WHITE PAPER

Protecting Your Cloud

Maximise security in cloud-based solutions.

EXECUTIVE SUMMARY

With new cloud technologies introduced daily, security remains a key focus. Hackers and phishers capable of malicious activity seek out vulnerable targets, sometimes causing severe damage that reaches well beyond a single event. Even small, seemingly innocuous gaps in security coverage can put everything at risk, including data, customer information, uptime and potentially your organisation's reputation. In this whitepaper, we will discuss these constant threats to cloud security and how to address them effectively.

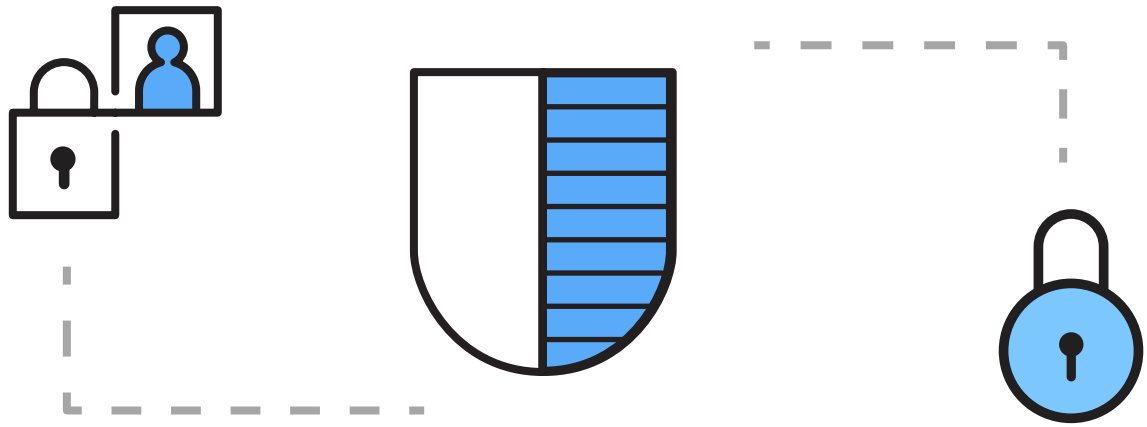
IBM

Trust and Accountability

In a managed cloud infrastructure, you outsource the management of IT resources to cloud providers, but you probably still wonder whether the benefits of cloud also come with security risks. You might worry about accountability, too. You may even question whether you can trust your cloud provider.

If any of those concerns sound familiar, rest assured that most cloud providers are well-reputed, known for protecting trust and for investing in their security infrastructures, including multiple levels of built-in, multi-layer security architecture options you can superimpose on your cloud environment. These security measures meet many of the standards set by governments and the industry, such as the U.S. Department of Defense (DoD) 5220.22-M standards, the NIST 800-53 framework and compliance with HIPAA, FISMA and SOC 2 Type II.

By themselves, these security measures exceed even the best protection that any individual organisation could implement on its own. But when it comes to securing critical information, accountability is everything. With so many cloud providers in the market, IBM® Cloud encourages organisations to perform due diligence before signing a contract. Businesses and organisations should always have the option to move to another provider if they are dissatisfied with their current provider.



Data Privacy and Protection

If your business or organisation traditionally stored its data in-house, moving data to cloud and ostensibly under a cloud provider's control can cause anxiety. You might question the cloud provider's ability to maintain the integrity of certain genres of information, such as personal, medical, or financial records of customers, while also meeting regulatory and legal requirements.

While we understand the concern in theory, there's little to worry about in practice. IBM Cloud is well aware of data privacy and sovereignty issues. It is our business to help you protect your customers' data against hackers and malicious attacks. We do our part to secure our infrastructure, too. This includes implementing automated Distributed Denial-of-Service (DDoS) migration, should a DDoS attack occur and offering intrusion protection systems, firewalls and SSL certificates so you meet your compliance requirements.

Q: Can cloud providers access, use, or share my organisation's data?

A: No. Multi-tenant cloud environments may reside on shared physical servers, but data is only accessible by you - not by any other tenants or the cloud provider.

Securely Leveraging the Cloud

How can a business or organisation provision a secure cloud-based solution on demand? Proper tools, including a set of security products and services with expert advice when needed, help any cloud novice build, deploy and manage a cloud solution. Here's a checklist for getting started:

- ☑ Provide secure connectivity, authentication, access control and audit capabilities for IT administrators and users.
  Include VPNs, multifactor authentication, audit control logs, API keys and other acute access control, allowing staff to securely access work data and connect to the application via HTTPS using SSL certificates.

- ☑ Enforce stringent data security measures. Leave data where customers put it. Never transfer customer data.
  Data cannot be shifted across borders and data-at-rest and data-in-transit must be encrypted. Use encryption solutions such as CloudLink®, Secure VM, IBM Cloud Data Encryption Services (ICDES) and ProtectV and Virtual KeySecure from SafeNet to ensure sensitive data-at-rest is not stored in clear text and that the customer maintains complete control of encryption keys.

- ☑ Ensure multi-layered security for network zone segmentation.
  Users and administrators must have confidence that their network is securely partitioned. IBM Cloud native and vendor solutions such as IBM Cloud VLANs, Vyatta Gateway, Fortigate firewall and Citrix NetScaler allow administrators to securely partition a network, creating segmentation according to organisational needs and providing the routing and filtering needed to isolate users, workloads and domains.

☑ Enforce host security using anti-virus software, host intrusion prevention systems and other solutions.

Apply best-of-breed third-party solutions like Nessus Vulnerability Scanner, McAfee Antivirus and McAfee Host Intrusion Protection to ensure administrators can protect their infrastructure from malware and other host attacks - enhancing both system availability and performance.

☑ Define and enforce security policies for hybrid cloud environments. Audit any policy changes.

Manage overall policies for the combined public-private environment using IBM solutions like QRadar, Hosted Security Event and Log Management Service and xForce Threat Analysis Service. Use solutions from vendors like CloudPassage, Sumo Logic and ObserveIT to automatically define policies around firewall rules, file integrity, security configuration and access control and to audit adherence to such policies.

Secure Your Cloud Now

Cloud security is more important than ever. In fact, cloud-based solutions are not only more flexible, scalable and dynamic in providing both short-term and long-term IT resources, but they are inherently more secure, more practical and make better economic sense.

Whether you are building your cloud solution for the first time or expanding your existing cloud environment, IBM Cloud has the resources to help you secure it. Contact us today to learn more about the security solutions discussed here or to learn more about other IBM Cloud products and services.

What can you do next?

- Learn more about firewalls, security software, SSL certificates and other security features: http://ibm.co/protect-your-cloud
- Read the IBM Cloud data security and privacy principles: https://ibm.co/datasecurity
- Read the IBM Business Conduct Guidelines: https://ibm.co/bcg
- Ask us questions at sales@bluemix.net or call us at 866-398-7638

IBM United Kingdom Limited
PO Box 41, North Harbour
Portsmouth, Hampshire PO6 3AU
United Kingdom

IBM Ireland Limited
Oldbrook House
24-32 Pembroke Road
Dublin 4

IBM Ireland registered in Ireland under company number 16226.

Please Recycle

KUW12521-GBEN-00