PIQUE SOLUTIONS

Securing Data and Applications in the Cloud

Comparison of Amazon, Google, Microsoft, and Oracle's Cloud Security Capabilities

PIQUE SOLUTIONS

January 2021

THE DEVELOPMENT OF THIS WHITE PAPER WAS SPONSORED BY ORACLE. THE UNDERLYING RESEARCH AND ANALYSIS WERE EXECUTED INDEPENDENTLY BY PIQUE SOLUTIONS.

795 Folsom Street, 1st Floor | San Francisco, CA 94107 | Tel.: 415.685.3392 | www.piquesolutions.com

Contents

Pique Solutions is a competitive research and market analysis firm supporting Fortune-500 technology companies. Pique is based in San Francisco, California.

Introduction

According to leading analysts, nearly 90% of organizations are currently using public cloud infrastructure services and over 50% will have all their data stored in such environments within two years. As business-critical services are migrated to the cloud in ever greater numbers, reducing the cloud attack surface is strategically critical for securing organizations' workloads.

A key aspect of security in infrastructure-as-a-service (IaaS) cloud platforms is who has accountability and ownership of the different layers of the cloud stack, from physical assets to data. Accountability is defined in the shared responsibility model as what the provider is responsible for and what is the onus of the user. Typically, the cloud provider is responsible for making sure infrastructure built within its platform is inherently secure and reliable, while the customer is responsible for securing their data, user access, applications, operating systems, and virtual network traffic. Typical challenges from the customer side include the following:

- Unencrypted data shared between users and applications.
- Configuration mistakes that allow for unauthorized access to applications.
- Shadow services deployed by enterprise users for specific business purposes with no oversight from IT security.
- User role–based permissions not correctly configured or understood, including the use of token-based access methods.

Understanding the security capabilities of an IaaS provider means examining the controls available to the customer combined with the underlying foundation of the cloud infrastructure. The key areas by which to evaluate an IaaS provider's security capability include the following:

- Physical security as implemented by the IaaS provider, such as protecting physical assets at a geographic location and resource isolation and zoning.
- Infrastructure security, such as ensuring that security patches are updated as soon as possible and that ports are scanned for abnormal behavior.
- Data and access security controls available to the user, such as encrypting data, controlling user privileges, and managing resource access.

Pique Solutions developed this white paper to help information security professionals chart a path through all this complexity. The paper features an independent, technical comparative analysis among the four leading cloud platforms—Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Oracle Cloud Infrastructure (OCI)—and evaluates how each vendor secures highly sensitive data and workloads on core cloud IaaS compute services. Drawing on the experience of subject matter experts and feedback from cloud customers, we used a qualitative approach to compare each cloud service provider (CSP). Six categories were selected to provide as much insight as possible into the broad range of security capabilities offered by each CSP in areas that prospective customers consider a priority.

Executive Summary

The cloud market has matured over the past decade, the core architecture expectations of what is required of a provider have matured and can be examined in six areas of capability. The four IaaS providers Pique Solutions looked at have many similarities in capabilities across the six areas examined. While all these providers offer a comprehensive suite of services for securing data, our research also found that each vendor has niche advantages over the competition in some areas.

AWS provides the greatest breadth of services, whereas Azure excels in compliance and monitoring, a user-friendly interface, and seamless integration with Microsoft Office 365. GCP is cost effective, is more open than other cloud providers, and possesses deep expertise in cybersecurity, artificial intelligence and machine learning, and container management. OCI stands out as offering more capabilities at no extra cost and features that are switched on by default to minimize human error.

Based on our assessment, the high-level differentiators among the four vendors are the following.

Perimeter Security

- AWS offers a wider range of services than the other providers.
- AWS offers the highest level of customization of any vendor.
- OCI's web application firewall (WAF) policy definition is the most intuitive and user-friendly of all providers.
- Unlike the other CSPs, OCI offers dedicated regions that make all OCI services available for deployment in customer datacenters at no additional cost.

Network Security

- Azure security groups and GCP firewall rules are stateful for both internal and external connections.
- AWS network access control lists (ACLs) are stateless, and security groups are stateful.
- OCI virtual security rules have an option for stateful or stateless firewalls.
- OCI supports both security lists and network security groups (NSGs), providing a more granular and flexible approach to securing a cloud network.
- Google is unique because it owns the physical network on which its cloud services sit, including worldwide telecommunication services.

Virtualization/Host

- AWS and OCI provide the most comprehensive bare metal services among the four CSPs.
- AWS offers bare metal instances that allow their Elastic Compute Cloud (EC2) customers to run application workloads that require direct access to bare metal infrastructure.

- Azure has a purpose-built bare metal infrastructure to scale workloads, although only for SAP high-performance analytic appliances (HANA).
- OCI designed its bare metal services from scratch to support high-performance workloads.
- Oracle's customers can run bare metal instances in customer-dedicated physical servers or as virtual machine (VM) instances, which are isolated computing environments on top of bare metal hardware.
- OCI takes virtualization of the network and disk IO out of the software stack and puts it in the network. This removes the requirement for hypervisors and other CSP code to run on customer instances, if running on bare metal or dedicated servers. Oracle Autonomous Linux is the first of its kind and gives OCI the edge, with automated zero-downtime patching, known exploit detection, and more.
- GCP uses Google's global ultra–low-latency internal network, which is proprietary to Google. With GCP, customers can easily build a global infrastructure with geo-distributed data. This is difficult with other providers.

Identity and Access Management

- Azure Active Directory (AD) is the most user-friendly option (similar to Microsoft AD).
- Azure AD features built-in synchronization with Microsoft AD (the other CSPs require another service or a third-party solution at a cost).
- AWS delivers the most granular access control but can be challenging to implement.
- AWS Identity and Access Management (IAM) access advisor and GCP Recommender help with auditing user permissions.
- GCP's Identity Management works extremely well due to G Suite's Cloud Identity. It provides single sign-on with multifactor authentication, so there's no need to use other solutions.
- OCI's compartment feature combined with policy-driven IAM provides a much easier way to implement IAM and very strong access control capability.

Security Posture Management

- A lack of automated configuration enforcement has historically contributed to serious incidents in AWS environments.
- No CSPs have a feature similar to OCI's Security Zones.
- AWS Config provides the best capability to monitor configuration changes.
- AWS and OCI have their own variants of Linux. AWS offers System Manager Patch Management services. OCI offers autonomous management via its OS Management Service.
- GCP operations suite with the addition of paid services such as virtual private cloud (VPC) flow logs can provide automated auditing capability.

- OCI Cloud Guard works to analyze data and to detect threats and misconfigurations automatically, as well as provides preconfigured auto-remediation without requiring human oversight. It continuously collects data from every part of the infrastructure and application stack.

Data Security

- Both OCI and Azure offer in-database encryption; however, Azure only offers this on its newer versions of both SQL and NoSQL services.
- Azure and OCI offer encryption by default on relational databases for Microsoft SQL server and Oracle services, respectively. Encryption needs to be manually enabled on AWS RDS (relational database service) and Aurora.
- Oracle Data Safe adds several security features at no additional charge for Oracle Cloud databases, including database security assessments, user risk scoring, sensitive data discovery, and data masking. This complements the strong native security features of Oracle databases.
- Google's infrastructure provides a variety of storage services, such as BigTable and Spanner, and a central key management service (KMS) to secure data.

With its new cloud services for security, including Cloud Guard, Security Zones, and Data Safe, Oracle has an edge over Amazon, Microsoft, and Google, as it provides a more centralized security configuration and posture management, as well as more automated enforcement of security practices at no additional cost. This allows OCI customers to enhance overall security without requiring additional manual effort, as is the case with AWS, Azure, and GCP.

Approach and Methodology

The methodology developed and followed by Pique Solutions is as follows:

1. Determine the key security characteristics and capabilities required to reduce the attack vector.
2. Develop a comparative assessment framework with assessment groups and components.
3. Evaluate, through secondary research and product documentation, how selected CSPs meet the defined security characteristics and capabilities.
4. Interview customers of AWS, GCP, Microsoft Azure, and OCI.
5. Interview cloud security subject matter experts and consultants.
6. Publish a detailed assessment of findings.

With the lens of mitigating key threats to application and data security in the cloud, we grouped the key capabilities into the six categories and components, as listed in **Table 1**.

Table 1. Categories and Components of Assessment

Perimeter Security	Network Security	Virtualization/ Host
▪ Protection against DDoS, bots, DNS, etc. ▪ Aspects of Web Application Firewall (WAF) ▪ Control over types of requests to ports	▪ Network Security Groups (NSG) ▪ Network firewall ▪ Routing ▪ Flow logs ▪ Security lists ▪ Aspects of WAF	▪ Customer Isolation ▪ OS management ▪ Virtualization ▪ Bare metal
Identity and Access Management	**Security Posture Management**	**Data Security**
▪ Access Management ▪ Privileged Accounts ▪ Segregation of Duties (SoD) ▪ Authentication ▪ Authorization ▪ IAM and group policies	▪ Audit logs ▪ Monitoring ▪ Configuration ▪ Enforcement	▪ Key management ▪ Data at rest ▪ Data in transit ▪ Encryption ▪ Database security ▪ Storage

The criteria are defined and assessed based on Pique Solutions' subject matter expertise and, where appropriate, based on the guidance of eminent cloud security governance programs and bodies such as the Federal Risk and Authorization Management Program, National Institute of Standards & Technology, and Cloud Security Alliance.

When comparing the capabilities of the four cloud services, we based our assessment on the categories and parameters outlined in **Table 2**.

Table 2. Assessment Parameters

Assessment Category	Assessment Parameters
Functionality	▪ Full functionality and secure by default ▪ Full functionality, secure by default, requires additional configuration ▪ Partial functionality, requires additional configuration ▪ Partial functionality, requires additional configuration and 3rd-party tools to achieve full functionality ▪ Not present
Granularity of Controls	▪ High ▪ Medium ▪ Low
User Interface	▪ Very Intuitive ▪ Somewhat Intuitive ▪ Not Intuitive

Finally, we interviewed cloud security subject matter experts and customers of Amazon, Google, Microsoft, and Oracle about their experience with the security capabilities of their cloud offerings.

Table 3 lists the organizations interviewed in this research study.

Table 3. Companies Included in Primary Research

Company	Title
Financial Services	Cloud Architect
U.S. Federal Government	Chief Information Security Officer
Healthcare Service Providers	Cloud Security Consultant
U.S. Government Agency	Cloud Security Consultant
Global Leader in Connected Vehicles and IoT	Information Security Manager
Global Customer Experience Services Provider	Vice President of Enterprise Application Services
Global Nonprofit Organization	Senior Director of Operations
Mobile Applications Development Company	President

Capabilities and Approaches

As already discussed, there are some major differences in the capabilities of the four IaaS vendors described in this white paper. They can be articulated as follows.

AWS

Amazon pioneered the public cloud market, primarily for IaaS and object storage. It has the largest security partner community of independent software vendors and system integrators. AWS Organizations and Control Tower help them manage AWS accounts to the point each developer can use their own AWS account. AWS has added security services over the past 15-plus years in a bid to reduce customers' attack surface. These bolt-on services can add extra cost, complexity, and confusion for customers due to the number of options and lack of coherency. System configuration on AWS requires careful attention, typically by highly skilled and, thus, expensive staff.

GCP

GCP started life as the Google App Engine in 2008, making it about as old as Azure. It is a public hybrid cloud hosted on Google Cloud Infrastructure, a private infrastructure utilized only by staff and using only Google-developed software. Although customers have no direct access to Google Cloud Infrastructure, it is responsible for implementation of the common controls for all Google offerings, including GCP. Google offers an operations suite (formerly called Stackdriver) for cloud monitoring and logging and was a pioneer of Zero Trust for granular access to files and services. This extra granularity, however, can make it difficult for those without in-house skills, exposing organizations to misconfiguration challenges. GCP does not offer native encryption within databases but instead relies on encryption at the storage level.

Microsoft Azure

Microsoft Azure is not quite as old as AWS but was first launched more than a decade ago. Microsoft has released a patchwork of services in the intervening 12 years designed to improve the security of Azure-hosted workloads. Azure provides many out-of-the-box services and features for customers migrating Windows-based workloads. For customers running Linux workloads, however, Azure does not have its own Linux variant for tighter integration with other Azure services. Microsoft offers default storage encryption with Transparent Data Encryption (TDE) for its Azure SQL database service. Microsoft's documentation states that TDE is enabled for all newly deployed Azure SQL databases and needs to be manually enabled for older databases; however, securing non-Windows workloads requires significant effort.

OCI

OCI is the youngest cloud provider of the four and is designed from the ground up around security. As an extra layer of defense against attacks, the physical network is hyper-segmented into "enclaves" to separate CSP code from customer workloads. Oracle Autonomous Database services provide secure data storage, utilizing a high degree of automation to minimize human error. OCI compartments provide strong security boundaries within tenants, supporting Least Privilege approaches and Zero Trust. Security Zones provide a secure enclave within customer tenancies for the most sensitive workloads, where security is mandatory and always on. Data

encryption is always on, everywhere, and dedicated regions enable customers to run OCI services in their own datacenters at no additional cost once a minimum spend requirement is met; however, OCI is new to the market and will need to prove itself to gain market share from the other CSPs.

Perimeter Security

While the concept of perimeter has diminished in the cloud and its shared resources architecture, there is still a need for defining the external boundaries of cloud data, applications, and services. Perimeter controls in a cloud environment focus on uptime and resource availability from attacks such as denial of service and DNS poisoning of cloud services. Perimeter also includes some aspects of a WAF for cloud applications, as well as control of remote access to cloud resources, such as port requests. All four cloud providers offer a complete range of controls for mitigating external-facing threats and sustaining uptime during a targeted denial of service. Google may have a slight edge in this category due to its machine-learning capabilities and out-of-the-box functionality, while the AWS WAF service offers the most customizable options.

AWS

AWS perimeter security services protect public-facing endpoints from Layer 7 attacks. To protect web applications or API workloads against common web exploits that may affect availability, compromise security, or consume excessive resources, AWS provides WAF and AWS Shield services. AWS WAF gives customers control over how traffic reaches their applications by enabling them to create security rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that filter out specific traffic patterns they define. AWS WAF is highly customizable, and users pay only when the rules are triggered. The solution is suited for medium to large companies that have personnel with the requisite skills.

AWS Shield is a managed dedicated denial of service (DDoS) protection service that safeguards applications running on AWS. All AWS customers benefit from the automatic protection of AWS Shield Standard (at no additional charge) for the most common, frequently occurring network and transport layer DDoS attacks. The solution is well suited for small organizations with limited security staff.

AWS Shield Advanced provides additional detection and mitigation in near real-time, alongside integration with AWS WAF and 24×7 access to the AWS DDoS Response Team. AWS WAF pricing is based on resource type usage per hour, whereas AWS Shield has a flat monthly charge. The solution is well suited for medium to large organizations that wish to augment or outsource their security team.

GCP

Google Cloud services accept requests from around the world using a globally distributed system called Google Front End (GFE). GFE terminates traffic for incoming HTTP(S), TCP, and transport layer security (TLS) proxy traffic, provides DDoS attack countermeasures, and routes and load-balances traffic to Google Cloud services.

GCP's Cloud Armor service mitigates DDoS attacks and allows users to create custom L7 filtering policies to enforce granular access controls on public-facing applications and websites. Cloud Armor is deployed at the edge of Google's network and tightly coupled with GCP's global load-balancing infrastructure. Armor includes customizable features such as geo-based access controls, preconfigured WAF rules, and L7 filtering policies using custom rules. The service has three-tier combined pricing based on a per–security policy, per-rule, and per-requests evaluated model.

Microsoft Azure

Microsoft Azure WAF on Azure Application Gateway provides centralized protection of web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks. WAF on Application Gateway is based on the Core Rule Set from the Open Web Application Security Project (OWASP). The WAF automatically updates to include protection against new vulnerabilities, with no additional configuration needed. The service has combined pricing based on the Application Gateway type and the amount of data processed.

> "Although OCI is new to the game, the modern infrastructure and security-first design architecture have allowed Oracle to provide cloud services that are faster with reduced effect to run secure workloads."
>
> *Chief Information Security Officer for U.S. Federal Government*

OCI

OCI WAF is a global security service that protects applications from malicious and unwanted internet traffic. WAF can protect any internet-facing endpoint, providing consistent rule enforcement across a customer's applications. WAF provides organizations with the ability to create and manage rules for internet threats, including Cross-Site Scripting, SQL Injection, and other OWASP-defined vulnerabilities. Unwanted bots can be mitigated while tactically allowing desirable bots to enter. Access rules can be limited based on geography or the signature of the request. Oracle is the only vendor among the four CSPs that provides DDoS protection at no additional cost. For extremely security-sensitive customers, Oracle-dedicated regions enable customers to run OCI services in their own datacenters.

Network Security

A challenge with network security in cloud computing is an organization's lack of visibility to monitor network traffic and respond to suspicious activity. Computing on a public cloud relinquishes control of networking and data from the user or enterprise to the CSP yet, in the shared responsibility model, the security of data is the customer's responsibility.

For this reason, it is imperative the cloud provider offers native capabilities and/or supports third-party tools to ensure key network security principles. These include isolation between multiple zones by using layers of firewalls, controls for traffic to and from applications, end-to-

end transport-level encryption, and standard secure encapsulation protocols, such as IPSEC, SSH, and secure sockets layer (SSL), used when deploying a VPC. On top of all these capabilities, the IaaS provider should support some method of network monitoring for threat detection and response, which means providing a data source of network traffic for security inspection.

AWS

The AWS network is divided into geographical regions and subsequent zones within each region. Each zone may consist of one or more datacenters. AWS also has Local Zone, an extension of an AWS Region in geographic proximity to users with its own internet connections, thus reducing latency. Each datacenter is segmented using VPCs. These allow customers to provision a logically isolated section of the AWS cloud where they can launch AWS resources in a virtual network that they define. Customers have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways.

Customers can use both IPv4 and IPv6 in their VPCs for secure and easy access to resources and applications. VPCs are secured by network ACLs that act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level. ACLs are stateless, which means that responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa). Routing tables and internet gateways are associated with VPCs to allow, restrict, or direct traffic.

Like ACLs, security group firewalls for associated Amazon EC2 instances control both inbound and outbound traffic at the instance level and are applied at the network interface level. Security groups, however, are stateful, meaning if users send a request from their instance, the response traffic for that request can flow regardless of inbound security group rules. Responses to inbound traffic can flow out, regardless of outbound rules.

GCP

GCP helped to pioneer the use of Software Defined Networking (SDN), the application of machine learning to networking, and the development of large-scale management infrastructure including telemetry systems. Google owns its telecommunication services, and all data is encrypted between datacenters on Google-owned infrastructure. Both the server boards and the networking equipment are custom designed by Google. Google does not rely on internal network segmentation or firewalling as the primary security mechanisms, though it does use ingress and egress filtering at various points in the Google network to prevent IP spoofing as a further security layer.

Google utilizes a variety of isolation and sandboxing techniques for protecting a service from other services running on the same machine. These techniques include normal Linux user separation, language and kernel-based sandboxes, and hardware virtualization. GCP's VPC network is a virtual version of a physical network, implemented inside Google's production network. VPC networks, including their associated routes and firewall rules, are global resources. They are not associated with any region or zone. Subnets are regional resources, and each subnet defines a range of IP addresses.

Google applies Zero Trust principles to define network access. This shifts access controls from the perimeter to individual devices and users. Google has applied these principles to how it connects machines, workloads, and services in its cloud services. To make all this work requires configuration and a client security operations team that understands the granularity that Zero Trust demands. This means properly setting up virtual networks (VNets) that are then monitored by tools like Google Operations Suite (formerly Stackdriver). Google uses its strength in machine learning to offer recommendations to optimize configuration of cloud infrastructure and security settings. Unfortunately, many organizations may struggle with the in-house skills and resources needed to make this work.

Microsoft Azure

Microsoft Azure's Availability Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. To ensure resiliency, there is a minimum of three separate zones in all enabled regions. Within each datacenter, customers create Azure VNets, which are the fundamental building blocks of customer private networks in Azure. VNets enable many types of Azure resources, such as VMs, to communicate securely with each other, the internet, and on-premises networks. VNets are like traditional networks that customers would operate in their own datacenter but bring with them additional benefits of Azure's infrastructure such as scale, availability, and isolation.

To filter network traffic to and from Azure resources in an Azure VNet, customers use an Azure NSG. An NSG contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. A flow record is created for existing connections. Communication is allowed or denied based on the connection state of the flow record. The flow record also allows an NSG to be stateful. Customers only need to specify an inbound security rule if communication is initiated externally. If inbound traffic is allowed over a port, it is not necessary to specify an outbound security rule to respond to traffic over the port.

OCI

OCI is organized into localized geographic regions with each region having at least one availability domain (a unique datacenter). Each AD is further segmented into three fault domains to allow for further physical segmentation. Customers create virtual cloud networks (VCNs) within a region that enable all the resources deployed within them to communicate securely with each other, with other Oracle services, and with the internet. They closely resemble a traditional network, with firewall rules and specific types of communication gateways. Customers use subnets, security lists, and NSGs to filter traffic between resources. Security lists operate at the subnet level, whereas NSGs operate at the VNIC level, which allows for more fine-grained access control (microsegmentation) between resources and for separation of the customers' VCN subnet architecture from their application security requirements. Rules for security lists and NSGs can be either stateful or stateless.

Virtualization/Host

IaaS customers are primarily responsible for securing the hosts provisioned in the cloud (such as virtualization software security or virtual server security), while the IaaS provider is responsible for the underlying physical hardware layer and supporting hypervisor configuration. This means the customer assumes responsibility and management of the guest operating system (including updates and security patches).

Additionally, customer workloads are isolated, and each customer account is tied to resources the customer consumes. Most enterprise workloads run on Windows and Linux operating systems, while the Windows operating system has auto patching capabilities, and the Linux operating system requires scripting or third-party tools.

All CSP offerings are built on similar virtualization infrastructure with APIs, console, and web interfaces. They all offer some form of bare metal services; however, only AWS and OCI have full bare metal services. Oracle Autonomous Linux is the first of its kind and gives OCI the edge.

AWS

AWS offers AWS Organizations, Control Tower, and VPCs to isolate and manage customer accounts and workloads. These services allow customers to centrally manage billing; control access, compliance, and security; and share resources across their AWS accounts. Additionally, AWS offers bare metal instances that allow EC2 customers to run application workloads that require direct access to bare metal infrastructure. AWS Outposts is a fully managed service that extends AWS infrastructure, AWS services, APIs, and tools to virtually any datacenter, co-location space, or on-premises facility for a truly consistent hybrid experience.

AWS supports and maintains Amazon Linux for use on EC2. It is designed to provide a stable, secure, and high-performance execution environment for applications running on Amazon EC2. AWS Systems Manager Patch Manager automates the process of patching managed instances with both security-related and other types of updates. Customers can use Patch Manager to apply patches for both operating systems and applications.

GCP

GCP sits on top of Google's global infrastructure that is designed to provide security through the entire information processing lifecycle. GCP provides several isolation boundaries including projects, folders, and organizations, in addition to ACL and network-based controls. Google offers virtual separation of workloads between customers through very strong compartmentalization using GCP projects which hold one to many VPCs. All data is encrypted at rest and in transit. Google offers single-tenant bare metal servers in a limited set of datacenters.

GCP offers patch compliance reporting and patch deployment-as-a-service for VM instances across Windows and Linux distributions. The operating system patch management service has two main components. First is patch compliance reporting, which provides insights on the patch status of VM instances across Windows and Linux distributions. Along with the insights, users can also view recommendations for their VM instances. Second is patch deployment, which automates the operating system and patch update process. A patch deployment schedules patch jobs, which run across VM instances and apply patches.

Microsoft Azure

Microsoft Azure management groups, subscriptions, and VNets provide customer isolation. Azure Stack Hub is an extension of Azure that provides a way to run apps in an on-premises environment and deliver Azure services in the datacenter. Azure also has a purpose-built bare metal infrastructure to scale workloads, although SAP HANA only. Azure VMs are one of several types of on-demand, scalable computing resources that Azure offers. Typically, customers choose a VM when they need more control over the computing environment than the other choices offer. Azure partners provide Linux images in the Azure Marketplace.

OCI

Oracle built its cloud with what it describes as a new and security-first design that separates customer workloads from each other and from Oracle cloud management code. OCI takes virtualization of the network and disk IO out of the software stack and puts it in the network. This removes the requirement for hypervisors or any other CSP code to run on customer instances, if running on bare metal or dedicated servers. Oracle customers can run Compute and Database services on bare metal instances, which are customer-dedicated physical servers, or as VM instances, which are isolated computing environments on top of bare metal hardware. Tenancy and Compartments enable customers to organize and separate their workloads.

Oracle Autonomous Linux based on the Oracle Linux operating environment provides autonomous capabilities such as automated zero-downtime patching and known exploit detection, to help keep the operating system highly secure and reliable. Other advantages of the product include hardened configuration, continuous configuration checks, and threat monitoring. Used in conjunction with the Oracle OS Management Service (OSMS), it allows users to choose which of their servers to automate or control manually. OSMS enables users to automate capabilities that will execute common management tasks for Linux systems, including patch and package management and security and compliance reporting.

Bare metal and VM instances run on the same types of server hardware, firmware, underlying software, and networking infrastructure, so both instance types have OCI protections built into those layers. This flexibility means OCI offers not only virtual separation but also bare metal servers that can be housed either at an Oracle datacenter globally or at a customer datacenter utilizing the full benefits of OCI cloud architecture and services. The latter may provide unmatched performance, cost, and security benefits for some customers.

Identity and Access Management

Identity is perhaps the most critical component that the customer is accountable for within cloud security. Identity keeps the integrity and confidentiality of data and applications while making access readily available to authorized users. Support for these identity management capabilities, for both users and infrastructure components, is a major requirement for cloud computing, and identity should be managed in ways that build trust.

All CSPs provide granular identity and access control that support most, if not all, authentication options. Azure, however, has a more user-friendly interface (Azure AD) that provides a look and feel like that of Microsoft Active Directory.

AWS

AWS IAM enables users to manage access to AWS services and resources securely. IAM enables customers to create and manage AWS users and groups, and permissions can be used to allow and deny access to AWS resources. IAM is a feature of every AWS account offered at no additional charge. Access in AWS is managed by creating policies and attaching them to IAM identities (users, groups of users, or roles) or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines permissions. AWS evaluates these policies when an IAM principal (user or role) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. AWS supports six types of policies: identity-based policies, resource-based policies, permissions boundaries, Organizations SCPs, ACLs, and session policies.

AWS IAM services include an access advisor feature to assist customers in implementing least privilege. For example, developers may be granted broad access to get up and running quickly but, as a project progresses, these permissions will need to be limited to only what they need. Access advisor will determine the permissions that developers have used by analyzing the last timestamp when an IAM entity (a user, role, or group) accessed an AWS service. This information helps customers audit service access, remove unnecessary permissions, and set appropriate permissions across different environments.

GCP

GCP Cloud IAM lets administrators authorize who can act on specific resources, giving full control and visibility to manage Google Cloud resources centrally. For enterprises with complex organizational structures, hundreds of workgroups, and many projects, Cloud IAM provides a unified view into security policy across the entire organization, with built-in auditing to ease compliance processes. IAM allows granular access to specific GCP resources and prevents unwanted access to other resources. It is based on the security principle of least privilege, as to enable only the necessary access required to manage resources.

IAM provides a single access control interface with fine-grained control, automated access control recommendations, and context-aware access free of charge. GCP also offers a wide variety of multifactor verification methods such as push notifications, Google Authenticator, phishing-resistant Titan Security Keys, and use of Android or iOS devices as a security key.

Cloud IAM uses Recommender (a free Google service) to compare project-level role grants with the permissions that each member used during the past 90 days. If a project-level role is granted to a member, and that member does not use all that role's permissions, then Recommender is likely to suggest that the role be revoked, and fewer permissions are allowed. Google's Cloud IAM offers benefits over rival providers when organizations lack formal audit policy and procedures for account management.

Microsoft Azure

Azure AD is Microsoft's cloud based IAM service, which helps employees sign in and access internal resources, such as apps on the corporate network and intranet, along with any cloud apps developed by their organization. It can also be used for external resources, such as Microsoft Office 365, the Azure portal, and thousands of other software-as-a-service (SaaS) applications.

The free tier of Azure AD provides Azure customers with core IAM features such as single sign-on, user and groups provisioning and management, multifactor authentication, device registration, and cloud authentication.

Customers who choose to upgrade to premium tiers (P1 and P2) get access to add-ons such as group-based access management, support for on-premises apps, and Azure AD Identity Protection to help provide risk-based Conditional Access to apps and critical company data and Privileged Identity Management to help discover, restrict, and monitor administrators and their access to resources and to provide just-in-time access when needed. These features provide a smoother lift-and-shift of on-premises resources to Azure. Identity Protection is one of several features added when a customer upgrades to the Premium P2 tier. It is not an a-la-carte upgrade option, however.

For customers who are interested in running an instance of AD in the cloud to support traditional AD features such as domain joins and group policies, Azure offers a service called Azure AD Domain Services.

OCI

OCI offers compartments and IAM policies to control access to the cloud network. OCI's IAM features are robust and secure by default. Users have no access to OCI resources until privileges are assigned via group membership (Zero Trust). As an important differentiator for Oracle, only groups get assigned access rights. Customers can ensure secure access with native multifactor authentication, assign users to groups based on role, and assign privileges to groups using simple, easy-to-understand policies. OCI's native IAM also provides basic federation capabilities out of the box. Additionally, at a cost, Oracle offers commercial identity solutions, including its capable cloud-based Identity Cloud Service, which provides hybrid identity management capabilities.

OCI tenant (Oracle account) administrators can manage access to OCI resources via compartments (a compartment is a collection of cloud assets, like compute instances, load balancers, databases, etc.). Within tenancies, compartments ensure strong security boundaries among business units, projects, or applications. This amounts to greater control, improved security, and easier management.

Another unique advantage of OCI is its SQL-like syntax for managing IAM policies. All parts of OCI can be access-controlled via these policies, which make programmatic management of IAM policies easier at scale.

A global retail chain chose OCI for disaster recovery, citing OCI's comprehensive security that includes the following: OCI's fine-grained IAM policies controlling access within databases, compartments for isolating different resources, and federation from on-premises AD for better control over users. Meanwhile, a SaaS provider in the construction sector chose OCI for segmentation via compartments. "This ensures every customer is deployed to its own compartment, with very strong isolation between each SaaS customer," explained its head of IT security.

Security Posture Management

Emerging and perpetual changes in the cloud make it arduous to keep track of whether customer data is stored appropriately. As cloud infrastructure grows and changes dynamically, the need to track and protect against misconfigurations must occur in tandem. Cloud security posture management should enable monitoring of configuration changes with some level of automation of policy enforcement. This includes queries that are run periodically, along with features enabled for automatic alerting to allow for manual or automated remediation of misconfigurations as they occur.

AWS

AWS offers a set of security tools typically bought separately to manage vulnerabilities. Many of these tools feed into the AWS Security Hub, which provides a comprehensive view of high-priority security alerts and security posture across AWS accounts. The suite of tools includes Amazon GuardDuty, a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect AWS accounts and workloads; Amazon Macie, a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS S3 Buckets; and Amazon Inspector, an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. CloudWatch agents can also be installed on servers on-premises and in the cloud, allowing customers to conduct performance monitoring.

The AWS Config service provides configuration management for EC2 instances, an Elastic Block Store volume, an Elastic Network Interface, or a security group. It keeps track of the configurations of all the AWS resources associated with an AWS account. This allows customers to get current and historical configurations of each AWS resource and information about the relationship between the resources. They can use the service to identify and roll back unauthorized changes. Additionally, the AWS Config automatic remediation feature allows users to apply remediation actions with AWS Config rules and choose to execute them automatically to address noncompliant resources without manual intervention. AWS Config rules are configured by the customer using AWS Lambda functions. Both the AWS Config and AWS Config Rules features come at a cost.

AWS VPC Flow Logs enables customers to capture information about the IP traffic going to and from network interfaces in a VPC. Flow log data can be published to Amazon CloudWatch Logs or Amazon S3. After a flow log is created, users can retrieve and view its data in the chosen destination. AWS Flow Logs can be enabled at the VPC, subnet, or network interface level. Flow logs are pushed immediately following the sampling window. They do not capture all IP traffic, including queries to the Amazon DNS server, DHCP traffic, and 69.254.169.254 instance metadata. Even with a flow log sampling of 1.0 or 100%, at most about 10% of packets at the VM level are processed due to the initial sample rate limitation.

GCP

Google offers many tools and services for monitoring, like VPC flow logs, which must be bought separately, and tools like its operations suite (formerly Stackdriver), which is designed to monitor, troubleshoot, and improve cloud infrastructure, software, and application performance.

These tools provide a great deal of information but are not prescriptive. Teams must annually set them up. GCP does not offer secure configuration enforcement for customer workloads other than alerts through the operations suite. Customers have used tools like Terraform to enforce known secure configurations. GCP offers VPC flow logs that include fields such as source and destination IP, source and destination port, protocol, and so forth. This is an excellent log for detecting port scans or anomalous behavior within Google's VPC network and is recommended to be enabled at full (100%) sampling rate. This could create a large amount of data, and it is worth the extra storage to gain full visibility into the customer's environment. If storage is an issue, the alternative is to enable full logging on specific subnets of the network. Again, this is something the customer must set up, which Google highly recommends.

Microsoft Azure

Azure offers Security Center, a consolidated dashboard for monitoring the environment. The Security Center service is a unified infrastructure security management system that provides advanced threat protection across hybrid workloads in the cloud—whether they are in Azure or not—as well as on-premises. Data is collected from virtual and physical servers using the Log Analytics agent, which reads various security-related configurations and event logs from the machine and copies the data to a user's workspace for analysis. The integrated dashboard provides a single view of identified threats and scores vulnerabilities in the environment to aid remediation efforts. Azure Security Center monitors for vulnerabilities on both IaaS and PaaS servers and is used to manage security policy and compliance.

Azure Policy evaluates resources in Azure by comparing the properties of those resources to business rules. These business rules must be manually configured by the customer, and their responses for handling noncompliance are the following: (a) deny the resource change, (b) log the change to the resource, (c) alter the resource before the change, (d) alter the resource after the change, and (e) deploy related compliant resources.

Azure's VNet uses the NSG flow logs feature of Azure Network Watcher for the logging of information about IP traffic flowing through an NSG. This allows customers to log the source and destination IP address, port, protocol, and whether traffic was allowed or denied by an NSG. Flow logs are enabled at the VNet/subnet level. Flow data is sent to Azure Storage accounts, from where users can access it, as well as export it to any visualization tool, SIEM, or IDS.

OCI

OCI Cloud Guard is a unified security solution that provides a global, centralized approach to the protection of all the customer's assets. It works to analyze data, detect threats and misconfigurations, and automatically provide multiple options for dealing with these challenges including automated remediation. Cloud Guard continuously collects data from every part of the infrastructure and application stack, including audit logs, Oracle Data Safe, and Oracle OSMS. It proactively detects and reports security problems and can be configured to remediate them automatically to stop anomalous activity it identifies. Cloud Guard gives Oracle an edge without the need for additional third-party services, as security posture can be automated to enforce preset configurations without any human intervention or additional cost.

OCI also offers Security Zones, which are defined at the compartment level where security is mandatory and always on. Customers effectively lock down resources to known secure

configurations, automatically prevent configuration changes, and continuously monitor and block anomalous activities. This automatically removes the need for constant analysis that would otherwise require labor-intensive and error-prone work. Oracle provides preconfigured mandatory security best practices for critical production workloads, which helps eliminate customer misconfiguration.

> "The simplicity of OCI's environment has enabled us to spin-up new environment and patch or update new images with the click of a button. It provides the stringent security we need to maintain global operations and comply with extremely strict audit compliance regulations."
>
> *Senior Director of Operations for Global Nonprofit*

OCI's VCN Flow Logs keeps detailed records of every flow that passes through the VCN and sends the data to OCI's logging service. The data includes information about the source and destination of the traffic, along with the quantity of traffic and the "permit" or "deny" action taken, based on network security rules. VCN Flow Logs currently do not collect Load Balancer logs.

"Azure presents the picture to you, but OCI Cloud Guard presents the picture and automatically fixes any problems, reducing mean-time-to-deliver and recover. AWS requires far more effort to gain insight into the environment," says a U.S. Government chief information security officer.

"The simplicity of OCI's environment has enabled us to spin-up new environment and patch or update new images with the click of a button. It provides the stringent security we need to maintain global operations and comply with extremely strict audit compliance regulations," says a senior director of operations at a global nonprofit organization.

Data Security

In the traditional datacenter, controls on physical access, access to hardware and software, and identity controls all combine to protect the data. In the cloud, that protective barrier that secures infrastructure is diffused. The data needs its own security. These controls should include encryption, data isolation, classification, rights management, and strong role-based access to data stores. All four cloud providers have a complete set of controls for ensuring encryption for data in use, in transit, and at rest. The difference is between native controls and additional costs of third-party tools. Oracle cloud, for example, includes additional features that are not available for Oracle databases deployed on other cloud platforms. It also includes security features such as full database encryption, internal access controls, security assessments, user risk scoring, and data masking.

AWS

AWS provides disk-level encryption to protect data at rest. Additionally, AWS provides support for object storage, file storage, and block storage services at a cost. For object storage, Amazon S3 encrypts each object with a unique key and encrypts the key itself with a master key that it

rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available to encrypt data—256-bit Advanced Encryption Standard (AES-256). AWS NoSQL service DynamoDB encrypts by default all data at rest. Customers can use the default encryption, the AWS-owned customer master key (CMK), or the AWS-managed CMK to encrypt all their data. DynamoDB now has added support to enable users to switch encryption keys between the AWS-owned CMK and AWS-managed CMK, without having to make any code or application modifications; however, encryption must be enabled on AWS Aurora RDS. Additionally, AWS offers nonproprietary RDS services (including Oracle and Microsoft SQL Server) and NoSQL services that utilize native database encryption, which varies depending on versions and licensing.

AWS KMS makes it easy to create and manage cryptographic keys and control their use across a wide range of AWS services and in applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under Federal Information Processing Standard (FIPS) 140-2, or are in the process of being validated, to protect keys. AWS KMS is integrated with AWS CloudTrail to provide logs of all key usage to help meet regulatory and compliance needs.

AWS secures data in transit within the AWS network using TLS and SSL. AWS will update all its AWS FIPS endpoints to a minimum TLS version of TLS 1.2 over the next year. This update will deprecate the ability to use TLS 1.0 and TLS 1.1 on all FIPS endpoints across all AWS Regions by March 31, 2021. No other AWS endpoints are affected by this change.

GCP

GCP's infrastructure provides a variety of storage services, such as BigTable and Spanner, and a central KMS. Most applications at Google indirectly access physical storage via these storage services, which can be configured to use keys from the central KMS to encrypt data before it is written to physical storage. This KMS supports automatic key rotation, provides extensive audit logs, and links keys to end users. Performing encryption at the application layer allows the infrastructure to isolate itself from potential threats at the lower levels of storage, such as malicious disk firmware. The infrastructure also implements additional layers of protection, like disk-level encryption.

GCP protects data if communications are intercepted while data moves between the customer site and the cloud provider or between two services. Google Cloud services accepts requests from around the world using its globally distributed system GFE. GFE terminates traffic for incoming HTTP(S), TCP, and TLS proxy traffic, provides DDoS attack countermeasures, and routes and load-balances traffic to Google Cloud services.

SSL policies provide the ability to control the features of SSL that Google Cloud SSL proxy load balancer or external HTTP(S) load balancer negotiates with clients. By default, HTTP(S) Load Balancing and SSL Proxy Load Balancing use a set of SSL features that provides good security and wide compatibility. Some applications require more control over which SSL versions and ciphers are used for their HTTP(S) or SSL connections. Customers can define SSL policies to control the features of SSL that a load balancer negotiates with clients.

Microsoft Azure

Microsoft Azure offers a variety of data storage solutions to meet different needs, including file, disk, blob, and table storage. Users can protect Windows and Linux VMs by using Azure disk encryption, which uses Windows BitLocker technology and Linux DM-Crypt to protect both operating system disks and data disks with full volume encryption. Data at rest in Azure Blob storage and Azure file shares can be encrypted in both server-side and client-side scenarios.

Azure Storage Service Encryption can automatically encrypt data before it is stored, and it automatically decrypts the data when users retrieve it. The process is completely transparent to users. Storage Service Encryption uses 256-bit AES encryption, which is one of the strongest block ciphers available. AES handles encryption, decryption, and key management transparently.

Azure SQL Database supports both server-side encryption via the TDE feature and client-side encryption via the Always Encrypted toolkit. TDE protects data and log files, using AES and Triple Data Encryption Standard encryption algorithms. Encryption of the database file is performed at the page level. The pages in an encrypted database are encrypted before they are written to disk and are decrypted when they are read into memory. TDE is now enabled by default on newly created Azure SQL databases, and Azure Cosmos DB is encrypted by default and cannot be disabled. Additionally, Azure offers nonproprietary RDS services that utilize native database encryption that vary in cost based on the database version.

Azure secures data in transit within the network using TLS and SSL. Beginning September 1, 2020, Azure Automation will enforce TLS 1.2 or later versions for all external HTTP(S) endpoints, and Microsoft recommends customers ensure all clients are ready to handle TLS 1.2 or later. TLS and SSL are cryptographic protocols that provide communications security over a computer network. Older versions of TLS/SSL have been found to be vulnerable and, while they still currently work to allow backward compatibility, they are not recommended, and the industry is quickly moving to abandon support for these older protocols.

OCI

The Oracle database supports several security mechanisms that are not available in other databases. This includes Database Vault, Label Security, and Real Application Security, all of which are included in Oracle Database cloud services. Oracle implements encryption inside the database, so protections remain for backups, archives, moves, and copies. Encrypted data is also protected in temporary tablespaces, undo segments, and redo logs and during internal database operations such as JOIN and SORT. Oracle Autonomous Database features auto-enforced encryption and audit alongside other automatically locked-down configurations, including disallowed high-risk actions, enforced Separation of Duties between admins and data, and automated patching and upgrades. Oracle Data Safe adds a layer of automated, centralized security. Security Assessments analyzes database configurations, user accounts, and security controls and reports on findings with recommendations for remediation. User Assessments also analyzes user security to identify high-risk users and assigns a risk score to each user. Sensitive Data Discovery, which can be tailored to specific needs, inspects data, and returns lists of sensitive columns. Data Masking removes sensitive data so that data sets are safe for nonproduction use. And Activity Auditing monitors user activity and flags unusual database activities.

The OCI Vault service provides centralized management of the encryption keys that protect data and the secret credentials that are used to access resources securely. The Vault service can be integrated with all OCI services and is used to create and manage vaults, keys, and secrets.

OCI storage services (such as Local NVMe SSD, Block Volumes, and Object Storage) are all encrypted at rest by default using the AES 256 encryption algorithm. For customer tenant data, OCI uses encryption both at rest and in transit. The Block Volumes and Object Storage services enable at-rest data encryption by default, by using the AES algorithm with 256-bit encryption. In-transit control plane data is encrypted by using TLS 1.2 or later.

Conclusion

Amazon was the first to market with an IaaS platform, and it did not take long for Microsoft and Google to quickly follow. For better or worse, this means that design decisions on how to architect and provide cloud services are consistent across all three platforms, and security was not a primary driver.

Oracle Cloud is a latecomer to the IaaS market and, although being late could appear to be a disadvantage versus the other three cloud providers, Oracle capitalized on observing and understanding the risks of existing IaaS platforms when designing OCI's security features.

> "Automated protections such as what Oracle Cloud Guard offers can become a game changer, as they reduce the risk to critical workloads and having to depend on knowledgeable staff and hard-to-find skillsets to keep your data secure".
>
> *President of Mobile Applications Development Firm*

Building OCI from scratch allowed Oracle to make some differentiated decisions in how it designed infrastructure, the network, and the software platform.

Maturity, however, does have its advantages: mainly in support of third-party vendors and the innovation they provide to existing and well-known cloud platforms. This is a strength of Amazon first, followed by Microsoft, and then Google. Because of this third-party support, it is possible for any organization to meet its security and compliance requirements with the implementation of layers of tools.

AWS has broad industry support and critically strong developer experience and support. This is perhaps its biggest advantage. Azure, based on decades of enterprise and security experience at Microsoft, is well thought out for meeting industry compliance and enterprise threat detection monitoring. Google, which entered the market later than Amazon and Microsoft, has focused on being cost effective and more open than other cloud providers while leveraging machine-learning techniques for automation.

The disadvantage of these older platforms is the need for additional layers of security—that is, there is an additional cost and complexity to ensuring a secure environment. These extra layers have also led to configuration mistakes being a core problem in IaaS deployments. For example, Capital One, leveraging AWS, was compromised with only three administrative commands using a temporary administrative token. This is an easy oversight to make for even the most security-first organizations.

One big differentiator among cloud platforms is bare metal. In addition to the performance benefits of dedicated hardware, bare metal closes a huge potential security hole of shared vulnerabilities from neighbor virtual instances. AWS launched bare metal instances in late 2017. Azure and Google announced bare metal last year, and Google is only making it available in the

summer of 2020. Interestingly, OCI took the opposite direction, starting with bare metal and then moving to virtual instances. Its cloud infrastructure services were designed from the start for high-performance workloads.

Another big differentiator among providers is the SDN that is capable of both Layer 2 and Layer 3 networking. The SDN for Oracle is a flat, nonblocking, non-oversubscribed virtual relay network designed to scale. Additionally, for OCI, there are no virtualization agents on the servers, which the SDN accesses strictly at Layer 2.

While Oracle IaaS shows strengths in the fundamental design of services, it is still behind on platform adoption and support from third-party vendors. However, the extension of OCI with Oracle Cloud Guard, Security Zones, and Dedicated Regions gives Oracle superior native security capabilities without the uptick in costs for services like centralized security configuration and posture management and automated enforcement of security practices. These services are free, as is Oracle Data Safe for securing Oracle Cloud databases.