October 2014

See clearly in the cloud with threat-aware identity and access management

Securely connect people, applications and devices to cloud environments

Highlights

- Traditionally, security has been a key inhibitor to cloud deployment.
- Next-generation security solutions can help securely connect people, applications and devices to the cloud.
- Threat-aware identity and access management can strengthen cloud security by enabling self-service.

Organizations of all sizes and types find a lot to like about cloud computing, including greater operational efficiencies and lower costs than with traditional IT deployments. However, many still have lingering concerns about reduced visibility into cloud infrastructure, less control over security policies, new threats against shared environments and the complexity of demonstrating compliance.

Security, though critically important, should not be an inhibitor to the adoption of cloud computing. A comprehensive and dynamic approach to cloud security can help organizations manage access, protect data and gain visibility across the cloud environment.

Cloud security solutions can transform clouds into highly safe and secure places, where trusted interactions can occur. For example, threat-aware identity and access management (IAM) can be a key line of defense in the cloud. Novice users and/or developers can use self-service IAM features to strengthen their own security in the cloud. And even if users have limited experience with security, the self-service mechanism can help ensure that their activities within the cloud environment are secure.

Core elements of cloud management

To manage access in cloud computing and securely connect people, applications and devices to the cloud, organizations need to meet or exceed the security of traditional IT environments. They need to address compliance requirements, reduce operational costs and enhance the overall security posture. Ultimately, organizations need to provide strong security that encompasses four core elements:

Identity lifecycle management

- Simplifying on-boarding of new internal users and assigning access privileges to cloud-based services; easily terminating user accounts and access privileges at the end of the user lifecycle
- Supporting user self-care for enrollment, password resets and recertification
- Providing identity services to validate and centrally manage access across private, public and hybrid cloud deployments
- Enabling access governance with management of role-based user entitlements and auditing of user activities

Access management

- Providing secure authentication of users and enforcement of context-based access policies after authentication
- Protecting infrastructure, applications and data with threat and fraud prevention
- Centralizing control for consistent execution of security policies across multiple applications and users
- Enabling single sign-on (SSO) across applications to improve the user experience and reduce help-desk costs

Directory services

- Simplifying identity synchronization between on-premises and off-premises infrastructure—for example, any changes in local directories can be synchronized with cloud identity services
- Providing cloud environments with access to enterprise authentication services—for example, a new private cloud can use the authentication services of existing enterprise infrastructure

Security intelligence

- Monitoring, auditing and reporting on user activity to reduce the risk of internal threats and help facilitate compliance with policies and regulations
- Providing insight into cloud operations with auditable intelligence on cloud access, activity, cost and compliance
- Delivering integrated analytics and access certification using tools to enhance federated directory for cloud integration

With these core capabilities in place, organizations can better manage access for cloud environments in order to improve their control of security threats.

The service approach to cloud delivery

When building a cloud environment, organizations can choose from multiple delivery models. At the most basic level, they can deploy an infrastructure-as-a-service (IaaS) environment, which provides the hardware, IT infrastructure, and dynamic scaling and management capabilities for business workloads. Or, they can deploy a platform-as-a-service (PaaS) environment, which helps support the rapid development of applications and application programming interfaces (APIs) using a catalog of composable services. Finally, at the most advanced level, they can deploy a software-as-a-service (SaaS) environment, which enables end users to use full-featured applications and services via the cloud. Each delivery model has its own security needs stemming from the applications commonly deployed and the business and user needs commonly supported.

IaaS: Securing workloads

When workloads move from a conventional, on-site data center to the cloud, security is often a concern. Workloads are, after all, the processes that get business done—and as such, they cannot tolerate compromise. Worries can be especially great when cloud services are hosted by a third party—including scenarios in which organizations are moving existing applications from on-premises data centers to cloud infrastructure.

Regardless of the hosting environment, however, the organization must achieve full operational visibility across the cloud deployment. It must govern use of the cloud infrastructure and monitor/report on user activities. Plus, it must protect the infrastructure and workloads to meet compliance objectives. For the many organizations that use cloud solutions—such as those from SoftLayer,[1] a server-managed hosting and cloud computing provider; Amazon Web Services, a cloud computing platform; VMware virtualization solutions; or OpenStack open-source software cloud computing software platform—capabilities for managing privileged administrators and controlling access to web workloads can be vital. When migrating workloads to an IaaS environment, organizations must ensure that they have a consistent security enforcement point to help protect all of the workloads that are deployed in the cloud, whether web, mobile or APIs, from inappropriate access and malicious tampering.

PaaS: Securing development

Developers need to build security into all applications—even if security is not their area of expertise. They need to provide visibility into and protection against fraud and threats via built-in access management capabilities, even as they focus on providing business functionality and a seamless user experience.

In developing and deploying applications, many organizations use solutions such as IBM® Bluemix™, a cloud-based platform for building, managing and running applications; force.com solutions for building multi-tenant applications; and Microsoft Azure, a solution for building, deploying and managing applications. For secure results in cloud environments, developers need to create products that can integrate and authenticate with existing identity stores. At the same time, however, cloud application identities are often managed separately from on-premises solutions, creating the need to support enterprise and cloud directories with common authentication policies. Furthermore, authentication solutions need to be easy to implement. Otherwise, developers may avoid using them, and, if applications are not secure, the PaaS environment is not a viable option for hosting them.

SaaS: Securing applications

The SaaS platform has undergone rapid adoption in recent years, thanks largely to its ability to save IT headaches by eliminating the need for on-site IT management. Challenges arise, however, from the need for application governance—the ability to control who has access to the system and how the organization provisions and de-provisions this access.

For the many organizations that deploy SaaS applications—such as IBM Kenexa® employment and retention solutions, Workday business management solutions, Salesforce customer relationship management solutions, Google applications or Dropbox file-sharing solutions—a two-pronged approach to security is required. To ensure application security, they need complete visibility into their software use. And to reduce threat and risk, they need access management capabilities such as identity federation, SSO and improved governance.

IBM solutions for cloud security

Regardless of which cloud deployment model an organization chooses to adopt—IaaS, PaaS or SaaS—IBM has security solutions to safeguard those environments, including:

- IBM Security Access Manager for Web and IBM Security Access Manager for Mobile, which provide a complete access management solution with integrated session management, context-based access, and strong authentication capabilities in a virtual appliance form factor that is easy to deploy in cloud environments
- A cloud security gateway solution leveraging the combined capabilities of IBM DataPower® Gateway and the IBM Security Access Manager for DataPower module to provide comprehensive security at the message-, infrastructure-, and user-level in a single, converged enforcement point
- IBM Single Sign-On for Bluemix, which provides a policy-based authentication mechanism that allows developers to build access security into their applications, without becoming security experts; it supports integration with many popular social identity stores such as Facebook, LinkedIn and Google, as well as integration with existing on-premises identity stores

- IBM Security Federated Identity Manager, which provides key federation capabilities that enable an organization to act as an identity provider for SaaS applications as well as provide a seamless SSO experience for end users
- IBM Security Identity Manager, which allows the creation of policy-based user provisioning and deprovisioning access to SaaS applications
- IBM Security Privileged Identity Manager, which provides control over and visibility into what privileged users and system administrators are doing in the environment, such as within SoftLayer cloud services
- IBM Security Directory Integrator, which provides a mechanism for unifying identity silos and helps build an authoritative data infrastructure from heterogeneous data sources
- IBM Cloud Identity Service, which provides a comprehensive cloud-hosted IAM service that combines best-in-class IBM IAM software with the global delivery capabilities of IBM Managed Security Services

For more information

To learn more about the IBM portfolio of identity and access management solutions for cloud environments, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
October 2014

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 or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a 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 systems and products are immune from the malicious or illegal conduct of any party.

[1] SoftLayer Technologies was acquired by IBM in July of 2013.

Please Recycle