WHITE PAPER

CLOUD PAM FOR ROBUST CLOUD SECURITY

May 21, 2019

Author by Adam Barngrover, Karen Walsh

CONTENTS

INTRODUCTION

Cloud migration, digitization, and IT modernization - all these terms describe using new technologies to ease business operation burdens and promote better customer experiences. While these new technologies empower businesses, they also create new risks to which the enterprises must respond.

According to Oracle and KPMG’s joint “Cloud Threat Report, 2018”:

90% of respondents store at least half of their sensitive data in the cloud

38% of respondents struggle with detecting and responding to cloud security issues

82% of respondents worry that employees do not follow cloud security policies

84% of respondents seek increased levels of security automation

Cloud Access Security Brokers (CASBs) and IGA legacy solutions show two sides of the same privacy and security coin.

A recent ISMG Security Report explained that while CIOs and CISOs recognize the data security risks arising from lack of Privileged Access Management (PAM), they struggle with:

- **Lack of policy and controls**
- **Complexity**
  - Cloud
  - Mobility
  - Employees
- **Outsourcing**
  - More than one individual administering systems
- **Trust in administrators**
  - Accidental misuse unexpected
- **Keeping systems running requires privileged access**
- **Lack of governance and enforcement**
- **Lack of reliable tools**

Not only do they still require IT administrators to manage multiple sources of information, they lack visibility into a primary privacy and security threat - Privileged Access. Connecting legacy solutions to the cloud differs from having cloud-native capabilities. Legacy solutions take time to connect to the cloud, but they do not live in the cloud. Therefore, they lack the ability to meet the speed and velocity of cloud activities.

Governing cloud identity requires proactive strategies that bring together all information about data access and use in a single location to streamline both business operations and compliance management.

CLOUD ENABLEMENTS: THE TRIFECTA OF COMPUTING POWER AND PRIVILEGED ACCESS MANAGEMENT RISK

IT modernization comes in a variety of forms. The first step to clearly defining who needs what access to data and how they access the resources requires outlining the enterprise cloud migration strategy.

The Greatest Risk to the Cloud? Privileged Access

The 2019 Verizon Data Breach Investigations Report (DBIR) noted that breaches arising from System Administrators increased between 2017 and 2019 while privilege abuse was the primary variety of misuse. Thus, with identity as the new perimeter, governance is the new strategic cybersecurity control, and continuous monitoring with intelligence is the new prevention.

The raw data used by the 2019 DBIR researchers highlights the impact a strong Cloud Privileged Access Management (PAM) program can have on data security and privacy. Under the "misuse" category, the researchers found the following varieties relevant to Cloud PAM and Cloud Security:

- **Data mishandling:** handling data in an unapproved manner
- **Email mishandling:** inappropriately using email or instant messenger
- **Knowledge abuse:** Abusing private or entrusted knowledge
- **Net misuse:** Inappropriately using network or web access
- **Privilege abuse:** Abusing system access privilege
- **Unapproved software:** using unapproved software or services
- **Unapproved workaround:** using unapproved workaround or shortcut

Misuse occurred across LAN access points, non-corporate facilities/networks, and remote access to networks. Although these misuse varieties led to data breaches, the research also notes that another result was elevation of privileges, or additional permissions arising from the misuse.

Embedded within the cloud security data, however, exists "user breakout" or elevation of privilege by another customer in a shared environment. Elevation of privileges within a shared environment can arise from collaboration tools or administrators escalating privilege without creating timebound deprovisioning.

With elevated privilege listed under both "misuse" and "cloud" categories, organizations need to ensure that they establish strong cloud IGA and PAM programs to limit misuse and protect data as they migrate to the cloud.

The Greatest Cost of a Data Breach? Time to Detect

While the greatest risk to data security is privileged access, the greatest cost is the time it takes an organization to detect and mitigate the threat.

continues

The 2018 Cost of a Data Breach Report notes:

- **$3.86 Million:** the average cost of a data breach
- **$12 per record:** the increased per capita cost per record when undergoing cloud migration
- **$160 per record:** the adjust data breach per record cost for organizations undergoing cloud migration
- **$3.11 million:** the average cost of a data breach when Mean Time to Identify (MTTI) was under 100 days
- **$4.21 million:** the average cost of a data breach when MTTI was over 100 days
- **$1.55 million:** the cost savings for a data breach when using automation

PAM's complexity increases the time it takes to identify a data breach arising from privilege misuse. As legacy solutions cannot meet the cloud's speed and velocity, they leave organizations open to higher data breach costs, particularly when compared with the increased number of data breaches arising from System Administrator accounts.

Software-as-a-Service (SaaS): The First Step

As companies begin to dip their toes in the waters of digitization, they often begin by creating suites of SaaS platforms. These applications enable them to streamline business operations but create more access points that increase risk.

For example, as business leaders seek to streamline their ERP systems using SaaS applications, their IT security departments struggle to maintain privacy and security across the ever-expanding ecosystem. According to the Oracle's 2018 report, "Securing SaaS at Scale," the mobile workforce redefines "perimeter" and legacy solutions cannot support the new cloud threat landscape. Similarly, the Cloud Security Alliance working group on Enterprise Resource Planning and Cloud Adoption noted in its 2019 "Impact of Cloud on ERP" report that the three key issues creating barriers to migration were:

Identity & Access

67.89% percentage of respondents using an Identity and Access Management tool

55.87% percentage of respondents using SSO and hybrid IT Infrastructures

78.85% percentage of respondents using Single-Sign-On for ERP

Time to Migrate

49.53% percentage of respondents said data migration took "much longer than expected" or "a little longer than expected"

Security & Compliance

59.05% percentage of respondents whose top concern was security

54.29% percentage of respondents whose top concern was compliance

64.76% percentage of respondents whose top concern was moving sensitive data to the cloud

continues

The disconnect between SSO use and IGA tool use indicates that although organizations express concern over compliance and security, they lack integrated tools that enable protection. SaaS applications require privileged access to databases or other applications across the overarching IT infrastructure. Their passwords, which often remain embedded and stored in unencrypted text files, create a security vulnerability. As cybercriminals increasingly use stolen credentials to gain unauthorized access to protected information, the passwords act as a point of entry. Even more disconcerting, as the applications interact throughout the cloud ecosystem and across multiple servers, this vulnerability exponentially impacts the whole organization.

Infrastructure-as-a-Service (IaaS): Step Two

With IaaS, organizations build their own clouds using platforms provided by cloud service providers (CSPs). Rather than leaving databases on premises, the enterprise moves data, operating systems, and applications to the cloud. While these services provide more mobility, they also create new security risks.

According to the McAfee "Cloud Adoption and Risk Report, 2019," the primary cloud adoption risks are:

Data Types:

21%	number of files stored in the cloud that contain sensitive data
17%	percentage increase in sensitive data stored in the cloud over the last two years
28%	percentage increase in confidential data stored in the cloud over the last two years

Sharing Data:

22%	number of cloud users share files in the cloud
48%	number of all cloud files are eventually shared
23%	increase in files containing sensitive information that are shared with "anyone with a link"

Insider and Privileged User Threats:

14.8%	average number of insider threat incidents per month
94.3%	average percentage of organizations experiencing one insider threat per month
4.3%	average number of privileged user threats per month
58.2%	average percentage of privileged user threats per month

As the enterprise adds more services to its IaaS, it adds more risk. The report further explained that of the 1,935 cloud services the average organization uses, 173 are considered "high risk" applications.

IaaS applications interact across an organization's ecosystem, often requiring privileged access to systems to interact with operating systems. These service accounts may have domain administrative privileges that require additional security controls and monitoring to ensure privacy and security.

Platform-as-a-Service (PaaS): The Final Frontier

PaaS enablements bring together SaaS and IaaS in one neatly tied package. They provide and operating system as well as linked applications. Thus, they offer flexibility and ease as the enterprise seeks to embrace cloud migration.

continues

While PaaS services bring together SaaS and IaaS enablements, they also create new challenges. Specific to PaaS, the journal article “MPSM: Multi-prospective PaaS Security Model” explains the unique data and infrastructure risks inherent in PaaS ecosystems:

- **Data location:** duplication of information in multiple locations that remain on the service provider’s network
- **Information leakage:** shared communication channels and resources can lead to “shadow IT” sharing similar to within an IaaS ecosystem
- **Privileged Access:** “built-in” debug feature grant privileged access to memory and data locations
- **Distributed system:** open default ports decrease visibility into how and where data can be accessed
- **Vulnerable hosts:** Multiple accounts (multi-tenancy) in PaaS ecosystem allows user objects to connect which leads to visibility issues that lead to infiltration

PaaS services lead to privileged access risk as they incorporate domain service accounts and require coordination across multiple systems. Within the PaaS environment, administrators need to apply access on a more detailed level. Traditional IGA services and privileged access management providers lack the ability to create fine-grained entitlements, such as limiting access at the file and folder levels. Coarse-grained entitlements, such as application level access, fail to secure privileged access in the cloud.

Securing identity and proving governance over access and use becomes challenging as the enterprise adds more human and digital users to its cloud. Once the enterprise ensures that the cloud environment is secure, it must also find an Identity Governance and Administration (IGA) solution to enable authentication, authorization, and traceability.

Conclusion

“As the data shows, organizations migrating to cloud infrastructures place themselves at a greater data breach risk. Whether using SaaS, IaaS, or PaaS platforms, organizations use collaboration tools for business enablement and customer-facing applications to increase customer engagement. However, organizations need to stay focused on their risk tolerance levels when incorporating new technologies. Managing Privileged Access needs to be a primary focus for securing these cloud enablements.”

THE SHARED RESPONSIBILITY MODEL: WITH GREAT POWER COMES GREAT RESPONSIBILITY

Computing power and the use of cloud ecosystems empowers organizations to scale. However, that power also comes with responsibility.

continues

Secure Service versus Secure Use

The Shared Responsibility Model requires the CSP to protect physical security, hardware security, and, in the case of PaaS operating system providers, operating software security. The customer is responsible for data, data classification, and user access controls to reading or writing to different environments within the cloud. With PaaS, for example, the CSP secures the operating system while the customer needs to control user access and user interaction with the resources.

According to Jonathan Trull, the chief cybersecurity strategist of enterprise security for Microsoft, an attack on the cloud often arises from remote desktop protocols (RDP), or the program function that allows computers to connect to the cloud so they can “talk” with one another. Organizations often only secure these with usernames and passwords. Cybercriminals obtain the information using brute force attacks, where they use software to compare known passwords with all known user logins. Given the number of users with weak passwords, this attack methodology is often successful.

As the organizations scale, the number of privileged accounts also increase. Moreover, many of these privileged accounts - such as domain service or application service accounts - retain a single, unencrypted password that makes them a primary target for cybercriminals.

Why Organizations Struggle with the Shared Security Model

The Shared Security Model for Cloud Services establishes a complex network of interrelated, and often ambiguous, requirements. While it might seem easy to understand the “secure service” versus “secure use” concept, interconnected cloud subscriptions and applications create a complex web of related identities - human and digital - that overlap and create visibility issues.

Service Level Agreements

When working with CSPs, organizations often rely on their service-level agreements (SLA) to define cybersecurity liability. However, each CSP provides its own SLA with its own language. Some SLAs define the responsibilities clearly while others use vague language. As enterprises increasingly embrace a multi-cloud strategy, they need to navigate the differing identity and access control requirements.

IaaS and PaaS infrastructures provide an example of the differences. Organizations contracting with IaaS providers must maintain governance over all service accounts - at both the application-to-operating system level and the domain service level. However, within a PaaS infrastructure, the governance shifts as the CSP must secure access to the operating systems in the cloud.

Access and Use Visibility

SaaS, IaaS, and PaaS infrastructures add value to the organization because they allow different business areas to communicate more effectively. Simultaneously, that increased connectivity decreases visibility. Employees and the cloud are both dynamic entities which means that movement and data access change daily.

continues

When the organization is unable to detect anomalous use, such as launching new instances, it places itself at a financial and data security risk. These instances create a significant privileged access risk as they often require just-in-time privilege escalation which can be left unattended leading to infiltration.

Trust Management and Policy Integration

In cybersecurity, trust management means that the organization has authorized and authenticated all identities within the system. However, increased robotic process automation enables remote system management but opens organizations up to risk because the way they exchange data lacks visibility, transparency, and auditability. Traditionally, organizations create policies to control user access to data and systems then engage in periodic reviews.

However, the expanded digital definition of identity now incorporates third-party applications that require access as well as internal and external human users. “Set and forget” policies no longer protect organizations since as the organization incorporates more interconnected applications, the service accounts can lead to a privileged access risk.

Privacy and Security Compliance: The Financial Risk

Struggles with the Shared Responsibility Model create financial risk arising from non-compliance with increasingly stringent regulatory requirements. 2019 brings with it enhanced due diligence, monitoring, and governance requirements to mitigate risks and protect from fines and penalties.

General Data Protection Regulation (GDPR): Data Protection by Design and Default

The GDPR’s strict controls require organizations to enforce user access. Specifically, Article 25 states:
. . . such measures shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons.

Thus, to meet GDPR objectives under article 24, data controllers need to ensure that they not only limit access from external actors but also internal actors. Data access is paramount to maintaining GDPR compliance.

New York Department of Financial Services (NY DFS) Cybersecurity Rule

Enforcement of NY DFS Cybersecurity Rule begins in 2019. As covered entities seek to meet the cybersecurity program requirements, they need to focus on access controls and identity management. Under Section 500.07, the Rule specifies:

As part of its cybersecurity program, based on the Covered Entity’s Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.

California Consumer Privacy Act (CCPA)

Similar to the GDPR, the CCPA focuses on maintaining data privacy while embedding security concepts within it. In the preamble, the CCPA states,

The bill would provide for its enforcement by the Attorney General, as specified, and would provide a private right of action in connection with certain unauthorized access and exfiltration, theft, or disclosure of a consumer’s non-encrypted or non-redacted personal information, as defined. The bill would prescribe a method for distribution of proceeds of Attorney General actions.

In addition, the CCPA also requires companies that collect information to verify customer identity in response to customer requests protected under the act.

While this list of regulations is not exhaustive, it highlights the similarity in regulatory provisions. As such, organizations need IGA solutions that manage internally and externally facing cloud applications to meet privacy compliance requirements.

THE LIMITATIONS OF CURRENT CLOUD PRIVACY AND SECURITY PROTECTIONS: THE PAM PROBLEM

IGA holds the key to protecting and securing data in the cloud. However, as organizations move from on-premises to hybrid infrastructures, ultimately seeking to transition to full cloud ecosystems, they find that their legacy IGA tools fail.

Interconnectability, while increasing business operation efficiency, leads to needing multiple tools to control access. As they add more integrations and more identities, they find the tasks overwhelming, lacking a single source of information and insight.

Digital Identity

With the plethora of digital identities, most organizations seek to create federated solutions using SSO. While federation protects access to the organization’s cloud, it does not provide the necessary access controls to protect access within the cloud.

Federation lacks the ability to govern privileged access to systems and data within the cloud which means it cannot protect against a cybercriminal stealing privileged credentials and accessing the cloud ecosystem.

Access Control

Creating RBAC/ABAC entitlements focuses on who people are and provides them with attributes related to job function or group roles. However, legacy systems fail to incorporate context which can lead to excess access within the cloud, such as “share with anyone who has the link” access risks.

An administrative account sharing just-in-time access creates the same type of risk. However, instead of a single file, the access can impact the entire infrastructure’s security if not deprovisioned in a timely manner.

Interoperation

Interoperability between systems and networks creates another unique problem when trying to secure access to data. Traditional static identity establishment fails in the cloud. Identities - digital and human - shift to interact with information and each other in new, constantly evolving ways.

Organizations need to adopt dynamic identities that address the way people, devices, and systems connect to one another requires continuous monitoring to ensure appropriate “least privilege necessary” access. Monitoring service accounts and domain service accounts for privileged access within the ecosystem better protects organizations using multiple cloud services and applications.

Virtualization Technologies

Virtualization technologies increase application performance while driving down costs. Segregating and masking networks, storage, and servers in the cloud increases resource sharing while also creating new risks by adding more identities that the organization must manage.

Automatic service provisioning in the complex IT infrastructure can lead to human error as the organization’s IT administrators manage provisioning/deprovising across the ecosystem. Unfortunately, most IGA and cloud PAM enablements lack the intelligent analytics to delegate authority based on policies and risk.

Interdomain Access Requirements

Embedded within the interoperability and virtualization struggles, IGA risks associated with interdomain access requirements increase the likelihood of data breaches. Creating a global policy and using role mining technologies ease the burdens associated with the privilege delegation necessary to streamline business operations in the cloud.

However, legacy solutions fail to create roles that ensure “least privilege necessary” across multiple domains and domain service accounts. Thus, organizations find themselves burdened by multiple solutions with different RBAC/ABAC controls as they attempt to create a cohesive IGA program.

Data Centric Security and Privacy

Data owners need to maintain control over their information assets. Collaborative platforms enable individual users to share and change information sharing settings which ultimately remove data owner control. Data centric security requires setting folder and file descriptions that retain data owner control across disparate environments to reduce risk and ensure privacy. Moreover, as data access changes dynamically, data owners need to continuously monitor for anomalous access to ensure compliance with policies.

ENSURE PRIVACY WITH CLOUD PAM FOR ROBUST CLOUD SECURITY

Cloud Privileged Access Management

As organizations migrate to the cloud, they need automation tools that provide a single source of information for governing access within the cloud infrastructure. Current models typically require multiple user IDs - one for business productivity and one for administrative activities - which increases the number of potential access points as well as the amount of monitoring required. Additionally, organizations need an integrated solution that provides IGA and PAM capabilities for the cloud rather than segregating them across multiple platforms.

To accelerate cloud migration strategies, organizations need secure vendors who enable privilege access and assignment management. Granular entitlements ensure access and data use continuity across the ecosystem. Enterprises need a solution that extends governance to privilege and service account ownership enabling user/group based ownership, periodic ownership certification/review, event-based/transfer ownership review, password management policy enforcement, and privilege/service account provisioning.

Maintaining Effective Security Across IT Environments

To meet their strict regulatory requirements, organizations need to engage in continuous monitoring over data access and user access/authentication. To protect integrity, confidentiality and accessibility, the organizations needs granular identity management and visibility across all user behavior. Additionally, the organizations needs intelligent analytics that compare users to their peers to ensure stronger identity access governance across all IT environments.

Maintaining Effective Security Across IT Environments

Continuous monitoring provides visibility into potential vulnerabilities that affect the cloud ecosystem. Peer group analytics and reporting tools providing documentation supporting continuous monitoring to enable a robust compliance program when they alert IT managers to anomalous access activities. Proving governance requires granular audit logs directly from the CSPs rather than keystroke logs to document continuous monitoring and assurance activities.

continues

Organizations also need their continuous monitoring to meet the speed and velocity of the cloud. Automated tools need to discover new workloads and mitigate risks in real-time rather than waiting for their traditional PAM solutions, which can take hours or days.

Infrastructure & Identity Lifecycle Governance

Organizations struggle to adopt cloud strategies because internal and external users change roles continuously. To monitor identity lifecycle governance, organizations should incorporate tools that automate SOD controls (including privileged accounts), take a risk-based approach to data and user access, enforce joiner/leaver/mover policies, connect roles to human resources job descriptions, and continuously monitor for out-of-band access.

Automation Eases Compliance Burdens

Automating the access lifecycle of users, groups, roles and federated access points ensures that organizations maintain compliance with internal controls for onboarding and role updates. With an intelligent access request tool, organizations can enable self-service, automate identity and access provisioning/deprovisioning rules, as well as Segregation of Duty (SOD) management on site and in the cloud.

WHY SAVIYNT? ASSURED COMPLIANCE-AS-A-SERVICE

Intelligent Identity. Smarter Security.

Saviynt’s platform is the first and only FedRAMP Authority-to-Operate (ATO) approved IGA service, giving customers assurance over our security practices to streamline vendor risk management practices.

We use intelligent analytics to provide peer-group based insights giving context for how users access data that ease provisioning and deprovisioning burdens. Moreover, our peer-group analytics automate risk analysis protecting the organization from potential Segregation of Duties violations by offering preventive actions.

Using our data access governance solution, organizations can create fine-grained entitlements that go beyond application and delve into rights and privileges at the file and folder level. These detailed privileges enable continuous monitoring and protect against the “anyone with a link” risk.

With Saviynt’s Cloud PAM solution, organizations can mitigate the risks associated with privileged access in the cloud. Saviynt’s Cloud PAM solution works inside the organization’s cloud to attach rights and privileges to identities so that organizations can streamline their governance. Rather than creating additional user accounts for privileged access that need to be monitored, Saviynt’s Cloud PAM solution enables administrators to assign timebound permissions to identities and then provides alerts to help remediate risks.

continues

As a cloud-native solution, Saviynt is the only platform that provides visibility into all data access and use while also enabling documentation in a single location. Our user friendly interface eases Identity Governance and Administration across the cloud ecosystem, securing data and ensuring privacy.

LEARN MORE

FIND OUT!

Why Saviynt received the highest product score for Midsize or Large Enterprise and Governance-Focused use cases in Gartner’s 2018 Critical Capabilities for Identity Governance and Administration.

CONTACT US

info@saviynt.com

ABOUT SAVIYNT

Saviynt is a leading provider of next generation **Identity Governance and Administration solution for Data, Infrastructure and Critical Applications in the Cloud and Enterprise**. Saviynt combines traditional IGA features with advanced usage analytics, data or infrastructure access governance, behavior analytics, real-time threat detection and compliance controls to secure organization's critical assets.