Securing your journey to hybrid multicloud
Protecting workloads to enable business innovation and growth
## Contents

3 Cloud security is critical to business growth

4 Building security into every phase of your cloud journey

5 How do we get started and what’s our goal?

5 Where is our critical data and who has access to it?

6 How do I build, deploy and manage secure workloads in the cloud?

7 How do I adapt to threats and respond to attacks?

7 Continuous improvement as cloud continuously evolves

8 Secure your future with IBM hybrid multicloud security
Cloud security is critical to business growth

Cloud technology has evolved from a cost-reduction initiative to a business innovation enabler. Today, ninety-four percent of organizations use not just one, but multiple cloud environments to support their business.¹ Yet enterprises will continue their digital transformation journey, as 80 percent of workloads have still not migrated to the cloud.²

A critical part of the cloud journey is ensuring the enterprise stays secure across its data and workloads throughout its digital transformation. The current hybrid multicloud environment, with a growing list of security tools (deployed and managed by the enterprise) as well as native controls available from the cloud service providers (CSPs), can lead to fragmented security solutions and a decrease in threat visibility.

In some instances, working with thousands of clients, we have seen as many as 85 tools from 40 different vendors being deployed to manage these issues. Although many are best in class at what they do, this often just creates a fragmented patchwork of solutions with limited integration.

As the graphic below illustrates, security teams must also now adapt to a shared responsibility model with their CSPs, depending on the type of native cloud security capabilities that are available. This change in responsibility for the enterprise further adds to today’s challenges in establishing visibility and control across fragmented environments.
Securing your journey to hybrid multicloud

Building security into every phase of your cloud journey

Securing a hybrid multicloud environment requires a different approach than previous security programs that solely considered on-premise environments. **A successful journey to hybrid multicloud requires security consideration at every phase of the journey.** These phases are not a linear list of what needs to be done, but rather a continuous iterative cycle of strategy, development, implementation and management to:

- Establish a secure cloud strategy and roadmap
- Move and build for the cloud with a coordinated DevSecOps approach
- Continuously manage cloud threats and ensure cloud resiliency

The most success (and the least risk) occurs when organizations focus on secure strategy, DevSecOps and threat management

---

Shift Left: To move security earlier in the development lifecycle; shifting security from being brought in at the end of development lifecycle to being baked throughout.
### How do we get started and what’s our goal?

A critical initiative for a successful journey to the cloud starts with a cultural change of organizational enablement and empowerment to help business and technical teams come together, establishing alignment to common business goals. Security teams need to be woven into the fabric of the business.

Once the value of collaboration across the business is understood, security teams need to develop and share their hybrid multicloud security strategy with the rest of the organization to demonstrate how it will enable, not impede, business goals. First establishing a baseline of where you are with your on-premise and cloud security, then defining a target state and building a roadmap, taking into account your key business needs and objectives. Before you get started, you’ll also need to define and classify your critical business data and locate where that data resides. Along the way, you’ll need to ensure that the same macro-level strategy is defined and addressed across every layer of the stack. With those pieces in place, you’ll be able to identify the ideal future state for your enterprise security program, who owns which responsibilities, compliance considerations and more.

### Where is our critical data and who has access to it?

Cyberattacks often target data, and then use stolen credentials to access it. In order to protect your data, security teams need to locate, classify, secure and manage it, wherever it is, on-premise or in the cloud. Plus, they need to identify users and manage access to data across a hybrid environment in a frictionless manner.

#### How can IBM help?

IBM Security offers solutions to help organizations locate, classify, secure and manage your critical data wherever it resides with **IBM Security Guardium Multi-Cloud Data Protection** and **IBM Data Security Services for Cloud**. Managing identity and access across multicloud environments is a crucial component of cloud security. To assist organizations in securing access (including privileged access) and delivering seamless identity management, IBM Security offers **IBM Cloud Identity** and **IBM Cloud Identity and Access Management Services**.

## What is Cloud Security?

Check out this Lightboard video with Nataraj Nagaratnam from IBM Cloud as he maps out what cloud security is and explains how important it is for enterprises to incorporate it into their business operations.

[Watch video](#)
How do I build, deploy and manage secure workloads in the cloud?

Prior to cloud computing, security, technical and operations teams existed in each of their siloed parts of the business. But as technology advanced with mobile, BYOD and SaaS, technical and operations teams came together, and their alignment brought greater strides for the enterprise. Now, with the integration of the cloud, they must also work collaboratively with security teams across the business.

A successful security program starts with embracing a secure-by-design culture. This, in turn, introduces security earlier in the development lifecycle, from enforcing the right set of traditional and cloud-native controls (e.g., network, endpoint, identity and data) to continuous testing and validation. The entire process is then supported under the foundation of automation: establishing a robust and automated DevSecOps toolchain, automated deployment of base security controls and policies.

Maintaining secure workloads in a hybrid multicloud environment means that security teams need to have the capabilities to:

- Automate secure application development
- Define policies by workload requirements
- Automate security controls using infrastructure-as-code
- Manage configurations in a multicloud environment
- Repeatedly test their security defenses

How can IBM help?

IBM Security can show you how to build security into the application development process before you discover security vulnerabilities later. This reduces risk and the costs associated with re-engineering applications while also reducing your time to revenue for new, innovative services. IBM can help you build, deploy and manage workloads that are secure-by-design with IBM Application Security Services and IBM X-Force Red Services.

X-Force Cloud Security Services

Cloud introduces a broad range of native security controls unique to each provider. Learn how IBM cloud security services meets enterprises wherever they are in their cloud journey and offers a programmatic approach to securing their hybrid cloud.

Watch video 🎥
How do I adapt to threats and respond to attacks?

Threat management in a hybrid multicloud environment requires a unique set of capabilities. These include the ability to centralize threat visibility across disparate cloud platforms as well as on-premise environments, adapt policies based on threat current intelligence, quickly detect attacks and orchestrate organization and third-party wide containment, remediation and recovery.

Continuous improvement as cloud continually evolves

Cloud security is far from static; like the cloud itself, it's constantly in motion. **Security teams need to continuously monitor and optimize their multicloud security processes, from incident response playbooks to compliance reporting.** As security requirements change and cloud technology evolves, organizations need to dynamically adapt to this movement, from re-orchestrating processes to re-thinking their security strategy and implementation.

How can IBM help?

A hybrid multicloud environment increases the complexity of performing core security tasks, from threat management and remediation to regulatory compliance. IBM Security helps organizations strengthen their security posture across all environments with solutions that enable centralized control and management, including **IBM Security QRadar** for analytics and security incident and event management; **IBM Security Resilient** for cybersecurity orchestration, automation and response; **IBM X-Force Threat Management Services** to help you detect advanced threats and quickly respond to and recover from disruptions; and **IBM Cloud Pak for Security** to help generate deeper insights into threats, orchestrate actions and automate responses — all while leaving your data where it is and integrating with your existing security tools.
Secure your future with IBM hybrid multicloud security

The cloud is a pathway to business innovation, but one where security teams need to re-align their strategies and re-think their processes to enable a more secure path to cloud-based innovation. This means doing things like building security into DevOps processes, augmenting cloud-native security controls with additional security, attaching policies to cloud-based workloads, orchestrating multiparty responses across multiple cloud platforms and monitoring compliance continuously — all things that IBM Security can help you do better.

With our hybrid multicloud security solutions, your organization can use any cloud with confidence, creating an environment of trust that enables businesses to innovate and grow. IBM Security is helping thousands of organizations of all sizes on their cloud journey, from defining the right security strategy to managing multicloud environments. Only IBM Security can deliver solutions based on extensive research into quantum computing, IoT, AI and the experience of monitoring 70+ billion security events every day.

IBM has a deep understanding of enterprise security in today’s hybrid multicloud world. Let us help you take the right steps toward a secure cloud journey today.
Sources


2. Kennelly, Denis, “3 reasons most companies are only 20 percent to cloud transformation,” IBM.com, March 5, 2019.