Locking down the cloud: Security’s new normal

Fine-grained security capabilities from IBM, for all the ways you use the cloud

Highlights

- Build a secure infrastructure for new cloud applications or using existing workloads in the cloud
- Share the cognitive power of IBM® Watson® for advanced analysis informed by IBM X-Force® threat data
- Lock down your applications to prevent unauthorized access to sensitive cloud data
- Test comprehensively for vulnerabilities in both development and production environments
- Ensure that employees and systems connect securely, to protect data and enforce access policies

Today’s cloud service providers generally do an outstanding job of providing operational security, but they don’t absolve IT of all security responsibilities. Providing end-to-end security falls on your shoulders, and the right way to approach cloud security really depends on your specific cloud agenda. Are you building new native cloud applications for your employees or customers, or deploying new workloads in the cloud? Are you integrating new cloud services with your existing applications and data? Are you consuming third-party software-as-a-service (SaaS) applications for specific business purposes—services such as Box or Salesforce?

Getting a handle on security in the cloud

More than likely, you’re using a combination of all these approaches to transform your business. And depending on your infrastructure and your specific cloud use cases, your security methodology and tool set may need to change. In a cloud-based universe, the security focus must shift to support the open perimeter of the environment. Managing access, protecting data, and gaining and maintaining visibility into cloud environments managed by third parties represent new security challenges.

IBM Cloud Security Portfolio

SECURELY CREATE

SECURELY INTEGRATE

SECURELY CONSUME

Create secure cloud services

With IBM, get all the tools you need in one place

IBM has all the tools you need to build a secure cloud infrastructure, whether you're creating new native cloud applications or pushing existing workloads into the cloud. With the IBM Bluemix® cloud platform, you can even incorporate the cognitive power of Watson. IBM cloud infrastructure services offer simplicity, predictability, interoperability and security. When you're ready to build a new cloud service, expand your remote storage capabilities or deploy a new cloud-based application, you can be confident that the components integrate seamlessly.

Using Bluemix for new workload deployments can simplify IT management for many organizations, especially those using DevOps processes to manage application development and those using converged infrastructure systems that merge storage, networking and processing. With IBM, building cloud applications (or deploying workloads in the cloud) is that much easier because you don't need to coordinate with multiple cloud-service vendors.

Solution spotlight: IBM Security AppScan

Even with a secure underlying infrastructure, it's important to keep your applications locked down to prevent unauthorized access to sensitive cloud data. That's where tools such as IBM Security AppScan® comes in. AppScan, with Dynamic Analyzer, Static Analyzer and Mobile Analyzer capabilities, enables you to perform comprehensive security testing in the cloud. Whether it's part of your application development process or part of routine vulnerability testing, AppScan can help you quickly identify and remediate application vulnerabilities.

- Watch the IBM video to learn how to get started with Bluemix.
- Download a free trial version of AppScan.

Integrate cloud with on-premises applications and data

Build a secure connection between cloud and enterprise

Many organizations have adopted a hybrid cloud model—some combination of public cloud, private cloud and on-premises resources. This approach allows IT organizations to apply the flexibility and on-demand virtues of the cloud to existing enterprise workloads. It can take many forms, from cloud storage for offline data to SaaS applications that integrate with existing enterprise services and data. When implemented carefully, this mix of cloud and on-premises services can integrate local and remote resources in a way that is transparent to the users while allowing IT to select the products and services that represent the best value, regardless of location or vendor.

However, integrating services from multiple sources means multiple upstream connections. For example, you may employ a mix of vendors for storage or data processing. And for each of those connections, you have to ensure that your employees and systems are all connecting securely to the cloud in order to protect data, enforce access policies and minimize risk. In this integrated infrastructure, it's not just users who are identified as part of identity services—it's also machines and services that connect in the background, such as when Marketo logs into Salesforce.

If you're integrating a mix of cloud and on-premises technologies, getting a firm grip on managing them—including tracking and controlling access—requires simplicity and visibility. With tools that consolidate your view into resources and give you fine-grained control over access, you can reduce complexity and minimize risk.

Solution spotlight: IBM QRadar and IBM Security Guardium

To fight threats, you need to first identify them. IBM QRadar® gives you visibility into the events that happen on your networked resources. It provides a cloud-delivered option for IBM QRadar Security Intelligence Platform, collecting, analyzing and storing log source data using a secure data gateway connection. Whether on-premises or cloud-hosted, QRadar is a flexible data-gathering and analytics powerhouse that can help your IT staff monitor threats, identify vulnerabilities, analyze risks and remediate data breaches.

IBM Security Guardium® helps secure your data—including cloud databases, big data, cloud file systems and more—by providing monitoring capabilities that show who is accessing the data, as well as assessment capabilities that reveal anomalies and vulnerabilities. Guardium is a flexible, cloud-ready data security platform that helps secure sensitive data across your full range of environments and use cases—and helps facilitate audit compliance.

- Watch the IBM video to see what IBM QRadar on Cloud can deliver.
- Read more on the web about the services that IBM offers to secure cloud-based applications.

Consume cloud services securely

Be alert for risks hidden in the cloud—and in your pocket

For many organizations, using third-party SaaS applications can provide significant benefits—connecting users to familiar applications quickly and at scale. You may be employing platforms such as Salesforce, Workday, Box or other SaaS solutions for everything from email to inventory control.

Even if the cloud vendor's side of the network is secure, your organization can still be vulnerable to threats resulting from poor password policies and mismanagement. In addition, the security of individual user devices plays a role. When users are accessing cloud applications via desktops, laptops, tablets and smartphones, these endpoints can become the most vulnerable part of the chain. In addition to application access control, locking down end-user devices is a critical component of your cloud security strategy.

Solution spotlight: IBM Cloud Identity Service and IBM MaaS360

One way to simplify access management for users and IT administrators alike is to implement centralized privilege administration. Whether an organization needs a simple and affordable federated single sign-on (SSO) service or a complete replacement of its entire on-premises identity and access management (IAM) infrastructure, IBM Cloud Identity Service can help. IBM Cloud Identity Service is a comprehensive identity-as-a-service (IDaaS) solution, robust enough for enterprises and yet accessible to smaller firms looking for a strategic platform that can grow with them. Premium, on-demand features offered by IBM Cloud Identity Service include identity governance and administration, access management, federation, self-service, audit and reporting, and application program interface (API) integration.

IBM MaaS360® secures your cloud environment at the point where users access it—their hardware devices. MaaS360 is an enterprise mobility management solution that protects the full range of end-user devices, from desktops to mobile devices, whether Microsoft Windows, Apple Mac, Google Android or other operating system platforms, making working in a cloud-based and mobile world simpler and safer.

- Watch a short 2-minute Cloud IAM video to learn more about IBM Cloud Identity Service.
- Read the IBM blog to learn more about locking down your cloud applications.

Go forth and cloud

Achieve new advantages, new opportunities

Just because you can't hug your server when you move to the cloud, doesn't mean security has to be out of reach. Security has traditionally been the biggest inhibitor to wider enterprise adoption of cloud, but IBM offers a powerful cloud security portfolio that addresses the risks of cloud computing while enabling innovation and accelerating time to value.

Although today's cloud vendors offer sophisticated security features, IT can't just pass the buck when it comes to security. Cloud security is just as important as any other component of enterprise security. That said, the approach to security you've been using for on-premises resources won't necessarily fit the bill. In addition to the many integrations and touchpoints associated with cloud implementations, cloud hardware and network resources themselves are abstracted, meaning your staff may not have direct access to the underlying platform. This creates a shift in how and where you can apply security controls.

Whether your organization is all-in on cloud, or just testing the waters with a few SaaS applications, you have to apply the appropriate security controls to safeguard your business. IBM offers solutions to help you build new cloud services, extend and integrate your cloud services, and consume third-party cloud services securely. With a comprehensive portfolio of products and services for your cloud environment, whether it's growing or mature, IBM enables you to manage access to applications and data, protect valuable resources, identify and address potential threats, and gain visibility into complex cloud environments. The result is an opportunity to transform your business with a cloud strategy that fosters innovation, increases efficiency and reduces risk.

- Learn more about IBM Security solutions for cloud.

For more information

To learn more about IBM security solutions for the cloud, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's largest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
February 2017

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.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.