A guide to securing cloud platforms

Key takeaways

1 Ideally, a cloud provider should be able to integrate your company's identity management system into their platform—and in any case provide a trustworthy identity management solution for you to use as needed.

2 As part of establishing trust, verify that a cloud platform offers well-integrated firewalls, security groups, and options for micro-segmentation based on workload and trusted compute hosts.

3 Expect cloud providers to offer BYOK solutions that allow your organization to exclusively manage keys across all data storage and services.

4 The best security practice for containers is to scan them for vulnerabilities both before deployment and while they are running.

5 Cloud platform security must effectively control access, operate at the level of workloads, track activity in detail and integrate into on-premises systems.

Rethink security for cloud-based applications

As more organizations move to a cloud-native model for developing apps and managing workloads, cloud computing platforms are rapidly limiting the effectiveness of the traditional perimeter-based security model. While still necessary, perimeter security is by itself insufficient. Because data and applications in the cloud are outside the old enterprise boundaries, they must be protected in new ways.

Organizations transitioning to a cloud-native model or planning hybrid cloud app deployments must supplement traditional perimeter-based network security with technologies that protect cloud-based workloads. Enterprises must have confidence in how a cloud service provider secures their stack from the infrastructure up. Establishing trust in platform security has become fundamental in selecting a provider.

Cloud security drivers

Data protection and regulatory compliance are among the main drivers of cloud security—and they're also inhibitors of cloud adoption. Addressing these concerns extends to all aspects of development and operations. With cloud-native applications, data may be spread across object stores, data services and clouds, which create multiple fronts for potential attacks. And attacks are not just coming from sophisticated cybergangs and external sources; according to a recent survey, 53 percent of respondents confirmed insider attacks in the previous 12 months.[1]

Five fundamentals of cloud security

As organizations address the specialized security needs of using cloud platforms, they need and expect their providers to become trusted technology partners. In fact, an organization should evaluate cloud providers based on these five aspects of security as they relate to the organization's own specific requirements:

1. **Identity and access management:** Authentication, identity and access controls
2. **Network security:** Protection, isolation and segmentation
3. **Data protection:** Data encryption and key management
4. **Application security and DevSecOps:** Including security testing and container security
5. **Visibility and intelligence:** Monitoring and analyzing logs, flows and events for patterns

Verify identity and manage access on a cloud platform

Any interaction with a cloud platform starts with verifying identity, establishing who or what is doing the interacting—an administrator, a user or even a service. In the API economy, services take on their own identity, so the ability to accurately and safely make an API call to a service based on this identity is essential to successfully running cloud-native apps.

Look for providers that offer a consistent way to authenticate an identity for API access and service calls. You also need a way to identify and authenticate end users who access applications hosted in the cloud. As an example, IBM® Cloud uses App ID as a way for developers to integrate authentication into their mobile and web apps.

Strong authentication keeps unauthorized users from accessing cloud systems. Since platform identity and access management (IAM) is so fundamental, organizations that have an existing system should expect cloud providers to integrate their company's identity management system. This is often supported through identity federation technology that links an individual's ID and attributes across multiple systems.

Why authenticate service calls?

In microservices-based architectures, APIs enable applications to communicate and share data. When an application runs, it uses APIs to call up services as needed to complete various operations. For example, your application might call an object store service for data. As part of fulfilling the request, the object store service itself might then call a key management service to get the encryption keys needed to decrypt the data. And as part of delivering its user experience, an app might use APIs to access user identity information, post content between apps (such as posting content from an app to Twitter), and determine a user's location to serve up location-specific information. **All of these integration points pose security challenges.**

Cloud providers should have a consistent way to authenticate the identity of a user or a service that needs to access an API or a service. Of course, as part of authentication, all access request sessions and transactions should be logged for auditing purposes. **APIs and services most likely hold valuable intellectual property; you don't want just anyone using them.**

Ask prospective cloud providers to prove that their IAM architecture and systems cover all the bases. In the IBM Cloud, for example, identity and access management is based on several key features (Figure 1):

Identity

- Each user has a unique identifier
- Services and applications are identified by their service IDs
- Resources are identified and addressed by the cloud resource name (CRN)
- Users and services are authenticated and issued tokens with their identities

Access management

- As users and services attempt to access resources, an IAM system determines whether access and actions are allowed or denied
- Services define actions, resources and roles
- Administrators define policies that assign users roles and permissions on various resources
- Protection extends to APIs, cloud functions and back-end resources hosted on the cloud

As you evaluate a cloud provider's security, look for access control lists together with common resource names that enable you to limit users not only to certain resources, but also to certain operations on those resources. These capabilities help ensure that your data is protected from both unauthorized external and internal access.

Extending your own Enterprise Identity Provider (Enterprise IdP) to the cloud is particularly useful when you build a cloud-native app on top of an existing enterprise application that uses the Enterprise IdP. Your users can smoothly log in to both the cloud-native and underlying applications without having to use multiple systems or IDs. Reducing complexity is always a worthy goal.

Key takeaway

Ideally, a cloud provider should be able to integrate your company's identity management system into their platform—and in any case provide a trustworthy identity management solution for you to use, as needed.

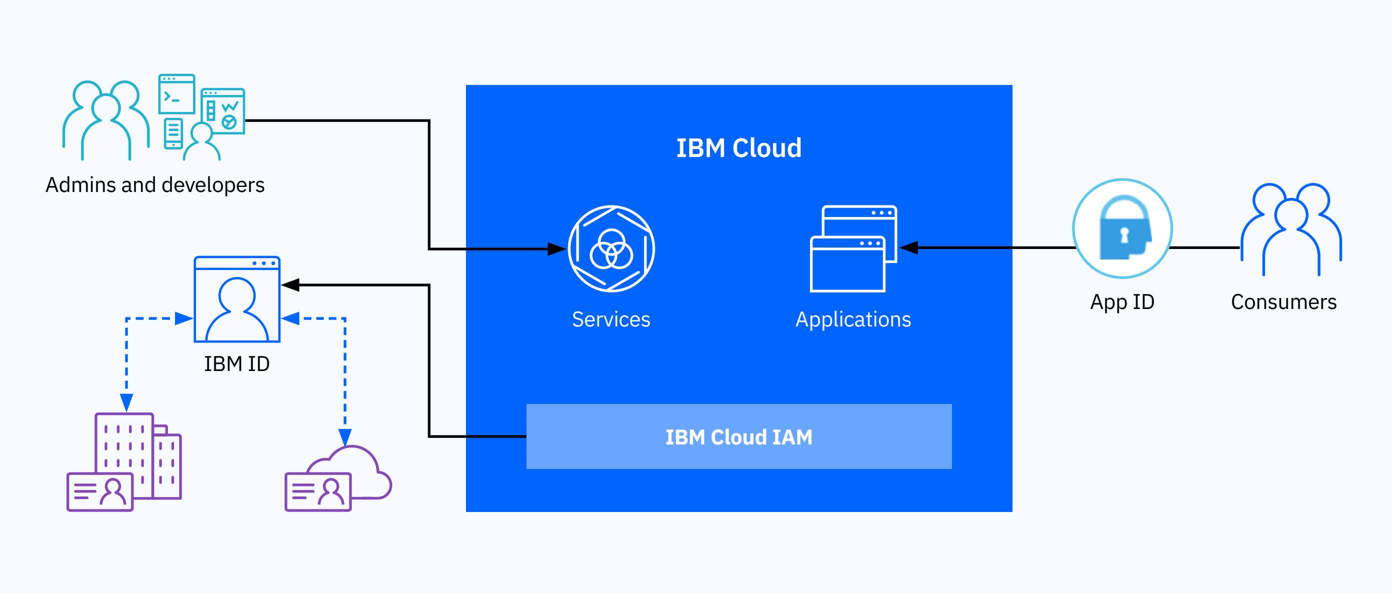

Figure 1. Separation of provider-managed and customer-managed cluster elements.

Redefine network isolation and protection

Many cloud providers use network segmentation to limit access to devices and servers in the same network. Additionally, providers create virtual isolated networks on top of the physical infrastructure and automatically limit users or services to a specific isolated network. These and other basic network security technologies are table stakes for establishing trust in a cloud platform.

Cloud providers offer protection technologies—from web application firewalls to virtual private networks and denial-of-service mitigation—as services for software-defined network security and charge per usage. Consider the following technologies as crucial network security in the cloud computing era.

Security groups and firewalls

Cloud customers often insert network firewalls for perimeter protection (virtual private cloud/subnet-level network access) and create network security groups for instance-level access. Security groups are a good first line of defense for assigning access to cloud resources. You can use these groups to easily add instance-level network security to manage incoming and outgoing traffic on both public and private networks.

Many customers require perimeter control to secure perimeter network and subnets, and virtual firewalls are an easily deployable way to meet this need. Firewalls are designed to prevent unwanted traffic from hitting servers and to reduce the attack surface. Expect cloud providers to offer both virtual and hardware firewalls that allow you to configure permission-based rules for the entire network or subnets.

VPNs, of course, provide secure connections from the cloud back to your on-premises resources. They are a must-have if you are running a hybrid cloud environment.

Micro-segmentation

Developing applications cloud-natively as a set of small services provides the security advantage of being able to isolate them using network segments. Look for a cloud platform that implements micro-segmentation through the automation of network configuration and network provisioning. **Containerized applications architected on the microservices model are fast becoming the norm to support workload isolation that scales.**

Key takeaway

As part of establishing trust, verify that a cloud platform offers well-integrated firewalls, security groups, and options for micro-segmentation based on workload and trusted compute hosts.

Protect data with encryption and key management

Reliably protecting data is a security fundamental for any digital business—especially those in highly regulated industries such as financial services and healthcare.

Data associated with cloud-native applications may be spread across object stores, data services and clouds. Traditional applications may have their own database, their own VM and sensitive data located in files. In these cases, encryption of sensitive data both at rest and in motion becomes critical.

Businesses are right to worry about cloud operators or other unauthorized users accessing their data without their knowledge, and to expect complete visibility into data access. **Controlling access to data with encryption and also controlling access to encryption keys are becoming expected safeguards.** As a result, a bring-your-own-keys (BYOK) model is now a cloud security requirement. It allows you to manage encryption keys in a central place, provides assurance that root keys never leave the boundaries of the key management system and enables you to audit all key management lifecycle activities (Figure 2).

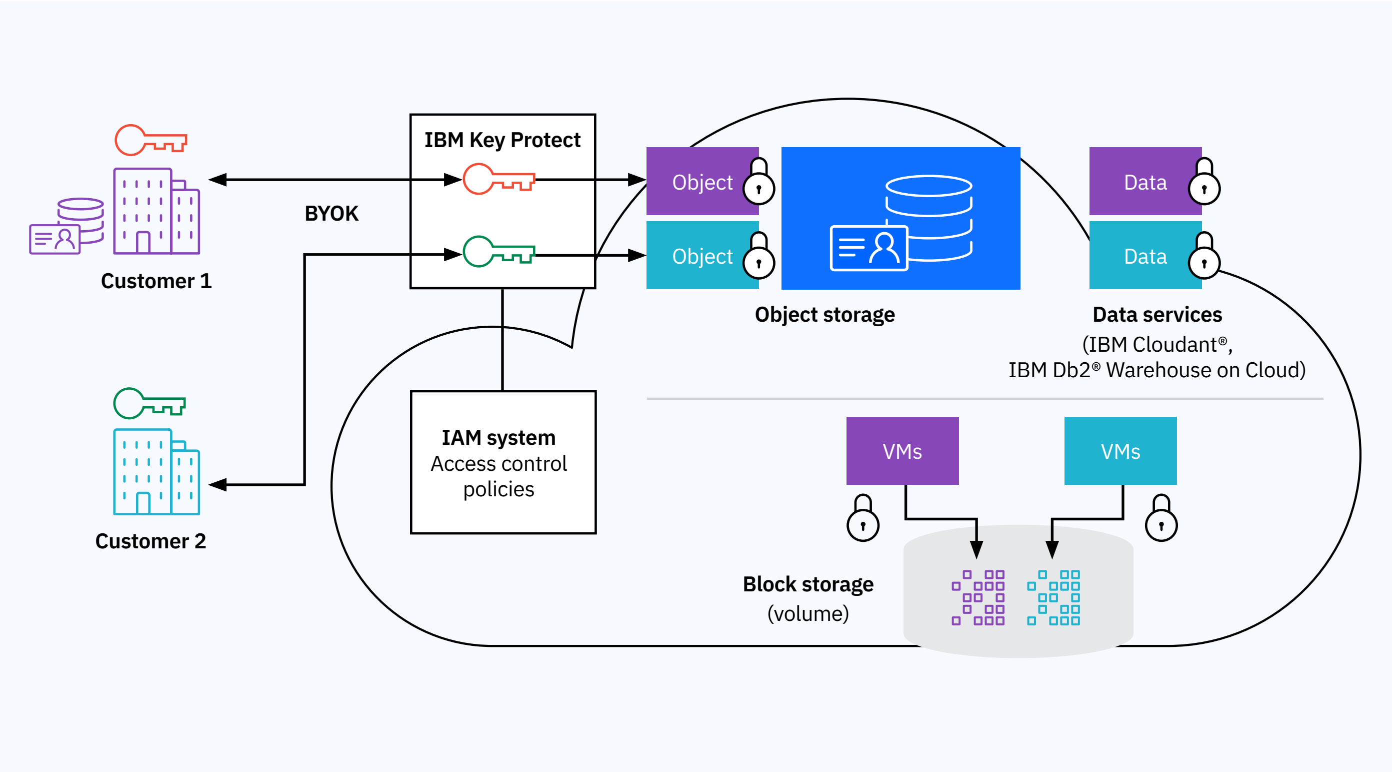

Figure 2. Architecture of a BYOK solution.

Trusted compute hosts

It comes down to hardware: nobody wants to deploy valuable data and applications on an untrusted host. Cloud platform providers that offer hardware with measure-verify-launch protocols give you highly secure hosts for applications deployed within the container orchestration system.

Intel Trusted Execution Technology (Intel TXT) and Trusted Platform Module (TPM) are examples of host-level technologies that enable trust for cloud platforms. Intel TXT defends against software-based attacks aimed at stealing sensitive information by corrupting system or BIOS code, or by modifying the platform's configuration. Intel TPM is a hardware-based security device that helps protect the system startup process by ensuring that it is tamper-free before releasing system control to the operating system.

Data protection at rest and in transit

Built-in encryption with BYOK lets you maintain control of your data, whether it's based on premises or in the cloud. It's an excellent way to control access to data in cloud-native application deployments. In this approach, the customer's key management system generates a key on premises and passes it to the provider's key management service. This approach encompasses data-at-rest encryption across storage types such as block, object and data services.

For data in transit, secure communication and transfer take place over Transport Layer Security/Secure Sockets Layer (TLS/SSL). TLS/SSL encryption also allows you to demonstrate compliance, security and governance without requiring administrative control over the cryptosystem or infrastructure. The ability to manage SSL certificates is a requirement for trust in a cloud platform.

Meeting audit and compliance needs

Providing your own encryption keys and keeping them in the cloud—with no service provider access—gives you the visibility and control of information required for CISO compliance audits.

Key takeaway

Expect cloud providers to offer BYOK solutions that allow your organization to manage keys across all data storage and services.

Automate security for DevOps

As DevOps teams build cloud-native services and work with container technologies, they need a way to integrate security checks within an increasingly automated pipeline. Because sites such as Docker Hub promote open exchange, developers can easily save image preparation time by simply downloading what they need. But with that flexibility comes the need to routinely inspect all container images placed in a registry before they are deployed.

An automated scanning system helps ensure trust by searching for potential vulnerabilities in your images before you start running them. Ask platform vendors if they allow your organization to create policies (such as “do not deploy images that have vulnerabilities” or “warn me prior to deploying these images into production”) as part of DevOps pipeline security.

IBM Cloud Container Service, for example, offers a Vulnerability Advisor (VA) system to provide both static and live container scanning. VA inspects every layer of every image in a cloud customer’s private registry to detect vulnerabilities or malware before image deployment. Because simply scanning registry images can miss problems such as drift from static image to deployed containers, VA also scans running containers for anomalies. It also provides recommendations in the form of tiered alerts.

Key takeaway

The best security practice for containers is to scan them for vulnerabilities both before deployment and while they are running.

Other VA features that help automate security in the DevOps pipeline include:

- **Policy violation settings:** With VA, administrators can set image deployment policies based on three types of image failure situations: installed packages with known vulnerabilities; remote logins enabled; and remote logins enabled with some users who have easily guessed passwords.
- **Best practices:** VA currently checks 26 rules based on ISO 27000, including settings such as password minimum age and minimum password length.
- **Security misconfiguration detection:** VA flags each misconfiguration issue, provides a description of it and recommends a course of action to remediate it.
- **Integration with IBM X-Force®:** VA pulls in security intelligence from five third-party sources and uses criteria such as attack vector, complexity and availability of a known fix to rate each vulnerability. The rating system (critical, high, moderate or low) helps administrators quickly understand the severity of vulnerabilities and prioritize remediation.

When it comes to remediation, VA does not interrupt running images for patching. Instead, IBM remediates the “golden” image in the registry and deploys a new image to the container. This approach helps ensure that all future instantiations of that image will have the same fix in place. VMs can still be handled traditionally, using an endpoint security service to patch VMs and fix Linux security vulnerabilities.

Kubernetes spoken here

If your DevOps teams work with the popular Kubernetes container orchestration software, ensure they can continue using their preferred tools. Also, evaluate how easily a platform provisions new and manages existing Kubernetes clusters.

Ask if a cloud platform provider supports Calico and Istio with its Kubernetes system. Calico and Istio are two important components of Kubernetes that help with application and workload security. Calico helps simplify management of IP addresses assigned to the workloads in a compute node, and programs access control lists in each compute node to enforce security policies. Using policy definitions set up and enforced through configuration labels, Istio provides certificate-based control of communication among microservices within a Kubernetes pod or cluster.

Create a security immune system through intelligent monitoring

When moving to the cloud, CISOs often worry about low visibility and loss of control. Since the organization's entire cloud may go down if a particular key is deleted or a configuration change inadvertently severs a connection back to on-premises resources or an enterprise security operations center (SOC), why shouldn't the operations engineers expect full visibility into cloud-based workloads, APIs, microservices—everything?

Access trails and audit logs

All user and administrative access, whether by the cloud provider or your organization, should be logged automatically. A built-in cloud activity tracker can create a trail of all access to the platform and services, including API, web and mobile access. Your organization should be able to consume these logs and integrate them into your enterprise SOC.

Enterprise security intelligence

Make sure you have the option of integrating all logs and events into your on-premises security information and event management (SIEM) system (Figure 3). Some cloud service providers also offer security monitoring with incident management and reporting, real-time analysis of security alerts and an integrated view across hybrid deployments.

IBM QRadar®, for example, is a comprehensive SIEM solution offering a set of security intelligence solutions that can grow with an organization's needs. Its machine learning capabilities train on threat patterns in a way that builds up a predictive security immune system.

Managed security with expertise

If your organization does not have significant security expertise, explore providers that can manage security for you. Some providers can monitor your security incidents, apply threat intelligence from a variety of industries and correlate this information to take action. Ask if they can also deliver a single pane of glass that integrates in-house and managed security services.

Key takeaway

Cloud platform security must effectively control access, operate at the level of workloads, track activity in detail and integrate into on-premises systems.

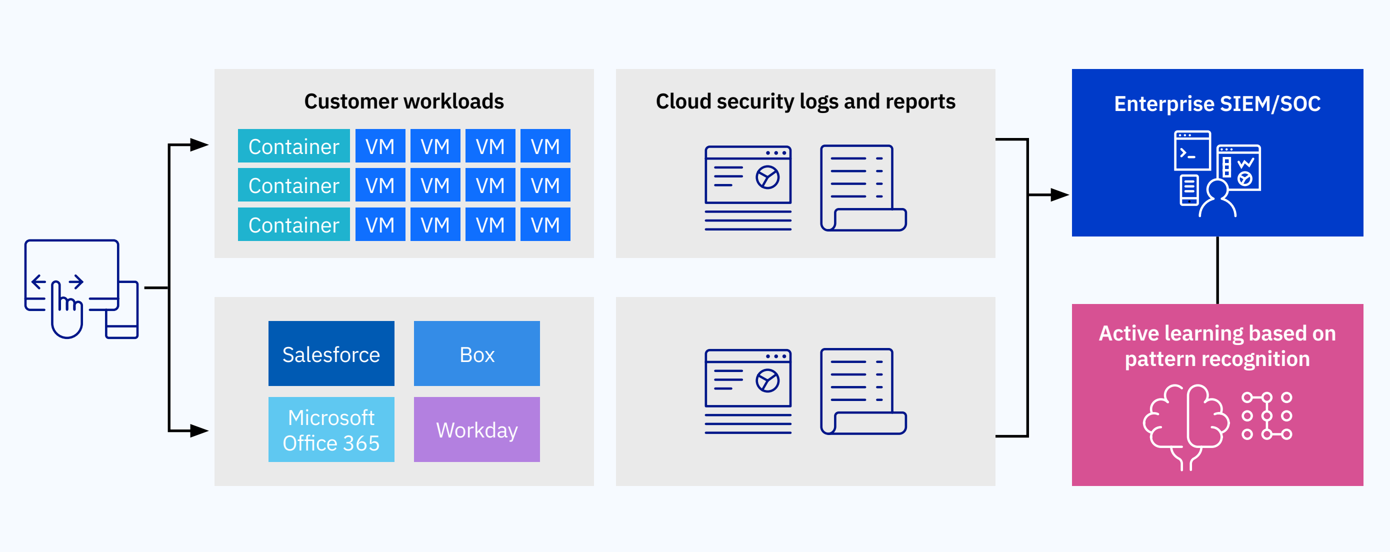

Figure 3. Integrating cloud visibility into an enterprise SIEM/SOC.

Security that promotes business success

With cloud technology becoming a larger and more important part of running a digital business, it literally pays to look for a cloud provider that offers the right set of capabilities and controls to protect your data, applications and the cloud infrastructure on which customer-facing applications depend. Expect the platform security solution to cover the five key cloud security focus areas: identity and access; network security; data protection; application security; and visibility and intelligence. The goal is to worry less about technology and focus more on your core business.

A well-secured cloud provides significant business and IT advantages, including:

- **Reduced time to value:** Since security is already installed and configured, teams can easily provision resources and rapidly prototype user experiences, evaluate results and iterate as needed.
- **Reduced capital expenditure:** Using security services in the cloud can eliminate many up-front costs, including servers, software licenses and appliances.
- **Reduced administrative burden:** By successfully establishing and maintaining trust in the cloud platform, the provider with the right security offerings assumes the greatest burden of administration, reducing your costs in reporting and resource maintenance.

For more information

To learn more about the five key areas of cloud security and related technologies and services from IBM, visit: ibm.com/cloud/security

Stay connected

IBM Cloud Blog

Follow us

@IBMcloud
Facebook

Connect with us

LinkedIn
YouTube

IBM Corporation
1 New Orchard Road
Armonk, NY 10504-1722

Produced in the United States of America, January 2018

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

[1] Insider Threat 2018 report, published November 2017, http://crowdresearchpartners.com/portfolio/insider-threat-report