White Paper

Privileged Identity Management In Cloud

With cloud technologies adoption gaining pace, effectively securing sensitive data has emerged a big challenge for organizations. As they embrace new technologies, newer threats keep cropping up both externally and internally. Of late, internal threats seem to be far more alarming as many of the reported security incidents have been caused by malicious insiders having authorized or unauthorized privileged access to potentially hundreds of vulnerable privileged accounts present as inactive, shared, default, mis-configured or poorly secured logins.

The situation is further exacerbated with the presence and speedy advancements in automated hacking tools, which means that even a small number of inappropriately secured privileged logins are virtually certain to allow access to customers' private data within minutes of an incursion.

Today cloud infrastructure is not only required to deliver high service availability at an absolute minimum cost, but also ensure security for privileged accounts and other file-based secrets to check hackers and malicious insiders.

Overview

Organizations are increasingly leveraging the power of cloud technology to manage their activities and offer various services and store critical data, thus making security as the top concern. With cyber-crimes looming large and a spurt in automation of hacking tools, securing sensitive data is seen as a big challenge.

A single security breach can not only lead to financial and reputation loss but might jeopardize an entire setup.

The requirement to control privileged users and protect the sensitive credentials has been the primary concern forsecurity and audit teams and with he migration to virtualize and cloud -based computing infrastructure, these long-standing concerns have been further accentuated.

These environments have introduced new challenges and requirements for privileged identity management.

Over the past few years, many organizations recognized the chaos associated with privileged account security and made a number of tactical changes but in spite of all the progress made, privileged accounts remain vulnerable as tactical changes are not enough to counter sophisticated cyber-attacks.

Cloud Shift

It's not surprising to see that the cloud platforms are only getting bigger. But it's not to be assumed that companies are moving in one direction. There has been a constant shift observed between various cloud strategies and organizations are exploring all possible combinations (Public, Private & Hybrid) to seek a fitment for their business strategies or tech need.

A study has found that more than 50% cloud users have made secondary shifts of infrastructure or applications following their original transition to the cloud. With popular trends including movement from Public to Private or Hybrid models.

As cloud computing becomes a default part of the IT landscape, more companies are relying on cloud computing for business processes such as storage, business continuity management and security. Few points to highlight the rapid growth and popularity of cloud infrastructure:

- Total global spending on public cloud services will reach more than double by 2016.
- More than 30% of virtualized assets consist of mission critical applications.
- It's estimated that at least four-fifth of the growth in the IT industry will come from cloud services by the end of the decade.
- In the US, the federal government has mandated a policy, 'cloud first', for new IT initiatives.

With all its benefits, the cloud also brings significant challenges to the ability of organizations to effectively manage risks and demonstrate compliance. According to identity experts, most enterprises today still experience a big gap in visibility and accountability when it comes to managing privileged accounts in the cloud. A dangerous situation that poses all of the same kinds of insider risks associated with poor privileged account management under normal circumstances.

The Challenge

Traditionally the privileged account management was mainly taking into account two main factors:

- Insider Attacks
- Compliance and Audit Requirements

But with the advancement in the cloud infrastructure new breed of threats are evolving with hackers inventing new ways to attack the privileged accounts.

While organizations have made marginal adjustments to privileged account security over the past few years, they are likely missing ammunition to combat new dangerous threats. Privileged accounts are being used as part of engineered web attacksconducted by organized hackers. Since the Advanced Persistent Threat (APT) attack on Google in 2010, many organizations have found similar intrusion attempts.

Privileged accounts are being used as part of engineered web attacks conducted by organized hackers. Since the Advanced Persistent Threat (APT) attack on Google in 2010, many organizations have found similar intrusion attempts.

Achieving the highest level of security is the most desired goal for organizations. But given the immaturity of cloud security models this goal is fraught with quite a few challenges, leaving privileged accounts extremely vulnerable. Some of the root causes for compromised privileged accounts in a traditional system include:

Hidden Privileged Accounts - Many a times, organizations are simply not aware of all of the existing privileged accounts, owing to random creation of admin users for direct and contracted staff.

Distributed Privileged Accounts - Organizations lack central control over privileged accounts which are distributed over a sea of infrastructure devices.

Poor Password Management - Mostly it's the same password for various accounts. These passwords are seldom changed and mainly handled manually.

Lack of Accountability - With accounts/ passwords as shared entities among various resources it becomes highly untraceable on who accessed what all and when.

With cloud migration, the new challenges have found their way into the system and traditional methods of privileged identity may not just be unsuccessful, but may also become inapplicable. Cloud infrastructure demands a more reliable and robust security model with extended management capabilities.

PIM for Cloud

Cloud stresses first generation PIM solutions by adding new breed of resources for protection. These have opened significant new attack surfaces to be protected, which are beyond the capacity of traditional PIM solutions.

Choosing a right PIM solution could be very tricky and requires a lot of consideration to come up with a fitment for the underlying cloud strategy. Some of the key considerations, which could be helpful while adopting Next Generation PIM solution are :

- It must offer tight integration with these new cloud consoles and deliver an adequate level of control and appropriate separation of duties.
- It should have the ability to easily integrate with new set of tools including, IAM, SIEM and Ticketing with unique capabilities for cloud deployments.
- Ability to protect new kinds of resources like APIs, which expose much of the functionality and are a critical point.
- Isolation of access point from the targeted IT devices/applications in the cloud.
- Secured and centralizing control over privileged account functions like provisioning/de-provisioning, reporting and analytics.
- Define, implement, and enforce consistent set of policies across all the

- Define, implement, and enforce consistent set of policies across all the different platforms that comprise the cloud.

- Discover and manage on platform, which is not bound by an identifiable perimeter as in the case of traditional on premise or virtualized systems.

- Flexibility of deploying over a broad range of resources across the cloud; servers, databases, networking devices, management consoles etc.

Conclusion

New era of virtualization and cloud environments have undoubtedly bring newer challenges and requirements for privileged identity management solutions. As described, the next generation PIM will be required to deliver additional capabilities to effectively manage privileged user and protect organizations of unfavorable conditions.

About ARCON

ARCON is a leading Information Security solutions company specializing in Privileged Identity Management and Continuous Risk Assessment solutions. With its roots strongly entrenched inidentifying business risks across industries, it is in a unique position to comprehend and identify inherent security gaps in an organizations infrastructure framework and build and deploy innovative solutions/products to significantly mitigate potential risks.