network is key, and security is implemented at the network level. This allows the network to monitor and control data flow, ensuring compliance with access control and defined security policies.

Finally, VMware’s approach is VMware-centric. Their take on cloud security is to provide security capabilities for virtualized compute environments built on vCloud Suite technologies, a step beyond device-based security but still not spanning the network as a whole.

In the following sections, we describe and analyze features that are important for a cloud offering and examine the approach that each provider takes. Please see Appendix A for a side-by-side, detailed feature comparison.

Cloud security

Cloud users would not store data in any cloud if they did not believe their data and applications would be secure. Meeting that expectation keeps cloud service providers in business. For some, this means maintaining the security of data stored in public clouds; for others, it means ensuring security at any connectivity endpoint and security of data, whether it is at rest or in motion.

AWS

AWS focuses on public cloud datacenter security, but does not address network security. Its security strategy appears to be to secure the cloud datacenter and provide secure pipes from AWS to client on-premises deployments, but not to provide network or endpoint security (as one would need for IoT deployments). AWS provides many data security certifications and is compliant with many global security standards, such as ISO 27001.[20] These include government security authorizations such as DIACAP, which allows AWS to work for the US Department of Defense.[21] AWS provides VPN and network security options for an additional cost to VM hosting.[22] Some AWS security features include: [23]

- Access lists
- Firewall rules
- Private subnets
- Multi-factor authentication

[20] aws.amazon.com/compliance/
[21] aws.amazon.com/security/
[22] calculator.s3.amazonaws.com/index.html
[23] aws.amazon.com/security/aws-security-features/

However, as AWS provides only public cloud services, their security products don't cover anything within the on-premises datacenter – except for products such as AWS CloudHSM,[24] a hardware-based cryptography solution installed on-premises that provides a secure connector to the AWS public cloud at added cost.

Cisco

Cisco provides policy-based cloud security and end-to-end cloud security, meaning datacenter, network, and edge device security.[25] Due to this approach, the security of Cisco cloud deployments can extend to IoT endpoint devices without available embedded device security. Cisco's approach allows users to choose an appropriate balance point between security and agility as needed for different workloads and use cases.

Cisco has three key components intended to help provide and manage end-to-end cloud security: Cisco Identity Services Engine (ISE), Cisco Cloud Web Security (CWS), and Cisco Application Centric Infrastructure (ACI). Cisco ISE, installed as either Cisco bare-metal instances or as a virtual appliance,[26] has components tailored and optimized for cloud, including support for VPNs or other networking access and support for BYOD models.[27] ISE provides identification of each user or device, handles provisioning, and offers a centralized view of policies and devices. According to Cisco, leveraging Cisco ISE can offer security and agility, as IT staff can gain detailed control, logged access to network resources, and policy-based automation of many security tasks.

Cisco Cloud Web Security focuses on delivering cloud Security-as-a-Software-Service (SaaS).[28] According to Cisco, CWS solutions are protected by features like physical security, logical separation, and Cisco firewall solutions (physical or virtual).[29] Cisco CWS includes connectors and clients that target mobile devices as well as cloud datacenter solutions. Cisco intends for businesses to control Web access across a broad range of devices while preventing malware.

Leveraging Application Centric Infrastructure in the cloud can also provide many security benefits that tie hardware, software, cloud management, and workloads together for top-to-bottom security.[30, 31] The Cisco ACI architecture can be fully

[24] aws.amazon.com/cloudhsm/

[25] www.cisco.com/c/en/us/solutions/enterprise-networks/cloud-web-security-connected/index.html

[26] www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/data_sheet_c78-656174.html

[27] www.cisco.com/c/en/us/products/security/identity-services-engine/index.html

[28] www.cisco.com/c/en/us/products/security/cloud-web-security/index.html

[29] www.cisco.com/c/dam/en/us/products/collateral/security/cloud-web-security/data-privacy-final-source.pdf

[30] www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html

[31] www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-732354.html

integrated with the Cisco Adaptive Security Virtual Appliance (ASAv), designed to create agility by providing enterprises with consistent security across physical, virtual, and software-defined layers. Cisco ASAv runs as a virtual machine, allowing for high availability and flexible provisioning.[32] Use of Cisco ASAv provides essential security services that protect data as it passes between nodes within cloud environments.

VMware

VMware includes security for the hybrid cloud similar to Cisco. Unlike Cisco, however, its security products cover only VMware products such as vCloud Air and vCloud Suite.[33] VMware vCloud Air includes a host of global security certifications, although not as many as AWS.[34] Like AWS, vCloud Air also has government certifications and contracts.[35] vCloud Air datacenters can provide extensive datacenter security and secure connections to other clouds and on-premises IT using vCloud Connector.[36, 37] VMware concentrates on virtual network and data security.[38]

Seamless networking

The core of cloud technology is connectivity, so network availability and accessibility are vital. For cloud service providers such as Cisco or VMware, this means having multiple options in hardware and software for catering to public, private, and hybrid clouds, both on- and off-premises.

AWS

AWS provides several options for connecting networks to its public cloud infrastructure. Among them, AWS Direct Connect provides users with private connections to their AWS storage and compute services.[39] In addition, Amazon offers a service called Amazon VPC (Virtual Private Cloud) that allows businesses to create private network spaces in AWS that work similarly to how on-site datacenters might function. Users must configure these features to create a seamless network topology.[40] This approach cannot be scaled up easily to hybrid clouds or to dense networks, like those that may be dominant with IoT.

[32] www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/datasheet-c78-733399.html
[33] www.vmware.com/cloud-computing/hybrid-cloud
[34] vcloud.vmware.com/service-offering/cloud-compliance
[35] vcloud.vmware.com/service-offering/security-overview
[36] www.vmware.com/cloud-services/infrastructure/vcloud-air-dedicated-cloud/specs.html
[37] pubs.vmware.com/vca/index.jsp#com.vmware.vcc.vca.doc/GUID-2645E1B6-031C-4791-92EF-9F790DDCB059.html
[38] www.vmware.com/files/pdf/products/vcns/vmware-vcloud-networking-and-security-overview.pdf
[39] aws.amazon.com/directconnect/
[40] aws.amazon.com/vpc/

Cisco

Cisco’s hybrid cloud strategy includes a number of solutions designed to create a seamless network for the hybrid cloud. At the heart of this approach is Intercloud Fabric (ICF). Installed as a suite of virtual appliances, ICF includes many networking features, including extending Layer 2 networking functionality from private to public clouds.[41] Cisco ICF also includes switching, routing, NAT, and firewall capabilities intended to extend security and networking to the hybrid cloud.

Cisco Cloud Connectors can work in conjunction with Cisco ICF to allow businesses to use cloud applications designed for a low-latency LAN environment across a higher-latency WAN environment, as you might find in public or off-site private clouds. The goal of utilizing a Cloud Connector in a virtualized environment is to provide secure cloud connectivity and networking to any location, datacenter, or public cloud. Cisco Cloud Connectors have important features such as Quality of Service (QoS), application-aware networking, and location-aware features.

Cisco also provides other tools for creating cloud-ready networks, including software-defined networking options such as the Cisco Nexus 1000V series switches for Hyper-V and vSphere.[42] ACI, which can help create a software-defined network solution, supports the use of the Nexus 9000 series switches in ACI-mode.[43] Cisco ACI fabrics are compatible with existing virtual switches (Cisco Nexus 1000v series) by use of the Cisco Application Virtual Switch (AVS). Cisco AVS extends the ACI control into the virtualization layer.[44]

Cisco’s approach enables seamless networking through a hybrid-IT deployment, spanning legacy IT, on-premises clouds, hosted private clouds, and public clouds.

VMware

VMware can provide seamless networking between vCloud Air and the on-premises datacenter by using network virtualization.[45] VMware makes this possible by leveraging technologies in VMware NSX and brands it as VMware vCloud Air Advanced Networking Services. VMware NSX offers virtual switch functionality by abstracting the network using a virtual controller. To support seamless connections to physical workloads (running on bare metal), VMware requires the use of an NSX Gateway, which can allow servers to run vSwitches and connect to the virtualized network.[46] VMware

[41] www.cisco.com/c/en/us/products/cloud-systems-management/intercloud-fabric/intercloud-fabric-for-business.html

[42] www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/dc-partner-microsoft/solution_overview_c22-687087.html

[43] www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html

[44] www.cisco.com/c/en/us/products/switches/application-virtual-switch/index.html

[45] www.vmware.com/files/pdf/vcloud-air/vcloud-air-Datasheet.pdf

[46] blogs.vmware.com/vcloud/2015/05/deep-dive-advanced-networking-services-vcloud-air.html

can achieve seamless networking for VMware deployments, but its approach does not secure connections to IoT devices.

Management suites and workload mobility

Any time that IT staff can devote to another part of infrastructure—instead of maintaining VMs—is a gain for a business. The effort of maintaining cloud solutions and moving VMs and workloads throughout a hybrid cloud can benefit from as much automation as possible. In addition, performing management tasks from a single pane of glass can make a positive difference in the daily lives of IT staff.

AWS

The AWS Management Console manages only AWS services and provides all necessary functionality for AWS.[47] There is also an AWS Management Console mobile app, available for both Apple iOS and Android.[48]

To import virtual machines into the AWS public cloud, users may use the AWS CLI or other tools to convert their VMs into the needed AWS Amazon Machine Image.[49] With Amazon's tools, users can import formats like RAW, VHD (but not VHDX), VMDK, and OVA. Amazon can export to any format listed above except for RAW. Exported images are saved in Amazon S3 and can be downloaded to a user's infrastructure.[50] The migration process in AWS is not automated, which means it can require dedicated time and labor from IT staff. In addition, users cannot migrate Elastic Block Storage data stores out of AWS, a problem that can require them to spend additional time and effort migrating such data to external on-premises or hosted-cloud infrastructure.

Cisco

Cisco's management and mobility portfolio includes Cisco Intelligent Automation for Cloud (IAC) products, Cisco UCS Director, Cisco ICF, the Cisco ONE Enterprise Cloud Suite, and the Cisco Prime Service Catalog.[51] Cisco IAC features many tools for cloud automation, including management of AWS EC2 instances, VMware vSphere installs, and more.[52] Cisco IAC is installed as a virtual appliance and offers a self-service portal, tenant segregation, provisioning automation, and integration with Cisco UCS, AWS, OpenStack, VMware vCloud Director, and others.

Cloud service providers, partners, and businesses can all use Cisco ICF for cloud management. For businesses, Cisco ICF is installed as a virtual appliance and designed to

[47] aws.amazon.com/console/
[48] aws.amazon.com/console/mobile/
[49] docs.aws.amazon.com/AWSEC2/latest/UserGuide/VMImportPrerequisites.html
[50] aws.amazon.com/ec2/vm-import/
[51] www.cisco.com/c/en/us/solutions/data-center-virtualization/cloud-management/index.html
[52] www.cisco.com/c/en/us/products/cloud-systems-management/intelligent-automation-cloud/index.html

offer workload mobility and seamless networking for Cisco partners, Azure, and AWS. ICF allows for a hybrid cloud framework and dashboard that includes support for Azure and AWS, with possibly more to come.[53] Cisco ICF allows for automated workload mobility and migration.

Cisco has an open approach to management packages. In some cases, Cisco cloud management tools can directly manage cloud infrastructure from other vendors. Cisco's hybrid cloud management tools can offer a single, straightforward interface for managing cloud conglomerates and seamlessly moving workloads.

VMware

VMware vCloud Suite and vCloud Air include support for vMotion, a VMware technology that allows users to move VMs and workloads.[54] Users may move workloads within the datacenter or across large distances (i.e. a multi-site datacenter). Live Migration capabilities extend even across high latency environments. VMware vCloud Suite includes products designed to manage cloud systems such as vRealize Operations, vRealize Automation, vRealize Business, vCenter Site Recovery Manager, and vSphere.[55] These technologies can provide features to enable a VMware-based cloud. To expand the hybrid cloud functionality to Azure and AWS, users need vRealize Operations and Automation Public Cloud Extensions add-ons. vCloud Air supports VM and workload mobility across VMware installations, and can extend such workload mobility to other leading public cloud deployments.

Hardware integration

Having capable, reliable hardware to support a cloud and its network connectivity is a key aspect of cloud infrastructure. Organizations implementing any kind of cloud need to consider how hardware components will affect them and determine which hardware portions of an infrastructure they can control.

AWS

AWS does not disclose the hardware that powers its public cloud solution or provide the user with any hardware integration tools. However, Amazon works with hardware vendors to offer certain services, such as Amazon CloudHSM.[56] Amazon enables users to deploy private hosted clouds inside AWS on AWS datacenters, but it doesn't provide any out-of-the-box private cloud solutions, like those from Cisco or VMware, that users could implement on-premises or that other cloud service providers could externally host.

[53] www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intercloud-fabric/datasheet-c78-732856.html
[54] www.vmware.com/products/vsphere/features/vmotion
[55] www.vmware.com/files/pdf/products/vCloud/VMware-vCloud-Suite-Datasheet.pdf
[56] aws.amazon.com/cloudhsm/

Cisco

Through ACI, Cisco Nexus hardware switches can respond to changing environments and workloads dynamically with the goal of shortening deployment times.[57] Cisco UCS hardware can be managed by Cisco UCS Director,[58] which provides many management features for implementing cloud solutions and integrating hardware management with cloud management. Cisco is a large manufacturer of networking, compute, storage, and other hardware solutions, including embedded low-power devices. They offer software management solutions to manage these components in a way that can make sense for cloud deployments.

Cisco also offers other cloud solutions, including many out-of-the-box solutions for both cloud service providers and enterprises. As an example, the Cisco OpenStack Private Cloud provides users with a remotely managed private cloud solution that resides on the customer premises.[59] According to Cisco, the OpenStack Private Cloud offering is targeted at solution providers. Cisco also offers bundled hardware solutions in their FlexPod and VCE vBlock solutions.[60, 61] In both solutions, Cisco partners with other hardware and software vendors to create multivendor, easy-to-deploy virtualization solutions.

VMware

VMware provides limited hardware integration with recently launched EVO:RAIL solutions.[62] EVO:RAIL solutions are software/hardware hyper-converged appliances, available through third-party hardware vendors, that leverage VMware hypervisors and cloud management for a complete out-of-the-box private cloud. VMware focuses on software-defined datacenter technologies while remaining hardware agnostic.[63]

Vendor lock-in & hypervisor choice

Some businesses prefer to use proven combinations of technologies, while others would rather make their technology choices independently. A wide array of supported hypervisors can offer customers flexibility and prevent vendor lock-in.

AWS

AWS uses the Xen hypervisor to host their EC2 instances. While AWS does allow import and export of virtual machines, users must convert their machines to the correct AWS format,[64] limiting many users to the AWS ecosystem. AWS supports a limited set of

[57] www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html#~products
[58] www.cisco.com/c/en/us/products/servers-unified-computing/ucs-director/index.html
[59] www.cisco.com/c/en/us/products/cloud-systems-management/openstack-private-cloud/index.html
[60] www.cisco.com/c/en/us/solutions/data-center-virtualization/flexpod/index.html
[61] www.cisco.com/c/en/us/solutions/data-center-virtualization/vblock-systems/index.html
[62] www.vmware.com/products/evorail
[63] www.vmware.com/software-defined-datacenter/
[64] aws.amazon.com/ec2/vm-import/

operating systems on their EC2 platform (see Appendix A).[65] A choice of AWS as cloud infrastructure can restrict vendor choice for the infrastructure layer.

Cisco

The Cisco cloud portfolio supports any hypervisor and any virtualized operating system for each supported hypervisor. Cisco also supports any hardware for its cloud solutions to use as compute, storage, or networking.[66] Cisco's strategy appears to be open: Provide maximum flexibility in vendor and cloud provider choice.

VMware

VMware vCloud Suite and vCloud Air use VMware vSphere and ESXi hypervisors,[67] so VMs running on top of these remain in VMware formats. VMware claims to support any x86-based operating system running as a virtual machine.[68] VMware's strategy is closed on the cloud-infrastructure software end, as it must be VMware.

Cloud support

Inevitably, there comes a time when IT staff have a question or need assistance troubleshooting something related to VMs. How quickly IT staff can get a response from support and resolve a matter can make a big difference in productivity and earnings.

AWS

AWS provides four tiers of support with different response times and features, which range from access to the AWS support API to 24/7 access to technical support. Amazon claims users who subscribe to the enterprise level of support get 15-minute response times, while users on the basic plan don't have a listed response time. The enterprise level of support comes at an extra cost, while AWS Basic support is standard with any use of the platform.[69]

Cisco

Cisco has different service solutions (for a fee, except for warranty) designed to help businesses maintain, manage, or support their cloud model. Cisco Solution support for ACI, for example, allows consumers to maintain and have replacement coverage of their hardware and software solutions.[70] Different levels of support under Cisco's model can allow coverage of hardware (Cisco Nexus 9000 switches) and provide on-site

[65] aws.amazon.com/ec2/faqs/
[66] www.cisco.com/web/solutions/trends/cloud/index.html
[67] www.vmware.com/products/vcloud-suite
[68] blogs.vmware.com/vcloud/2014/12/vmware-vcloud-air-supported-operating-systems.html
[69] aws.amazon.com/premiumsupport/
[70] www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/sspt-aci-aag.pdf

support.[71] Cisco also offers support under the Cisco Data Center Solution Support Service brand,[72] which Cisco claims offers the expertise of specialists in many Cisco technologies and includes product-specific experts if needed. Under the Cisco Powered Cloud Services and Cisco Powered Managed Services brand, enterprises can leverage Cisco partners to provide services such as support, managed cloud services, and Cisco Managed connectivity services.[73] Cisco provides an extensive portfolio of support models.

VMware

According to VMware documentation, VMware provides support services of on-premises and vCloud Air with one support call and a single point of contact.[74] A list of support tiers and supported products is publicly available on their website.[75] Support with VMware can be structured for only single products or span multiple VMware products, as well as some third-party solutions.

Cloud consulting services

For cloud service providers like AWS that offer low-end cloud solutions and have a low touch approach to client relationships, availability of consulting services may not be an issue. With a diverse portfolio like Cisco's, consulting services may be the first step in determining what kind of cloud solution is best for an organization. This is also the case with VMware.

AWS

Amazon has partners that can help businesses design, build, and manage their cloud deployments and applications hosted on AWS.[76] AWS doesn't provide consulting services in-house, but it offers consulting partners as part of the APN Consulting Services brand.[77] Amazon allows users to search for consulting partners on their website.

Cisco

Cloud consulting services offered through Cisco and Cisco partners include services that can help businesses determine how much, where, and what type of cloud solutions to purchase, as well as offerings for pre-existing cloud environments.[78]

[71] www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/sspt-aci-overview.pdf

[72] www.cisco.com/c/dam/en/us/products/collateral/data-center-virtualization/sales-tool-c96-730421.pdf

[73] www.cisco.com/web/solutions/trends/cisco-powered/services.html#~Services

[74] pubs.vmware.com/vca/index.jsp?topic=%2Fcom.vmware.vca.ug.doc%2FGUID-5001DAA0-E7F7-41FE-B137-AE673A5DD192.html

[75] www.vmware.com/files/pdf/support/Support-by-Product-Matrix.pdf

[76] www.aws-partner-directory.com/PartnerDirectory/PartnerSearch?type=SI

[77] aws.amazon.com/partners/consulting/

[78] www.cisco.com/web/services/enterprise-it-services/cloud-enablement-services/index.html

According to Cisco, enterprises can discover what they're spending on cloud services and figure out how to minimize cloud spending through Cisco Cloud Consumption Services.[79] The Cisco Cloud Enablement Services for Enterprises provides services built around the Cisco Domain Ten framework,[80] which is a novel structured method of planning and implementing IT services and roadmaps for future transitions. Cisco and Cisco partners provide these flexible-consulting options to any cloud consumer.

VMware

VMware provides three different types of consulting services.[81] Two of the options—Accelerate Advisory Services and Technology Consulting Services—include cloud-based components. VMware offers consulting services that target cloud automation, risk analysis, financial concerns, cloud operations, and hybrid cloud analysis.[82, 83]

Data Sovereignty

Some organizations, such as financial institutions, require that data reside at specific locations throughout the world, depending on local laws and regulations. Countries may have laws that require information from the country to be processed, stored, and kept within the country's geographical boundaries. Having a widely available net of datacenters to host public, private, or hybrid clouds can offer a greater ability to do more business on a global scale. All three cloud providers recognize this need and provide their own global datacenter and partner networks to deliver such services.

AWS

Amazon uses "availability zones" placed in strategic places around the globe to provide cloud services. Amazon has 13 availability zones in the US in four regions with 20 AWS "edge locations." Globally, including the US, there are 29 availability zones and 53 AWS edge locations. That includes 3 availability zones in South America, 5 in Europe, and 8 in Asia, plus 15 AWS edge locations in Asia, 16 in Europe, and 2 in South America.[84]

[79] www.cisco.com/web/solutions/trends/cloud/cloud-consumption-services.html
[80] www.cisco.com/en/US/services/ps2961/ps10364/ps11104/cloud_enablement_services_aag.pdf
[81] www.vmware.com/consulting/
[82] www.vmware.com/consulting/accelerate.html
[83] www.vmware.com/consulting/technology-consulting-services.html
[84] aws.amazon.com/about-aws/global-infrastructure/

Cisco

Cisco Intercloud Providers and Cisco Powered partners are publicly available and provide a combined 355 datacenters in 50 countries.[85] Cisco's current count of partners is greater than 60.[86]

VMware

VMware vCloud Air provides 11 locations in 5 countries, including 2 US government-only locations.[87] The VMware vCloud Air Partner Network includes over 4,000 partners in over 100 countries. These providers use VMware vSphere for their virtualization technologies.

CONCLUSION

Business agility depends on IT agility, or how quickly IT can deliver new business solutions to business problems. Today's increasingly fast-paced business environment requires companies to move away from traditional ways of thinking about new business and data architectures. Instead, companies need data reduction and analysis at the edge, where data originates, so they can quickly extract value from the data as it hits the organization with increasing volume, velocity, and variability.

For these reasons, both the datacenter and edge devices are becoming critical to new IT solutions built to address business needs. Today's IT solutions have to protect data assets, both at rest and in motion, and implement strong governance to support regulatory and legal compliance and data sovereignty. They also have to be easy to create, update, and deploy.

Cloud service providers take specific technology and business approaches to address problems like these. Their approaches can be device-centric, network-centric, or application-centric. They can have minimal contact with clients or emphasize partner networks and professional services. The kind of approach a cloud provider takes can determine which features are available to its clients. Further, availability of specific cloud features can affect how a company conceptualizes, designs, implements, and deploys its cloud solutions—and more importantly, affect the type and scope of business problems that they can use the cloud to address.

In this research paper, we examined the approaches of three major cloud providers—Amazon AWS, Cisco Intercloud, and VMware vCloud—and how the approaches affect the key features of their cloud solutions. We found differences in

[85] newsroom.cisco.com/documents/10157/7542607/Intercloud_Partner_FactSheet+Mar+11+as+of+3-10.pdf
[86] blogs.cisco.com/partner/igniting-the-intercloud-partner-ecosystem
[87] vcloud.vmware.com/explore-vcloud-air/vcloud-air-location

security, seamless networking, and cloud management, which can affect the balance among security, agility, and ease of use.

AWS maintains security of data in its public cloud, provides a seamless network after users configure features, and manages only AWS services. The Cisco cloud portfolio aims to ensure policy-defined security at any connectivity endpoint, enables seamless networking through an intelligent fabric geared to hybrid-IT deployment, and offers cloud management through either Cisco or non-Cisco cloud management packages. Finally, VMware concentrates on datacenter and data security. It secures cloud solutions based on VMware cloud technologies, provides seamless networking to on-premises IT through network virtualization, and includes products designed to manage a VMware-based cloud and expand hybrid cloud functionality through add-ons.

With a cloud space constantly in flux, we aimed to create a snapshot—as of the date of this report and based on publicly available data—of a few, key cloud providers. We expect cloud offerings to continue to shift and grow over the coming months and years, and we are eager to see what the future of the cloud holds.

APPENDIX A – DETAILED COMPETITIVE FEATURE COMPARISON

Figure 3 presents a detailed feature comparison for AWS, Cisco cloud, and VMware vCloud Air.

Feature Categories: Infrastructure

Hardware infrastructure

Amazon Web Services	Cisco cloud	VMware vCloud Air
• No physical infrastructure, but special-purpose hardware offered at client premises for high-grade security (AWS Hardware Security Module or HSM)	• Allows both Cisco infrastructure and client-provided infrastructure • Cisco UCS provides validated, converged solutions for cloud, such as FlexPod, VCE Vblock, and Cisco Cloud Architecture/Microsoft Cloud Platform • Provides a fully managed Cisco OpenStack to on-premises private clouds built on Cisco UCS hardware	• No hardware offering, constrained to use VMware virtualization infrastructure • Hyper-converged hardware offerings starting to appear based on EVO:RAIL and EVO:RACK that are pre-packaged, easy to install, and provide an on-premises private cloud

Supported hypervisors, VMs, and OS

Amazon Web Services	Cisco cloud	VMware vCloud Air
• Only VMs running on Xen hypervisor • AWS supports Windows and many flavors of Linux. Supported OSs include ○ *Microsoft* – Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2; ○ *Amazon* – Amazon Linux; ○ *Red Hat* – Red Hat 008 R2, Windows Server 2; ○ *SUSE* – SEL 11, SEL 12; ○ *Other Linuxes* – Debian, Ubuntu Linux, FreeBSD 10, FreeBSD 9	• Supports any hypervisor/VM on any x86-based OS and other OSs as stated below • ICF (as of 5/13/15): ○ *Hypervisors*: Citrix Xen, MS Hyper-V and VMware V-Sphere ○ *OS*: any from list below • Cisco platform (as of 5/13/15): ○ *Hypervisors*: VMware V-Sphere, Microsoft Hyper-V, Red Hat KVM, Citrix Xen, Oracle OVM ○ *OS*: any x86-based OS • OS support (as of 5/13/15) ○ *Microsoft* – Windows Server 2012 , Windows Server 2012 R2, Windows 8, Windows 8.1, Windows 7, Server 2008, Windows Server 2008 R2 , Server 2003, Windows Small Business Server 32-bit, Windows Vista, Windows XP Professional, Windows 2000, Windows NT, Windows 3.1, MS-DOS; ○ *Red Hat* – RHEL 6, RHEL 5, RHEL 4, CentOS; ○ *SUSE* – SEL 11, SEL 10; ○ *Oracle* – Linux 6, Linux 5, Linux 4; Oracle Solaris for X86	• Only VMware VMs • VMware claims to support any x86-based OS. Supported OSs include ○ *Microsoft* – Windows Server 2012 , Windows Server 2012 R2, Windows 8, Windows 8.1, Windows 7, Server 2008, Windows Server 2008 R2 , Server 2003, Windows Small Business Server 32-bit, Windows Vista, Windows XP Professional, Windows 2000, Windows NT, Windows 3.1, MS-DOS; ○ *Red Hat* – RHEL 6, RHEL 5, RHEL 4, CentOS; ○ *SUSE* – SEL 11, SEL 10; ○ *Oracle* – Linux 6, Linux 5, Linux 4; ○ *Ubuntu* – Ubuntu Linux and other Linux

	○ *Ubuntu* – Ubuntu Linux and other Linux	

Seamless networking

Amazon Web Services	Cisco cloud	VMware vCloud Air
• Amazon provides VPN access, but users must pay extra – no seamless networking or networking dashboard	• Cisco provides this functionality via connectors installed on third-party VMs (Cisco Cloud Connectors) • Cisco and Cisco partners provide multiprotocol label switching (MPLS), Quality of Service (QoS), and virtual private networks (VPNs), using routers and switches that run Cisco IOS for end-to-end networking and solutions • Cisco Intercloud Fabric (ICF) connects provider clouds and on-site datacenters or private clouds, allowing seamless mobility for workloads between on-premises clouds and hosted private and public clouds • Implements secure connections between hypervisors – the same security used by Cisco Intercloud Fabric in the on-premises datacenter is used for the connection to public clouds (secure, key-based cryptographic connections) • Implements end-to-end fabric policy management and security	• VMware only provides seamless public-to-private networking for their vCloud Air and vCloud Suite solutions

Public cloud support

Amazon Web Services	Cisco cloud	VMware vCloud Air
• AWS does not directly support other public clouds, although other vendors provide connectivity to AWS	• Supports Cisco Intercloud Providers and Cisco Powered partners, as well as AWS and Azure	• Provides connectivity to VMware-based public clouds • Can create AWS cloud endpoints, compute and storage resources via vCloud Automation Center and vCloud Suite solutions

Network virtualization

Amazon Web Services

- AWS provides the Amazon Virtual Private Cloud, which uses network virtualization to logically separate components
- AWS provides secure VPN services that can be strengthened with the Amazon Cloud Hardware Security Module

Cisco cloud

- Cisco Network Virtualization Solutions provide features such as access control, path isolation, and services edge
- Path isolation can utilize technologies like MPLS, virtual routing and forwarding (VRF), and generic routing encapsulation (GRE) to support VPNs
- Cisco Catalyst series switches are marketed for network virtualization

VMware vCloud Air

- VMware NSX is a network-virtualization platform produced by VMware that works with many switch and compute vendors, including Cisco Nexus and UCS
- VMware NSX allows deployment in a pre-existing environment

Internet of Things (IoT) / Internet of Everything (IoE)

Amazon Web Services

- AWS provides components for implementing IoT infrastructure:
  - Compute via EC2 with burstable, compute, memory, storage, and GPU-optimized instances
  - Large, distributed, real-time data stream processing with Amazon Kinesis
  - Security mechanisms for both data in motion and data at rest, including Amazon Identity and Access Management (IAM), Amazon Secure Token Service (STS) with built-in encryption and key rotation, Amazon Cognito for securing mobile infrastructure, and special-purpose hardware security modules for secure key storage
  - Auto-scaling as the number of devices grows
- Open-source tools such as Mosquitto MQ telemetry transport for sensors and mobile devices, and Apache MQ integration services

Cisco cloud

- Cisco provides a spectrum of products, solutions and services to support IoT and IoE
- Cisco's IoT supports device interconnection from field networks, industrial networks to embedded solutions
- Industrial network IoT supported with Cisco Connected Grid Network Management
- Support of industrial sensor networks via Cisco Field Network Distribution Architectures (e.g. energy grid)
- Embedded networks use Cisco 59xx ESRs (Embedded Services Routers) and Cisco 2020 Embedded Services Switches to extend networks to extreme edge devices
- Cisco management and analysis tools use Cisco IoX, which builds on Cisco IOS, to extend coverage to compute, storage, and memory at the network edge; IoX makes these resources accessible via an open environment for application development
- Cisco created the IoE Index to survey and calculate potential value for IoE initiatives

VMware vCloud Air

- No clear product, solutions, or services portfolios for IoT or IoE
- In Oct 2014, VMware was part of the Industrial Internet Consortium to accelerate IoT in the enterprise
- VMware acquired AirWatch in Jan 2014; AirWatch provided some products aimed at the IoT

Feature Categories: Cloud management

VM migration

Amazon Web Services

- AWS allows VMs to be exported and imported in certain formats, but doesn't provide a simplified dashboard or console to do so
- AWS provides availability zones that back up workloads, data, and virtual machines, but still hasn't released any information on live migration
- Lack of cloud interoperability: difficult to move workloads off AWS to other clouds

Cisco cloud

- Cisco Intercloud Fabric provides uniform and transparent VM and workload movement from one cloud location to another (whether on-premises or off-premises—either hosted or public)
- The ICF vision is to allow "anything running on anything," and is in process of being implemented
- Cisco's Intelligent Automation for Cloud provides comprehensive cloud management from infrastructure anything-as-a-service (XaaS) platforms from a single, unified interface providing lifecycle, governance, and consumption management views for each user type

VMware vCloud Air

- VMware vCloud Suite and vCloud Air allow live migration of any VMware ESXi-based virtual machines and workloads
- Claims any x86-based system can be moved onto vCloud/vCloud Air
- Lack of cloud interoperability: difficult to move workloads off AWS to other clouds

Usability and unified dashboard

Amazon Web Services

- AWS provides a management console that only allows a view of AWS components; plugins exist for vCenter, but are not universal

Cisco cloud

- Single interface for end-to-end hybrid cloud management
- Simplified, unified dashboard that spans multiple vendors and technologies

VMware vCloud Air

- Unified dashboard only for vCloud Air and vCloud Suite products; plugins may allow third-party integration with other clouds (AWS)

Elasticity

Amazon Web Services

- Amazon's Elastic Compute Cloud (EC2) allows users to rapidly expand or shrink capacity based on business needs, and includes pay-as-you-go (hourly), monthly, and yearly subscriptions

Cisco cloud

- Cisco allows users to build or buy workload capacity using cloud service providers, on-premises UCS, or managed services

VMware vCloud Air

- VMware vCloud Air provides models that include pay-as-you-go, subscriptions, and prepaid options, allowing users to rapidly expand or shrink capacity

Metrics and monitoring

Amazon Web Services

- Amazon includes their AWS CloudWatch for additional cost, but this provides only performance metrics for AWS services; no end-to-end metric collection or reporting. AWS also provides itemized bills

Cisco cloud

- Cisco Prime infrastructure enables unified management of network, devices, applications, and users
- It offers 360 views of fault, configuration, accounting, performance, and security (FCAPS) monitoring and management for Cisco servers and ACI-ready Cisco Nexus-based infrastructure

VMware vCloud Air

- vCloud Director collects and monitors information on VMs within the VMware ecosystem; VMware provides itemized bills

	• It provides wired and wireless lifecycle management and application visibility and control, with policy monitoring and troubleshooting via Cisco Identity Services Engine (ISE) and location-based tracking of mobility devices with Cisco Mobility Services Engine (MSE) • Cisco Cloud Consumption Services collects metrics on cloud services consumed by an organization, enabling handling of shadow IT while allowing multiple vendors and cloud providers and providing detailed and consolidated reporting capabilities	

Performance benchmarks

Amazon Web Services	Cisco cloud	VMware vCloud Air
• PT studies on AWS, many other third-party benchmarks • AWS instances (storage, compute) can be scaled if performance isn't adequate	• Many different Intercloud providers and Cisco partners with many different configurations • Customizable configurations enable tuning architecture to desired performance • Recent studies (e.g. IDG's on SAP Hana and Cisco UCS/Nexus) show that Cisco's flexible and scalable infrastructure is well matched to edge data processing of in-memory applications that require clustering and cooperative processing between nodes; in addition, Cisco UCS service profiles significantly reduce time to deployment • Other studies point to increased flexibility and scalability as well as reduced risk and cost in deployments of JD Edwards EnterpriseOne 9.1 on SmartStack using Cisco UCS and Oracle	• PT studies on VMware vCloud; VMs can be dynamically allocated more resources if not performing as necessary

Feature Categories: Security and compliance

Security

Amazon Web Services	Cisco cloud	VMware vCloud Air
• Amazon allows secure-link encryption, but users must pay extra for services like VPN; no end-to-end security except within AWS	• Cisco ISE and ACI provide application-aware, complete end-to-end security, encryption, and logged access to infrastructure • Cisco ISE and ACI also provide a complete mobility solution, spanning infrastructure and mobile devices	• VMware provides vCloud Networking and Security as part of the vCloud Suite, including encryption, which is available for an extra fee

- Cisco end-to-end network security enables the ability to secure IoT devices
- Cisco ACI combined with Cisco Firepower security enables
  - Deployment of application-specific security over multi-vendor security devices
  - Physical and virtual security devices to be inserted into an application's data traffic flow; and
  - Securing inner application flows, going beyond standard edge security, and ensuring that different workloads or users can't interfere with each other in a multi-tenanted cloud network

Data sovereignty

Amazon Web Services

- Amazon uses "availability zones" placed in strategic places around the globe
- At time of writing, Amazon has 13 availability zones in the US in four regions, with 20 AWS edge locations
- Globally, including the US, there are 29 availability zones and 53 AWS edge locations – 3 availability zones in South America, 5 in Europe, and 8 in Asia; 15 AWS edge locations in Asia, 16 in Europe, and 2 in South America
- There are 53 global locations for CloudFront edge points, with 20 locations in the United States, 16 in Europe, 15 in Asia, and 2 in South America

Cisco cloud

- Cloud partners have locations around the globe—Cisco has over 75 Intercloud providers and a large, growing number of global datacenters (about 300)
- 450 Cisco Powered Services providers and resellers
- 500+ services deployments
- 21 cloud and managed services reference architectures (portfolio breadth)
- Clients can increase availability zone coverage using either Intercloud provider networks or other Cisco-powered cloud service providers

VMware vCloud Air

- VMware provides its own datacenters and vCloud Air Network around the globe
- VMware owns 11 locations worldwide, of which 7 are in the US
- vCloud Air datacenters located in
  - US: Northern California, Nevada, Texas, Virginia, and New Jersey, with government datacenters in Arizona and Virginia
  - Europe: UK and Germany
  - Asia: West Japan
  - Australia: South Australia
- VMware vCloud Air Network (Partners): 4,000 Service Providers in more than 100 countries

Feature Categories: Ecosystem and partner network

Marketplace

Amazon Web Services

- *AWS Marketplace* – software infrastructure, developer tools, and business software that run on AWS EC2 instances

Cisco cloud

- Cisco's partner-centric cloud approach consists of Independent Software Vendor (ISV) partners, Intercloud providers, and Cisco Powered partners
- *Cisco Marketplace* – Services and technology partners; validated solution catalog for analytics, mobility, enterprise networking, datacenter, security, and collaboration

VMware vCloud Air

- *vCloud Air Marketplace* – Solution catalog spanning application development and deployment, infrastructure, security, databases, and others

	- Cisco Intercloud providers and Cisco Powered partners are Cisco-validated solution providers, delivering end-to-end QoS	
Partner cloud service provider network		
Amazon Web Services	Cisco	VMware vCloud Air
- 22 aligned AWS resellers with professional services and consulting capabilities	- Cisco Cloud Marketplace/Cloud and Managed services program; over 70 Intercloud providers and over 300 datacenters	- VMware vCloud Air network provides a list of providers that use VMware vCloud Air and Director services
Development tools		
Amazon Web Services	Cisco cloud	VMware vCloud Air
- Amazon provides AWS toolkits for Eclipse, and an AWS toolkit for Visual Studio to help create applications built on AWS	- Cisco provides public, documented APIs to developers with OpenStack, Intelligent Automation for Cloud, Prime Home, and Intercloud Fabric; Cisco also hosts developer training sessions	- VMware provides SDK for vCloud, vCenter, vSphere, etc. and publishes documented APIs for many of their products

Figure 3: Detailed information about the three cloud offerings.

ABOUT PRINCIPLED TECHNOLOGIES

Principled Technologies, Inc.
1007 Slater Road, Suite 300
Durham, NC, 27703
www.principledtechnologies.com

We provide industry-leading technology assessment and fact-based marketing services. We bring to every assignment extensive experience with and expertise in all aspects of technology testing and analysis, from researching new technologies, to developing new methodologies, to testing with existing and new tools.

When the assessment is complete, we know how to present the results to a broad range of target audiences. We provide our clients with the materials they need, from market-focused data to use in their own collateral to custom sales aids, such as test reports, performance assessments, and white papers. Every document reflects the results of our trusted independent analysis.

We provide customized services that focus on our clients' individual requirements. Whether the technology involves hardware, software, websites, or services, we offer the experience, expertise, and tools to help our clients assess how it will fare against its competition, its performance, its market readiness, and its quality and reliability.

Our founders, Mark L. Van Name and Bill Catchings, have worked together in technology assessment for over 20 years. As journalists, they published over a thousand articles on a wide array of technology subjects. They created and led the Ziff-Davis Benchmark Operation, which developed such industry-standard benchmarks as Ziff Davis Media's Winstone and WebBench. They founded and led eTesting Labs, and after the acquisition of that company by Lionbridge Technologies were the head and CTO of VeriTest.

Disclaimer of Warranties; Limitation of Liability:

PRINCIPLED TECHNOLOGIES, INC. HAS MADE REASONABLE EFFORTS TO ENSURE THE ACCURACY AND VALIDITY OF THE RESEARCH IN THIS PAPER, WHICH REFLECTS PUBLICLY AVAILABLE INFORMATION AND CONTAINS CITATIONS FOR ALL SOURCES IN FOOTNOTES. HOWEVER, PRINCIPLED TECHNOLOGIES, INC. SPECIFICALLY DISCLAIMS ANY WARRANTY, EXPRESSED OR IMPLIED, RELATING TO THE RESEARCH AND ANALYSIS, THEIR ACCURACY, COMPLETENESS OR QUALITY, INCLUDING ANY IMPLIED WARRANTY OF FITNESS FOR ANY PARTICULAR PURPOSE. ANY PERSONS OR ENTITIES RELYING ON THE RESULTS OF ANY RESEARCH DO SO AT THEIR OWN RISK, AND AGREE THAT PRINCIPLED TECHNOLOGIES, INC., ITS EMPLOYEES AND ITS SUBCONTRACTORS SHALL HAVE NO LIABILITY WHATSOEVER FROM ANY CLAIM OF LOSS OR DAMAGE ON ACCOUNT OF ANY ALLEGED ERROR OR DEFECT IN THE RESEARCH CONTAINED IN THIS REPORT.

IN NO EVENT SHALL PRINCIPLED TECHNOLOGIES, INC. BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH ITS RESEARCH, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL PRINCIPLED TECHNOLOGIES, INC.'S LIABILITY, INCLUDING FOR DIRECT DAMAGES, EXCEED THE AMOUNTS PAID IN CONNECTION WITH PRINCIPLED TECHNOLOGIES, INC.'S RESEARCH. CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES ARE AS SET FORTH HEREIN.