PAM IN THE CLOUD

The Importance of Privileged Access Management in a Cloud Environment

WALLIX
CYBERSECURITY SIMPLIFIED

PAM in the Cloud

The Importance of Privileged Access Management in a Cloud Environment

TABLE OF CONTENTS

WALLIX
CYBERSECURITY SIMPLIFIED

INTRODUCTION

Companies are moving to the cloud in greater numbers than ever, targeting flexibility and access for their increasingly distributed workforces. According to a recent Forrester Research report, 58 percent of companies surveyed outsource half or more of their data center operations, servers, network, and storage infrastructure, clearly illustrating the shift businesses are making to cloud environments.

Cloud migration of all critical resources, or even a portion for hybrid environments, presents serious security challenges and risks to the organization. The cloud is an attractive target to hackers, and is highly vulnerable to insider threat by negligence or malicious intent. Organizations need to implement rigorous cybersecurity practices to control access to critical systems and protect sensitive data, whether operating on-premise or in the cloud.

Cloud Migration

Understanding the Cloud

More and more, businesses are making the move to the Cloud. Cloud migration of data servers and other important resources improves organizations' scalability and flexibility in a fast-moving business environment. Moving assets to the cloud increases accessibility for remote and geographically diverse teams, and reduces the need for massive on-premises server rooms.

In short, whether operating in a pure cloud or hybrid environment, cloud migration simplifies IT and business management.

Cloud adoption is moving quickly, but migration is a significant undertaking and companies are not always prepared to move all their applications and resources in a single pass. Rather than moving completely off-premises to a "pure cloud" environment, businesses often move some parts of their IT resources to the cloud while keeping others in-house, resulting in a "hybrid" infrastructure environment.

What is a Hybrid Cloud?

By definition, a hybrid cloud operates with some of its resources in-house and others managed in the cloud. But what does that truly mean?

According to Forrester Research, a true hybrid cloud is one in which applications operate seamlessly both on-premise and in the cloud; where public and private resources are interoperable; and in which provisioning, visibility, and management all occur on the same management plane through a common portal.

As noted above, companies rarely move all resources to the cloud at once, instead preferring to keep some on terra firma, on-premises. The reasons for migrating in stages might include resource constraints, application readiness issues, accessibility concerns in remote locations and environments, or the company may simply want to take the time to become comfortable with the new systems, if they plan to move to a pure cloud strategy at all.

As the data from IDC shows, almost every modern company operates in a hybrid computing environment today. Even companies whose ultimate goal is an "all-cloud" strategy typically move through a hybrid phase on their way to total cloud support. Many companies never make the leap to pure cloud.

Regardless of the stage of the company's cloud journey, one factor is critical. Security and access management must be a top consideration at every step of the cloud transition. A hybrid Infrastructure can be complicated to secure, as the means of access and system attributes can be quite different.

The Impetus to Cloud Migration

Since most IT departments operate on tight budgets, the opportunity to outsource the mundane aspects of IT operations at a low cost is attractive. In addition, cloud operations offer several advantages that make cloud or hybrid IT operations appealing.

1. Scalability

The cloud offers easy scalability and flexibility as a company grows or contracts. This can make planning easier as the company adds users or remote office; there's no need to make room for new servers on-site. Scalability also simplifies on-going budgeting, because the company does not have to purchase hardware to support peak requirements during month-end periods or audits, or reserve funds for spares to support hardware failures or upgrades.

2. Efficiency

One of the most attractive aspects of the cloud is that it frees the in-house IT team from performing mundane tasks like backups. A cloud infrastructure offers automated back-up to ensure data is well-saved. Routine tasks like manually backing up servers eat up time that would be better spent on more strategic projects when the cloud provider takes on the burden.

3. Accessibility

The cloud is accessible from anywhere using a modern browser, so it is ideal for remote locations, remote or traveling employees, and especially for external partners who need to access the company's business systems.

While there are many compelling reasons for companies to move to the cloud, this shift comes with its own challenges for the CISO. Whether the company is operating fully in the cloud or in a hybrid environment, the cloud increases the need for security measures to protect critical assets, no matter where they're stored.

Control over access privileges to these target resources is important for IT operations in any environment, but they are essentials when operating in a hybrid cloud environment because of the unique characteristics of a hybrid setup.

Security Challenges of the Cloud

The savvy CISO recognizes that shared resources and applications can present a heightened security risk when compared to and on top of the security vulnerabilities inherent even in operating in-house. This increased risk stems from several factors stemming from the nature of operating in a cloud environment, whether hybrid or pure cloud. These risk factors include multi-tenancy on servers or shared resources, remote accessibility from any location, and the need to share data across cloud and in-house resources.

Security in the Cloud

Accessibility is the double-edged sword of the cloud. Ease of access is what makes the cloud so useful for companies with multiple locations or remote users, but it also presents an attractive target for hackers.

IT security is an increasingly critical challenge for businesses, made even more difficult when financial data or other sensitive assets are moved off-site to the cloud, where access is less controlled.

With global cyberthreat ever on the rise across every industry, clearly, IT security is a critical component for every organization.

The best way to protect company assets is to isolate the cloud environment and minimize potential attack surfaces. But what are the biggest challenges to achieving cloud security?

Cybersecurity Statistics

- In its 2018 Global Risk Report, the World Economic Forum labeled cyberattack as the 3rd likeliest risk, behind only extreme weather events and natural disasters. It was estimated to have the sixth largest impact for 2018.

- According to a report from the **Ponemon Institute**, the average cost of a cyber breach is $148 per record, and most breaches involve thousands of records. In addition to the monetary cost, a breach can lead to loss of customers or intellectual property, either of which can quickly outpace the cost of repairing the breach.

Remote Access

By its very nature, the cloud enables remote accessibility to key assets, whether users are located at company headquarters or are logging in remotely from some distant location. This privileged access, however, is the root of most data breaches.

What is privileged access? A user with access privileges is one who has login credentials to access the back-end, administrative side of IT infrastructure. Privileged users can be system administrators in the IT department, C-level executives, or even external, 3rd-party vendors.

Any number of people may need privileged access to accomplish their daily tasks, but unfettered accessibility is a major security vulnerability. Each time access privileges are granted, a new point of vulnerability is opened, as a user's login and password could be lost, stolen, or shared indiscriminately.

- **60% of cyber attacks**[1] are conducted by insiders, according to IBM research
- **81% of hacking-related breaches**[2] results from stolen or weak passwords
- **42% - less than half** [3] **–** of all organizations have controls to protect against insider threat

Remote access to a business' most sensitive resources, from financial data to customer details or even DevOps code, presents significant challenges to securely operating in the cloud.

Multi-Tenancy

Migrating to the cloud necessitates a Cloud Service Provider (CSP). These CSPs host data for hundreds of clients, potentially running on the same cloud resource, all of whom have privileged credentials to access the cloud infrastructure. This multi-tenant environment naturally presents an additional vulnerability.

Residents in an apartment building, all clients must enter the same building yet stay isolated from others' private apartments. Divisions between tenants and locks to each unit must be robust to prevent accidental or malicious security breaches. Though CSPs have their own security measures, they have clients accessing their servers who may not have the same rigorous standards. Each individual tenant can fortify their own property with additional security measures for increased peace of mind.

As a client of a Cloud Service Provider operating with multi-tenancy, it becomes imperative for businesses migrating to the cloud to add layers of access control to ensure no breaches occur.

DevOps

DevOps teams responsible for software development present a particular challenge to IT security. While many solutions such as Puppet, Ansible Tower, Octopus, and RapidDeploy aim to assist the DevOps

1. http://www.financierworldwide.com
2. http://www.business2community.com
3. http://www.haystax.com

team in creating and deploying apps and code to the cloud, most leave security up to the developer.

Many cloud or hybrid functions run in unattended mode, opening applications and passing data between cloud and on-premise applications using scripts. This is simple and highly efficient because it ensures that jobs run as needed, but in most cases, it opens the organization to an unexpected security risk.

To work more efficiently, DevOps often resort to hard-coding passwords into the scripts. This means that anyone who gains access to the script can see the password, which are frequently "all-access" or privileged accounts that have wide-ranging access to data and resources on the entire network. DevOps teams need a secure, streamlined, efficient solution that eliminates the need to hard-code passwords into scripts yet keeps workflows undisrupted to ensure productivity doesn't suffer.

PAM for Secure Cloud Infrastructure

A Privileged Access Management (PAM) solution offers a secure, streamlined way to authorize and monitor all privileged users for all relevant systems – both on-premises and in the cloud. It keeps your organization safe from both accidental or deliberate misuse of privileged administrator access to critical systems and resources.

Centralized Access Management

A PAM system provides a central management console that enables quick, streamlined management of all users across multiple or disparate systems, including and especially hybrid cloud environments. By definition, an Access Management solution allows the IT security team to grant, revoke, and define access privileges. Doing so from a single point of control gains time, efficiency, and oversight over all privileged users active in all systems.

• Many organizations deal with frequent personnel changes, people changing roles frequently, or external, third-party vendors who require internal access. Having a single console for access management allows for easy system and password control, even in a multi-tenant or hybrid environment. Not only can centralized management improve security, it also increases IT productivity and efficiency.

• Super-administrators can grant access to users only for those systems for which they are authorized as and when it's needed, for defined time periods, and revoke access automatically when the need expires. This helps ensure the safety of critical infrastructure and resources as user accounts aren't forgotten or left dormant, eliminating an easy target for hackers.

Robust Password Management

Each privileged user with access to IT assets represents a potential opportunity for insider threat or hacker breach. A robust password management solution and policy keeps these threats at bay by closely protecting administrator passwords.

• A password manager eliminates the need for individual users to ever have local passwords or root access to sensitive systems. What's more, a robust password management tool can impose strict complexity requirements on passwords and rotate them frequently to further increase system security. And by passing through a password manager, access is simplified for the user and reduces the number of entry points that must be managed or contained if a user leaves the organization or changes roles.

• When a company uses cloud applications, there may be a need to pass data securely between applications or to run jobs like reports or analysis in unattended mode. As noted before, without a PAM solution, DevOps often embed passwords in their scripts. While this conveniently allows the jobs to run unattended, it can be a huge potential security risk. The ideal solution has two components: a secure password vault and an **Application-to-Application Password Manager** (AAPM) to authenticate passwords between cloud applications. The AAPM unlocks the secure vault to retrieve the correct password, which is made available to the script for the duration of the process. By delivering access through the AAPM, you separate the credentials from the script, making it much harder for unauthorized sessions to gain access.

Audit & Oversight

A Privileged Access Management solution can generate an unalterable audit trail for any privileged operation, so your IT security team can track, view or replay the actions of any privileged user.

• Review any privileged session with complete session monitoring. Whether for training purposes or for incident response, session management features are a valuable component of a strong PAM solution. Administrators can see what actions any user has taken in any cloud or on-premise system, and can automatically terminate sessions attempting unauthorized operations, protecting your cloud infrastructure from suspicious activity, instantly.

• Regulatory compliance is a necessity for every organization, and cloud or hybrid systems make complying with cybersecurity standards complex. PAM solutions make compliance easy, responding to critical aspects of any government or industry IT security regulation, and providing proof of compliance for audit purposes.

Customer Case Study: PAM in the Cloud

Organization: Large Transnational European Company
Industry: Utilities & Public Services (water, energy, and transportation)
Challenge: Migration of infrastructure to AWS cloud
Goal: Enforce security and have complete visibility into everything happening within the organization's IT infrastructure.

This large organization wanted to move their infrastructure to AWS cloud to eliminate the task of managing physical servers and data centers. Before the migration, the organization determined that any part of the infrastructure that couldn't be moved to the cloud would instead be outsourced to a third party.

In their previous infrastructure setup, the organization had several isolated perimeters on-premise and wanted to maintain a similar structure in their cloud migration. The plan was to maintain core-activity data on one side and use the other side for infrastructure. In order to ensure security and enforce auditability for all users, the organization decided to implement the WALLIX Bastion solution.

Using a PAM Bastion, the organization:

- Wanted to able to answer the questions "Who, what, where, when, why, and how?" for all administrative and privileged user activities
- Was looking for a way to enforce security for their DevOps team
- To support their "full cloud" migration efforts by modifying working habits and utilizing the automation of Virtual Machines

Initially, DevOps was using Ansible and Terraform scripts to interact with the cloud infrastructure. Using this method forced the need for passwords to be hard-coded into scripts, which is not secure and leaves these critical passwords potentially vulnerable.

By using WALLIX's PAM solution, the organization was able to eliminate hardcoded passwords using AAPM technology to retrieve passwords automatically from a secure vault.

In addition, by utilizing a PAM Bastion with their cloud infrastructure, they now have the assurance that no critical administrative tasks will be performed directly within the environment. Instead, the Bastion will act as a man-in-the-middle, significantly mitigating the risk of potential data leaks and providing complete auditability in the event of an incident to quickly stop a breach in its tracks.

Choosing a PAM solution to Protect On-Premise and Cloud Operations

When looking for a PAM solution to protect your IT environment, look for a single solution that includes all critical components of privileged access management.

- A centralized management console that works across cloud, hybrid, and on-premise systems to streamline and simplify access control across all IT systems
- AAPM for application to application password management to enable DevOps efficiency without the risks attendant to embedding passwords in scripts
- A secure password vault to store and rotate passwords, and enforce complexity requirements
- Session monitoring offering comprehensive oversight over all privileged session activity, real-time alerting, and unalterable audit logs.

The cloud makes it easy to connect remote employees to IT resources, and to use common applications and servers. This enables flexibility and efficiency for the organization, but IT needs a simple yet powerful centralized solution for managing sites and resources, whether in a pure cloud, hybrid or on-premise environment.

WALLIX's Privileged Access Management suite offers a single console for super-admin management while enabling access to all sites and solutions without requiring multiple logins or risking stolen credentials. This solution supports the CISO's need for access control while still allowing internal teams – like DevOps – to maintain or increase productivity without sacrificing tight security.

The WALLIX Bastion is an ideal solution for companies at every step of the cloud transition. With access, password, and session management components, the Bastion offers comprehensive oversight and control over who has admin access to IT infrastructure, what they do with it, and when. Whether operating in the cloud on on the ground, WALLIX's PAM solution ensures all business assets are protected and compliant with cybersecurity regulations.

Conclusion

Every company should consider a PAM solution, whether they operate on-premise, in the cloud or in a hybrid environment. For those who are just starting their migration to the cloud, PAM is the first step to a smooth transition; those already operating in the cloud will find that the right PAM solution helps solve many of their ongoing security and access management challenges.

A centralized management console provides a single point of control for all resources, regardless of whether the company operates with legacy on-premise systems, in a pure cloud environment, or a hybrid infrastructure blending old and new. Granting, monitoring, and revoking privileged administrative access to sensitive resources is streamlined, secure, and centralized. This improves IT productivity and efficiency without compromising the organization's security.

If you would like to learn more about Privileged Access Management, visit www.wallix.com today.

WALLIX
CYBERSECURITY SIMPLIFIED

WALLIX

CYBERSECURITY SIMPLIFIED

WALLIX Group is a cybersecurity software vendor dedicated to defending and fostering organizations' success and renown against the cyberthreats they are facing. For over a decade, WALLIX has strived to protect companies, public organizations, as well as service providers' most critical IT and strategic assets against data breaches, making it the European expert in Privileged Access Management.

As digitalization impacts companies' IT security and data integrity worldwide, it poses an even greater challenge if the data involved is highly sensitive. The recent regulatory changes in Europe (NIS/GDPR) and in the United States (NERC CIP/Cyber Security Directorate) urge companies belonging to sensitive sectors to place cybersecurity at the heart of their activity.

In response to these challenges, WALLIX created a bastion designed to secure organizations' core assets while adapting to their daily operational duties: WALLIX Bastion. The WALLIX bastion accompanies more than 100 operators in sensitive sectors to conform with regulations and over 400 organizations in the protection of their critical assets, securing the access to more than 100,000 resources throughout Europe and the MEA region. It was also the first government-certified solution in the market.

WALLIX partners with a trained and certified network of over 90 resellers and distributors that help guarantee effective deployment and user adoption.

WALLIX is the first European cybersecurity software editor to be publicly traded and can be found on EuroNext under the code ALLIX. As one of the leaders of the PAM market, major players trust WALLIX to secure access to their data: Danagas, Dassault Aviation, Gulf Air, Maroc Telecom, McDonald's, and Michelin are among them.

WALLIX is the founding member of Hexatrust. The WALLIX bastion was elected "Best Buy" by SC Magazine and awarded at the 2016 Computing Security Awards, BPI Excellence, and Pôle Systematic.

Twitter: @wallixcom
More information on: www.wallix.com

OFFICES & LOCAL REPRESENTATIONS

WALLIX FRANCE (HQ)
http://www.wallix.com/fr
Email : sales@wallix.com
250 bis, rue du Faubourg Saint-Honoré
75017 Paris - FRANCE
Tél. : +33 (0)1 53 42 12 90
Fax : +33 (0)1 43 87 68 38

WALLIX UK
http://www.wallix.co.uk
Email: ukinfo@wallix.com
1 Farnham Rd, Guildford, Surrey,
GU2 4RG,UK
Office: +44 (0)1483 549 944

WALLIX DEUTSCHLAND
http://www.wallix.de
Email: deinfo@wallix.com
Landsberger Str. 398
81241 München
Phone: +49 89 716771910

WALLIX USA (HQ)
http://www.wallix.com
Email: usinfo@wallix.com
World Financial District, 60 Broad Street
Suite 3502, New York, NY 10004 - USA
Phone: +1 781-569-6634

WALLIX RUSSIA & CIS
http://www.wallix.com/ru
Email: wallix@it-bastion.com
ООО «ИТ БАСТИОН»
107023, Россия, Москва,
ул. Большая Семеновская, 45
Тел.: +7 (495) 225-48-10

WALLIX ASIA PACIFIC
(Bizsecure Asia Pacific Pte Ltd)
Email: contact@bizsecure-apac.com
8 Ubi Road 2, Zervex 07-10
Singapore 408538
Tel: +65-6333 9077 - Fax: +65-6339 8836

WALLIX AFRICA
SYSCAS (Systems Cabling & Security)
Email: sales@wallix.com
Angré 7ème Tranche Cocody
06 BP 2517 Abidjan 06
CÔTE D'IVOIRE
Tél. : (+225) 22 50 81 90

www.wallix.com