Cloud-native security practices in IBM Cloud

White paper

Table of Contents

Introduction

IBM Cloud™ is IBM's high-performing public cloud platform, with data centers around the world that deliver cloud computing options from infrastructure as a service (IaaS), platform as a service (PaaS) to software as a service (SaaS). Security is a fundamental design principle for our cloud platform with market-leading security capabilities enabled for regulatory workloads.
Additionally, the IBM Security business unit provides advanced cybersecurity capabilities that run on the platform. Whatever you need to run: compute-intensive workloads, cloud native or commercial applications, big data, analytics, or AI, IBM Cloud helps businesses innovate with confidence.

This paper lists fundamental cloud-native security practices, with a focus on how to use them in IBM Cloud. It incorporates common practices from across IBM's global client base and industry best practices. The scope spans cloud security strategy, operations, management, shared responsibilities, and controls to meet compliance requirements. Cloud security is accomplished in layers, with particular attention on data and workloads in a cloud-native world.

This paper is designed for security and technology professionals who are evaluating or deploying workloads in the IBM Cloud. It covers the scope of concerns from deployment of a single application to complex, hybrid or multi-cloud environments. If you are starting out the information here will set you on the path to cloud native best practices, if you are transforming your enterprise the topics defined here will let you more easily identify gaps and opportunities to improve your security profile.

Cloud security shared responsibility model

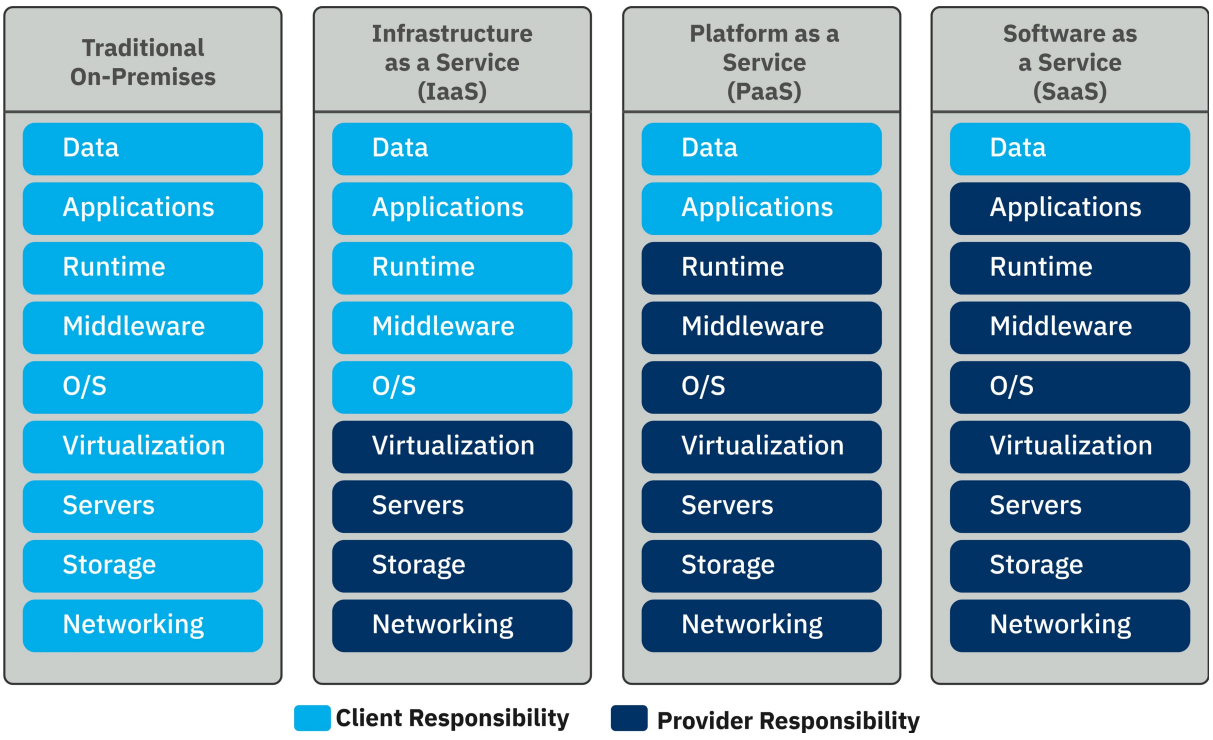
Securing the cloud depends on a shared responsibility model. By understanding the proper responsibilities, clients can better avoid security gaps.

Consider an example where IBM is the provider that sets up the home security system, but a business is the tenant who sets up access code. Who is responsible for ensuring that the alarm is active when the homeowner is away? It's a shared responsibility, where the client must activate the alarm and the provider must ensure that it is actively monitored.

In the model that follows, the tenant is responsible for all aspects of security in light blue, while the provider has obligations for enabling security for the components in dark blue.

For IBM Cloud generally, IBM as the provider is responsible for the security of the data center, hosting the servers, and the connectivity and uptime of the data center for the tenant's use.
IBM Cloud comprises a set of trusted facilities and systems. All locations adhere to the same standards and controls. Tenants can achieve compliance with controls and certifications by combining their responsibilities with IBM's responsibilities.

Shared responsibility for security in cloud services



IBM Cloud: When using IaaS

As the provider, IBM is responsible for the security of the data center, hosting the servers, and the connectivity and uptime of the data center for the tenant's use. IBM provisions the servers, virtual or otherwise. As the tenant, the client is responsible for these activities:

- Securing the entire workload, including servers, operating system updates, and patching, securing the applications, data, managing access, monitoring, and threat management.
- While IBM Cloud provides the VPN for VPC service that encrypts traffic by using IKE/IPsec from the client's premises to within the client's VPC, if a client requires true end-to-end encryption of traffic from their premises endpoint to their IBM Cloud VM, establishing that end-to-end encryption is the client's responsibility. If the application can be updated, TLS v1.2 or later should be used to establish layer 4 encryption end-to-end. Where the application cannot be updated, an IPsec tunnel should be used between the endpoint and the VM to establish layer 3 encryption.
- Using IBM's tools or its own tools to manage and secure workloads and data, independent of IBM.
- Hiring IBM service teams or other third-party teams to provide services, such as any security management and administrative tasks. These services are done upon request. When IBM fulfills such requests, it acts as an extension of the tenant.

IBM Cloud: When using PaaS

When it comes to PaaS, IBM as the provider is responsible for platform services that deal with application deployment. Those services include Kubernetes Services, data services such as object storage or database services, and other enabling application integration services, such as identity services, messaging services, logging services, and DevOps services.

IBM is also responsible for enabling security for the server configuration, patching operating systems and middleware in a timely manner, and the threat management of those platform components. As the tenant, the client is responsible for these activities:

- Maintaining the security of the applications and data that it installs or runs on the platform.
- Monitoring, threat detection, and responses on the application and data.
- Using IBM's tools or its own tools to manage and secure applications and data, independent of IBM.
- The tenant might hire IBM service teams to provide security management and assist with defined regulatory compliance and reporting requirements. In such cases, IBM acts as an extension of the tenant, who is still responsible for the security of its applications and data.

IBM Cloud: When using SaaS

As the provider, IBM is responsible for the cloud stack, but as the tenant, the client is responsible for these activities:

- Maintaining the security of any data that is processed and that it introduces into the service at any level in the stack.
- Proactive data protection, encryption, key management, access control, data and IP theft detection, and responses on data incidents.
- Using IBM's tools or its own tools to manage and secure workloads, independent of IBM.
- Might hire IBM service teams to provide security management and assist with defined regulatory compliance and reporting requirements. In such cases, IBM acts as an extension of the tenant, who is still responsible for the security of its data.

A secure journey to cloud: Culture, skills, and expertise

As clients look to meet their security responsibilities (IaaS, PaaS, and SaaS), it's important to understand the fundamental shift in culture, skills, and expertise. People, culture, process, and technology all must adjust to embrace the cloud-native paradigm that is brought forward by cloud environments. Architects and developers need to adopt secure-by-design or threat- modeling concepts upfront in the process to identify any gaps, design security in, and remediate issues before they deploy a vulnerable application. In short, as part of the DevOps approach, security must "shift left" in the design, development, and operational processes so that security is a forethought and becomes a DevSecOps model that is embraced by the entire organization.

Clients that are adopting cloud need to enhance the skills of their staff or acquire skilled members and integrate them into their current teams in a programmatic way. The teams must be trained to maintain the corporate defined standards while they use a specific cloud service provider. Deep expertise of the cloud service provider environment is required while incorporating cloud configurations, leveraging native-to-cloud provided security features.

The automation of activities such as penetration testing, configuration, deployment, alerting, and remediation is a foundational design principle in achieving continuous security. To achieve repeatable security, clients need automated deployments that use formation templates, monitoring and management of cloud-native workloads by using cloud service provider features, and APIs.

IBM Security and the IBM Garage Methodology bring extensive expertise and offerings to advise and support clients on their journeys to cloud adoption. Advisory and managed security services can be provided by using a combination of IBM Security and the IBM Garage Methodology based on the client's scenario and requirements. Advisory and managed services offerings include Governance, Risk & Compliance, Security Operations (SIOC), X-Force Threat Management (XFTM), X-Force Offensive Testing (XF RED), X-Force Intel & Response (XF IRIS), and others.

Cloud-native security practices

The effect of cloud on security practices and operational focus is transformative. Adoption of cloud services presents an opportunity to rethink and improve the security practices used to build, deploy, and manage applications. In the cloud services model security becomes a joint responsibility between the client and the cloud provider. After cloud adoption begins, organizations will find the focal points and responsibility for security shifts from traditional perimeter-based controls and infrastructure centric policies to security controls and policies more focused on overall operational practices, including data and workload technologies and development practices.

New cloud development and operations models have an overall effect on an organization's security culture. Continuous development is one of the most valuable features of the cloud native model, and security cannot lag releases. The goal of the cloud native organization is to maintain continuous development and achieve continuous security. To keep pace application teams must take on more security responsibility and accountability and developers must be enabled to embed security into the DevOps process. When security is baked into your DevOps and culture from the beginning you've achieved DevSecOps.

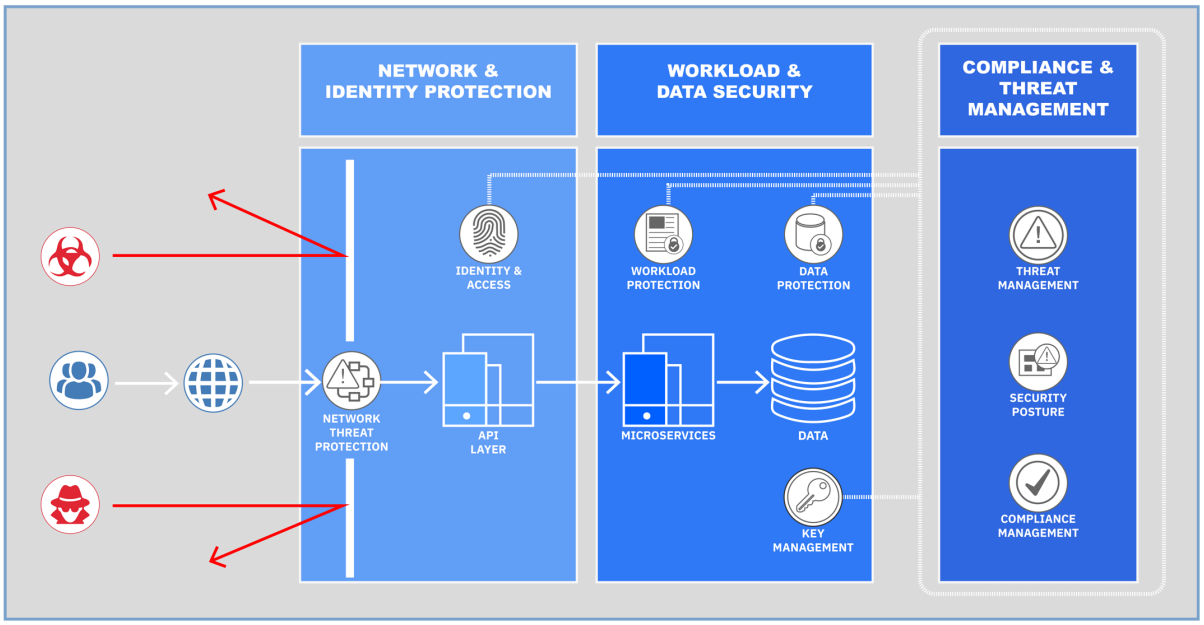
A thoughtful approach to aligning security practices begins with an overall consideration of your organization's cloud security strategy and approach:

- Take a risk-based view: You need to know what kinds of workload and data you are able to move to the cloud and which need transformation. Starting with a risk-based assessment gives you visibility, and a high-level roadmap for phasing your cloud adoption.
- Understand the shared responsibility model: Review the provider's cloud terms of service and your organization's existing security policies and requirements, including regulatory compliance. Identify if responsibilities have shifted from you to the provider, or if there are gaps in your existing policies or responsibilities matrix.

- Establish a collaborative culture and organization: Drive a collaborative culture between application, IT/ops, and security teams where application teams understand the importance of security and compliance in their role.
- Define, review or modify controls and processes: Security must be a forethought and not an afterthought. Take an end-to-end approach to achieve this on IBM Cloud. Ensure that the right controls and processes are in place to adopt a cloud native approach from the very first deployment. Security should be part of reviews of design and architecture. Include the security team in reviews.
- Practice continuous monitoring for security and compliance: Security controls are not one-time enforcement actions. Instill the practice in the organization, process, and culture, and use technologies and tools.
- Ensure proactive planning for cybersecurity events: Prepare for an orchestrated response to incidents, including keeping incident response professionals such as IBM X-Force IRIS on retainer.

Clients require an end-to-end approach to security that helps them achieve the three core objectives shown in the figure below. These include structured security practices like:

- Consistent use of network protection and identity and access management (IAM) tools to control access
- Increased client control and fortified workloads to protect data
- Continuous security and compliance with through clearly communicated controls, monitoring and both broad and targeted threat management, which add efficiency and visibility to how risk and compliance requirements are monitored and managed.



Manage user identity and access

Manage access to cloud resources by setting authentication and access policies with IBM Cloud IAM. You can specify which users or services can access which cloud resource on IBM Cloud. For example, your administrators can set policies so that only a particular user has administrative access to create virtual servers or Kubernetes clusters. You can also require users to authenticate with multifactor authentication when they access your cloud resources.

Access to applications requires the same attention as access to cloud resources. Business applications are the gateway to your business' or your customer's data. It is your responsibility to add authentication to the applications that are built on IBM Cloud. IBM Cloud App ID allows developers to add enhanced authentication to their web and mobile applications and better secure their cloud-native applications and services on IBM Cloud. Developers can extend this authentication with IBM Security Cloud Identity for advanced capabilities such as device verification and drive toward the goal of adaptive risk-based authentication.

Isolate and protect the network

The need for isolated and secure private network environments is central to layered security protection. VPCs, firewalls, VLANs, routing, and VPNs are all necessary to create isolated private environments. This isolation enables virtual machines and bare-metal servers to be more securely deployed in complex multitier application topologies and be better protected from risks on the public internet. Distributed Denial of Service (DDoS) attacks are a frequent threat. IBM Cloud Internet Services is a rich set of edge network services that clients can use to better secure internet-facing applications from DDoS attacks, data theft, and bot attacks.

The approach to cloud native network security must also consider the service types in use. To safeguard the network from an application located on a public cloud isolation, segmentation and micro-segmentation might be used. For customers using IaaS, isolation can be achieved by using a virtual private cloud (VPC). Additionally, security groups can add instance-level security to manage inbound and outbound traffic on both public and private network interfaces. Containers require additional attention when it comes to network security. When building cloud-native applications with a Kubernetes Service, limit the worker nodes or applications that can be accessed externally and use network policies to manage cluster isolation.

Enable protection for data at rest, in transit and in use

As you look ahead to the next era of computing, there are many predictions and assumptions about what the next great innovation might be, but one thing is indisputable: data and securing that data is and will remain important to companies and consumers. The protection of data and the management of encryption keys are standard items in security policies and controls. IBM Cloud encrypts the data in database and storage services with built-in encryption. For higher levels of data protection, you can manage the encryption keys that encrypt the data at rest. For sensitive data, gain control of encryption keys by using Bring Your Own Key (BYOK) with IBM Cloud Key Protect. Clients can hyper-protect data and keep their own keys with exclusive control of the keys and the hardware security modules (HSM) by using Keep Your Own Key (KYOK) with IBM Cloud Hyper Protect Crypto Services. For highly sensitive data, clients can consider encrypting the data at the application level before they store it in a cloud data service.

To help secure data in transit use TLS/SSL-enabled endpoints for applications and APIs. In Kubernetes environments, clients can enable TLS termination for cloud-native applications in the ingress controller and use TLS termination IBM Cloud Load Balancer Service when they deploy workloads on infrastructure with virtual servers or bare metal. For inter-cluster communications within a service, clients can centrally manage the certificates by using IBM Cloud Certificate Manager. With better visibility to your certificate lifecycle and automated expiry notifications you can proactively manage certificate expirations and avoid service outages. Connectivity to data centers in hybrid deployments often need a better secured tunnel, such as is provided by IBM Cloud Virtual Private Networks. In the above context, references to TLS indicate TLS v1.2 or later.

As the reliance on data grows in the era of hybrid cloud, the need for data privacy becomes even more critical for everyone, and for businesses, it's imperative. Confidential Computing protects data in use by performing computation in a hardware-based Trusted Execution Environment. That secure and isolated environment prevents unauthorized access or modification of applications and data while in use, thereby increasing the security assurances for organizations that manage sensitive and regulated data.

IBM has been investing in Confidential Computing technologies for over a decade and is on its fourth generation of the technology, delivering on end-to-end Confidential Computing for its clients' cloud computing for more than two years. From IBM's point of view, data protection is only as strong as the weakest link in end-to-end defense, which means that data protection must be holistic. Companies of all sizes require a dynamic and evolving approach to security that is focused on the long-term protection of data. Solutions that might rely on operational assurance alone don't meet IBM's standards.

IBM first announced generally-available Confidential cloud computing capabilities in 2018 with the release of IBM Cloud Hyper Protect Services and IBM Cloud Data Shield. The family of IBM Hyper Protect Cloud Services is built with secured enclave technology that integrates hardware and software and leverages the industry's first and only FIPS 140-2 Level 4 certified cloud hardware security module (HSM) to provide end-to-end protection for clients' entire business processes. IBM Cloud Data Shield provides technology that helps developers to seamlessly protect containerized cloud native applications without needing any code change.

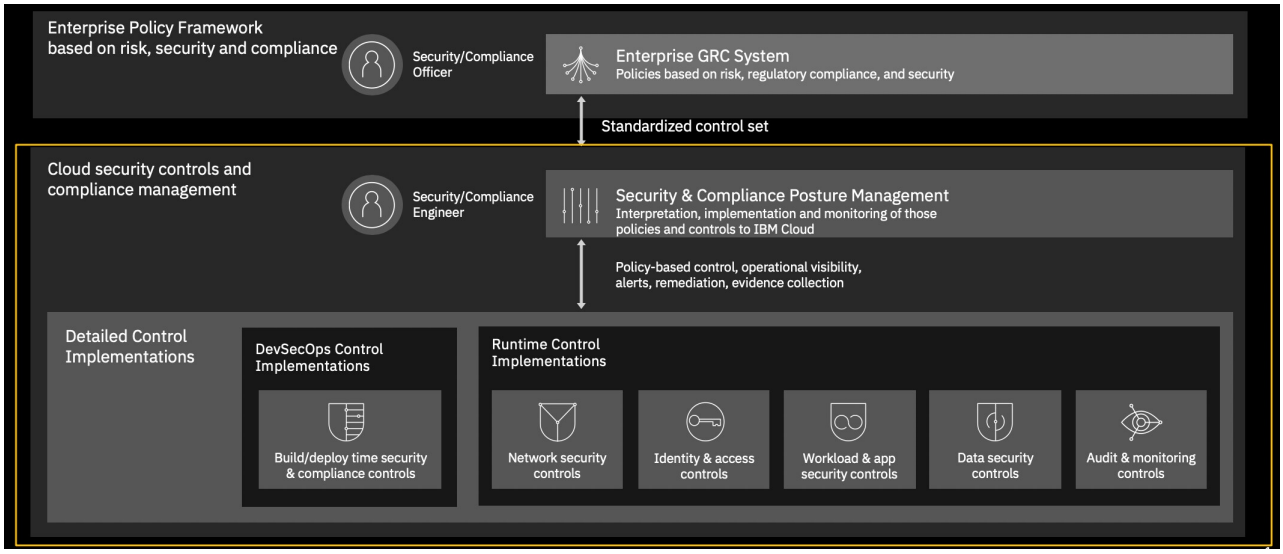
Data classification and data activity monitoring are two effective methods to help secure critical information. Before a client can adequately protect sensitive data, the client must identify and classify it. Automating the discovery and classification process is a critical component of a data protection strategy to prevent a breach of sensitive data. IBM Security Guardium provides integrated data classification capabilities and a seamless approach to finding, classifying, and protecting the most critical data, whether in the cloud or in the data center. Activity monitoring provides visibility into who is accessing sensitive information and what information is being accessed, creating alerts when certain conditions are met, and even blocking or quarantining connections where warranted.

Manage cloud security posture, compliance, and threats

As enterprises move regulated workloads to public cloud, it is essential to prove that security and compliance concerns are handled better, faster, and easier than their status quo. IBM recognizes the magnitude of these issues for all types of clients who are moving workloads to public cloud. The sheer complexity they have to endure to achieve a security or compliance standard is exhausting.

At the heart of the solution to achieve continuous security and compliance is the IBM Cloud Security and Compliance Center. The Center is a new security and compliance management platform on IBM Cloud where customers can define controls, assess posture, monitor security and compliance, remediate issues, and collect audit evidence. For example, an enterprise might define a collection of controls, such as a sensitive

workload profile, to address the security and compliance requirements for a cloud-native application that handles sensitive data. These controls can cut across data security, network protection, identity and access management, application security, and audit logging. From the enterprise policy framework, the controls are then standardized based on the NIST 800-53 control set. By adopting DevSecOps methodology, clients can also shift left to enforce appropriate guardrails as part of their CI/CD pipelines where security gates can be defined. In addition to posture management, the Center brings together capabilities to define configuration rules to enable governance and integrate to the capabilities of IBM Cloud Security Advisor that provide insights about vulnerabilities and threats.



With capabilities from IBM Cloud Security and Compliance Center and by aligning with IBM Cloud Satellite to enable enterprises to take advantage of their distributed cloud environment, clients can assess the security and compliance posture of their workloads in a hybrid cloud deployment.

Cloud governance, security and risk policies, and industry compliance standards all rely on some level of monitoring, reporting and audit. To guarantee an audit trail means tracking user access activities. IBM Cloud Activity Tracker, on IBM Cloud provides aggregated activity logs of administrative and developer actions completed on IBM Cloud resources. These logs are needed by DevSecOps and other security teams to carry out their duties. Security teams can also instrument applications so user or transactions logs can be sent to a logging store or other security system. IBM Cloud Log Analysis with LogDNA can be used as that log service.

Vulnerability and patch management processes and solutions need to be established according to the tasks and accountabilities associated with a shared responsibility model. During your planning phase assess risks and identify threats that need to be handled, such as malware, for endpoints, virtual machines and bare-metal servers. The IBM Cloud marketplace has catalogs of trusted vendors for these kinds of solutions.

Managing vulnerabilities in applications is an important part of managing security and compliance posture. With IBM Cloud Security Advisor, which is now integrated into IBM Cloud Security and Compliance Center, clients can get an integrated view of their security and compliance posture across vulnerabilities and certificates. IBM Cloud Security Advisor also provides a way to integrate the client's security tools and third-party security tools. There are tools to help ingrain security into your DevOps practices, assuring that security is considered upfront in the development process from build through deployment and runtime. Use Vulnerability Advisor in IBM Cloud to detect and manage vulnerabilities in

container images when building, deploying, and managing cloud-native applications. Run network vulnerability scans for any endpoints on the IBM Cloud network.

An organization's cloud threat management approach needs to be defined and integrated in the context of their overall threat management and security operations. The cloud threat management planning begins with the risk assessment of your cloud workloads and what kind of monitoring and reporting is necessary. To get an integrated view of security information and event management integrate cloud platform logs and flows into IBM Security QRadar. With this view, security analysts can manage incidents appropriately through IBM Resilient. Use the security and cyber expertise of IBM Security Managed Security Services to better manage the security of the enterprise and cloud platform. The IBM Security Managed Security services teams can provide a range of capabilities from "a single pane of glass" for hybrid multi-cloud to specific solutions for container security.

Cloud security and compliance

Compliance with controls is a top consideration that organizations encounter when they decide to fully engage in a cloud-first strategy. Clients can address compliance in the cloud and capitalize on the business agility and growth that the cloud inherently provides.

Compliance

IBM Cloud is designed for organizations that want a cloud environment that's security-rich, open, hybrid, multicloud, and manageable. IBM Cloud compliance and trust certifications reaffirm IBM's commitment to protection of customer data and applications. Designed with secure engineering practices, the IBM Cloud platform features layered security controls across network and infrastructure. For more information, see IBM Cloud compliance programs.

To achieve compliance for the workloads and applications that run on IBM Cloud, clients are responsible for ensuring security controls and managing those for their part of the shared responsibility model, as described earlier.

Data privacy

IBM is committed to protecting the privacy and confidentiality of personal information about its employees, clients, Business Partners (including contacts within clients and Business Partners), and other identifiable individuals. Uniform practices for collecting, using, disclosing, storing, accessing, transferring, or otherwise processing such information assists IBM to process personal information fairly and appropriately, disclosing it or transferring it only under appropriate circumstances.

With nearly 60 data centers across six continents, IBM offers a cloud architecture that enables clients to know exactly where their data and applications are running in the IBM global data center network. IBM is fully committed to protecting the privacy of clients' data. While there is no single approach to privacy, IBM complies with applicable data privacy laws in all countries and territories in which it operates. IBM supports global cooperation to strengthen privacy protections.

Protecting clients' data is mission-critical to IBM Cloud. IBM services are designed to protect clients' proprietary content and data. Access to data is strictly controlled and monitored in accordance with IBM's internal privileged user monitoring and auditing programs.
For more information about cloud privacy, see Privacy on the IBM Cloud.

Data centers

IBM's data centers are built with multiple deployment options for clients' unique workload needs. Clients can choose where to deploy from nearly 60 locations in 19 countries. IBM also offers 13 TBps of connectivity between data centers and network points of presence and three separate networks: a public, private, and internal management network in each data center around the globe.

All IBM data centers have industry certifications to better help clients build compliance into a complete cloud solution. Compliance is a critical decision point for organizations that are adopting a cloud platform. Moving internal workloads to the cloud can provide key business and technical benefits, such as elasticity, flexibility, and op-ex model. But moving to the cloud also means that the cloud must demonstrate a secure and compliant infrastructure that meets all the regulations and standards that the customer needs to build their application layers. IBM Cloud adheres to many stringent governmental and industry-specific standards. For more information and a list of all compliance certifications and regulations that are adhered to by IBM Cloud, see IBM Cloud compliance programs.

Building a cloud cybersecurity management system

Ultimately, cloud security practices are most effective when they are consistently applied against and governed as part of a formal cloud cybersecurity management system. A cloud cybersecurity management system formally defines these items:

1. Cybersecurity policy and operations governance
2. Cybersecurity risk management program and assessment
3. Cybersecurity controls definition and gap assessment
4. Cybersecurity threat management operations process and response

Cybersecurity policy and operations governance

Cybersecurity policy is crucial for defining how to properly manage cloud assets and resources relative to business and technology risks. The essential parts of a cybersecurity policy are as follows:

- Cybersecurity objectives
- Regulatory, contractual, and legal requirements
- Cloud vendor management processes and procedures
- How attainment of objectives and requirements are measured and governed

For instance, when it comes to cloud vendor management, vendor oversight is essential to ensure that the cloud, or any service provider, is fulfilling the obligations as set forth in the contracts.
Engage in business only with parties who have the required expertise and that are trusted. Insist on transparency and the disclosure of any subsuppliers, their locations, and their workforce

management practices. Supervise these cloud partners with validation programs such as testing their commitment to security and related hygiene. They should be held to the same standard of delivery as if the client were driving the execution.

For more information, see Security to safeguard and monitor your cloud apps.

Cybersecurity risk management program and assessment

The basis of an effective and executable cloud cybersecurity management system is understanding the prioritized business and technology risks that a firm faces. Cybersecurity teams must closely collaborate with business and IT owners to build a composite view of risk in order to properly prioritize their efforts.

Use a risk assessment methodology such as NIST 800-30, ISO 31000, or OCTAVE to create a prioritized risk register of assets, threats, and vulnerabilities based on assessing the current environment. Revalidate and reprioritize this risk register at least every six months.

Cybersecurity controls definition and gap assessment

After the prioritized risks are identified, the corresponding set of controls that can best address or mitigate those risks should be identified. Use a risk management controls framework such as NIST, ISO 27002, or CobiT. Then, document the specific controls that most effectively address the prioritized risks.

Analyze each of those controls to set a target maturity level according to a risk maturity model such as NIST or ISO 27001, and assess to determine the current maturity. Prioritize the resulting maturity gaps to drive cybersecurity operational and investment plans.

It's important to consider the responsibility for designing, implementing, and monitoring the controls in the context of the specific cloud services that are being consumed. Enumerate those responsibilities explicitly in the contract of service. For instance, core controls such as privileged identity management, vulnerability management, logging and monitoring, network security, and data security must be integrated in the context of the client's security practices and processes, including incident response, secure engineering practices, physical security, background screening of the workforce, and data security controls to secure cloud workloads.

Cybersecurity threat management operations process and analysis

All the previous steps feed the cybersecurity investment plan and program for threat management, which include these activities:

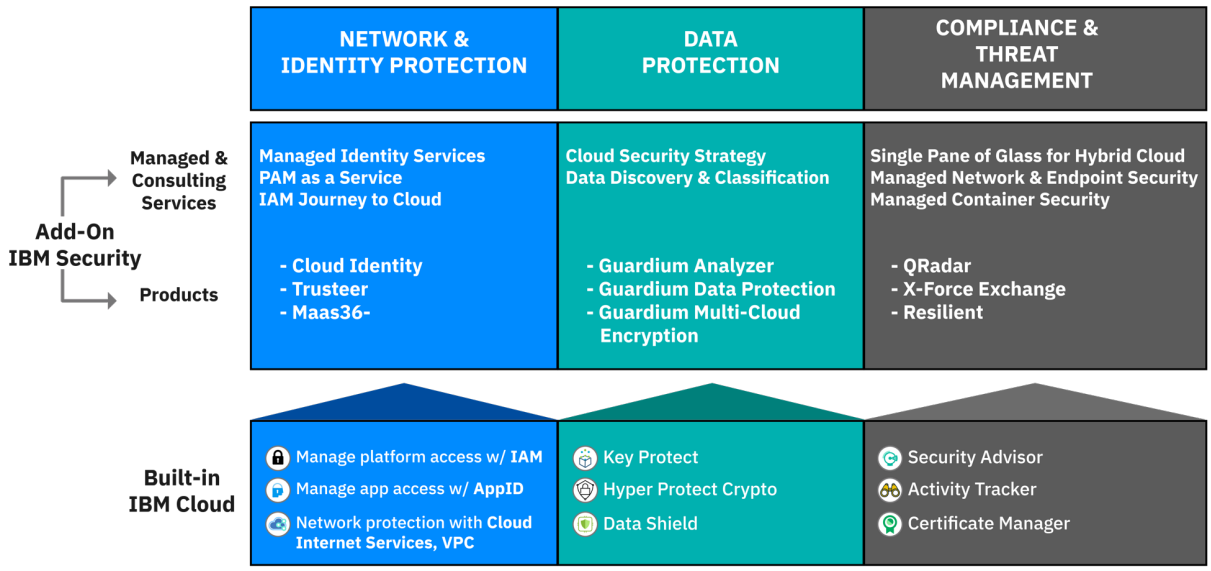
- Finding threats and vulnerabilities: "Finding the needles in the haystack"
- Confirming that each threat or vulnerability must be addressed: "Confirming that each needle is sharp enough to warrant a response"
- Fixing the threat or vulnerability when a response is warranted through a well-defined and up-to-date incident response runbook that is part of a formal Security Orchestration, Automation and Response (SOAR) program

Collectively, these steps provide an approach to building a formal cloud cybersecurity management system.

IBM Cloud security portfolio

IBM provides a set of security services and capabilities to meet the client's obligations as a tenant of a cloud platform. Aligned with the areas that are identified in the practices, IBM has built-in capabilities in the IBM Cloud catalog that can be integrated with DevSecOps processes. As add-ons, IBM provides industry-leading security products and a services portfolio from IBM Security, that can be leveraged together to build a strong security practice and implementations for achieving a confident cloud journey.

The set of IBM Cloud security capabilities is outlined in the following image. For more information, see Security in the IBM Cloud.



Further information

This paper discussed cloud-native security practices from across IBM's global client base, spanning cloud security strategy, operations, management, shared responsibilities, and compliance. For more information, see the links that are included throughout this document.