Centrify®

DISCOVER IDENTITY-CENTRIC PAM
TO ENABLE CLOUD TRANSFORMATION

BEST PRACTICES FOR SECURELY MOVING WORKLOADS TO THE CLOUD

www.centrify.com

ABOUT CENTRIFY

Centrify is redefining the legacy approach to Privileged Access Management by delivering multi-cloud-architected Identity-Centric PAM to enable digital transformation at scale. Centrify Identity-Centric PAM establishes a root of trust, and then grants least privilege access just-in-time based on verifying who is requesting access, the context of the request, and the risk of the access environment. Centrify centralizes and orchestrates fragmented identities, improves audit and compliance visibility, and reduces risk, complexity, and costs for the modern, hybrid enterprise. Over half of the Fortune 100, the world's largest financial institutions, intelligence agencies, and critical infrastructure companies, all trust Centrify to stop the leading cause of breaches — privileged credential abuse.

To learn more visit www.centrify.com.

Introduction

Driven by the promise of cost savings, speed, and scalability, enterprise cloud adoption is surging forward. A 2020 survey of cloud users and decision-makers by Flexera found that 93% have a multi-cloud strategy. Eighty-seven percent said they have a strategy for hybrid cloud.[1]

These types of IT environments have become the rule, and they have brought with them new levels of complexity — not the least of which involve ensuring security. Last year, research from Centrify entitled *Reducing Risk in Cloud Migrations* found that 60% of respondents viewed security as the main challenge for cloud migration projects. Often, the difficulties organizations face are rooted in misunderstandings of the concept of shared responsibility and a failure to extend the same security protections from their on-premises environment into the cloud.

The leading challenge facing cloud migration projects is **security**, selected as a top consideration by **60%** of survey respondents.

The penalty for failure is high. Data breaches in the cloud due to misconfigurations and user credential abuse have increased in the past few years, and the resulting costs of the ensuing customer churn, incident remediation, and reputation damage remain significant.

In this environment, enabling the secure migration of workloads to the cloud empowers businesses to seize the advantages provided by cloud computing without compromising security or compliance. Doing that successfully, however, requires a security strategy supported by effective identity and access management (IAM). In this white paper, we will discuss how businesses should approach migrating data and applications safely to the cloud, and the strengths and shortcomings of the strategies many enterprises are using today.

Key Takeaways:

- Putting identity at the center of security efforts is critical to stopping attacks due to the threat of privileged credential abuse and the requirements of regulatory compliance.
- Multi-directory brokering leverages an organization's preferred directory to authenticate users across their hybrid environments, reducing the attack surface by only requiring IT to maintain a single logical directory for their hybrid or multi-cloud infrastructure.
- Best practices for protecting the cloud include consolidating user identities, ensuring accountability, auditing everything, enforcing least privilege, leveraging multi-factor authentication (MFA), and adopting a common security model across cloud and on-premises environments.

Flexera, 'Flexera 2020 State of the Cloud Report,' April 28, 2020, https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020.

Cloud Computing: Understanding Security Risk

The growth of cloud services has facilitated the digital transformation modern businesses are experiencing. With its scalability and ease of deployment, cloud computing has led to faster application development and deployment cycles and fundamentally altered IT consumption. It has also enabled the creation of new revenue streams for businesses. Companies not aboard the cloud computing train will have little choice but to join in soon.

For IT leaders, having to migrate workloads to the cloud is not a question of if, but when. Yet the adoption of cloud services has brought more than speed and scalability to the enterprise. It has also brought a new layer of complexity and added management, governance, and integration challenges. But perhaps the biggest challenge of all is securing the multi-cloud and hybrid environments enterprises are now responsible for. As organizations migrate their IT infrastructure to the cloud, they need to adopt the correct approach to security to protect against cyber-threats — an approach focused on secure access.

FIGURE 1: Cybersecurity Threats: Eight Critical Principals, IDC

There are several threats to cloud platforms, from DDoS attacks to ransomware. However, it is privileged credential abuse that poses the most significant risk. Phishing attacks are increasingly targeting credentials for cloud services. Adding to this problem is the number of reported data breaches caused by misconfigurations, which rose significantly between 2018 and 2019. Misconfigurations are a common cause of data breaches affecting infrastructure-as-a-service (IaaS) deployments and can take several forms, such as poorly managed permissions, a failure to restrict inbound traffic on port 22, and more. But whatever their technical cause, misconfigurations related to access are rooted in an inability to properly define and apply the appropriate policies, user roles, and privileges.

Some of this failure can likely be attributed to misconceptions about the shared responsibility model, which delineates what elements of security are the responsibility of the enterprise versus the cloud provider. In the Centrify study noted earlier, 60% of respondents said they believe the service provider is responsible for securing privileged access, even though the shared responsibility model makes it clear it is the job of the customer. Like in an on-premises environment, it takes only one stolen or compromised credential to enable data theft in the cloud. Identity is the connective tissue between administrative users, on-premises systems, and the cloud, and it is the inability to protect and manage those identities that is a common thread between cloud data breaches. Protecting the cloud environment requires adopting an identity-centric approach based on Zero Trust principles that enforce least privilege for access permissions.

Identity at the Center of Security

As the traditional network perimeter has disappeared, the focus for forward-thinking companies has shifted away from the trust-but-verify approach of the past. Instead, security teams must switch to a never trust, always verify paradigm. This change is necessitated by the distributed nature of today's workforce, the increase of outsourced IT, and the explosive growth of mobile devices and cloud services. With this backdrop, managing user identities and verifying who is trying to access critical resources are crucial parts of defending against attacks. Information about access requests should be gathered and contextualized to provide the basis for sound decisions. If a database administrator (DBA), for example,

wants access to a database, the access decision should be based on details such as whether or not there is a trouble ticket for that particular database. If the DBA is attempting to access a database for no apparent reason, it could be a sign of malicious activity.

Such security controls need to be risk-aware and powered by user behavior analytics. If a user is taking an action that is out of the norm or attempting to access an enterprise resource from an atypical location or during unusual hours, additional verification steps can be applied. Chief among these steps is multi-factor authentication (MFA), which can be utilized in response to suspicious activity or policy violations.

Unfortunately, many organizations are not putting these security best practices in place for the cloud. According to Centrify's survey, only 60% said they used MFA for all privileged access to their cloud environment. Nearly 68% admitted they are not eliminating local privileges in favor of federated access controls, and 57% are not implementing least privilege to limit lateral movement in the event of a successful attack.

60%

of organizations surveyed said they used MFA for all privileged access to their cloud environment.

68%

Nearly 68% admitted they are not eliminating local privileges in favor of federated access controls and…

57%

are not implementing least privilege to limit lateral movement in the event of a successful attack.

Centrify, 'Reducing Risk in Cloud Migrations'

As organizations migrate to the cloud, legacy approaches to privileged access management (PAM) need to be abandoned. In the days when organizations only needed to worry about protecting data and systems on-premises, legacy PAM worked fine. When system administrators required access to servers, they would check out a shared privileged account from a password vault; the approach scaled well. PAM today, however, must be automated for hyper-scale — it must extend out to cloud environments and cover hundreds of containers in addition to access requests from machines, services, and APIs. Guarding against cloud data breaches means defending a much broader attack surface, and accomplishing those goals takes a comprehensive strategy rooted in practices that should follow workloads from the data center to the cloud.

Security Strategy for the Cloud

After an organization has identified its security and compliance requirements and selected a cloud provider, it can begin developing a plan for the actual migration. To migrate workloads safely to the cloud, enterprises need an approach underpinned by six critical best practices:

- Develop a common security model
- Consolidate identity
- Audit everything
- Ensure accountability
- Use multi-factor authentication
- Implement least privilege

The first point is often a source of confusion. One of the myths surrounding cloud security is that organizations need to adopt a security model that is different from their strategy for their on-premises environment. However, that is not true — all your policies and roles should migrate to the cloud and be the same as in the data center. The same security and compliance concepts still apply both on-premises and in the cloud, and the roles and responsibilities assigned to users should be the same to maintain alignment with the demands of regulations.

Along these same lines, just as identity access management best practices in the on-premises environment call for identity consolidation in the name of security, so too does the cloud environment. Identity sprawl broadens the attack surface and occurs when unsynchronized, siloed directories manage user identities. To avoid this situation, organizations should rely on a central directory and use federated login. By standardizing on a single identity repository, enterprises with hybrid environments can reduce risk.

Visibility and accountability are also critical and must be maintained at all times. Through continuous auditing, logging, and monitoring of user sessions, organizations ensure that any activity can be traced back to a single individual user. This ability is vital for demonstrating compliance with certain industry regulations. Regulations such as PCI DSS and Sarbanes-Oxley (SOX) apply the same in cloud environments as they do in the data center. Auditing guarantees accountability and enables enterprises to see who is behind a particular access request. By focusing on audibility, organizations can ensure they can still prove they are abiding by the regulations regardless of where sensitive data resides.

The final support beams for an effective identity-centric approach are the implementation of MFA and least privilege. MFA provides an additional layer of security verification and can be triggered based on any number of factors, including the sensitivity of the resource a user is attempting to access. In this way, MFA helps organizations enforce the principle of least privilege and only give users the permissions they need according to their role. Having the ability to limit privileges to basic entitlements for the minimum amount of time needed to accomplish a specific task prevents unauthorized lateral movement on the network and shrinks the potential threat surface. Elevation of those privileges should be governed by dynamic access controls, which can be configured to only allow users to elevate privileges according to specified criteria, such as a specific amount of time or on a particular server. In this way, users are granted just enough access for just enough time, reducing the risk to corporate resources.

Applying Best Practices to Use Cases

Each of these best practices strengthens security practices around identity management for organizations looking to migrate to the cloud. During migration projects, there are two primary use cases where these best practices should be brought to bear — securing access to the cloud service management console and securing access to cloud instances and containers.

1 Securing access to the cloud service management console

2 Securing access to cloud instances and containers

In the first scenario, there are three issues for organizations to take care of: vaulting the root or billing account credentials to protect the keys to the kingdom, leveraging SAML-based federation instead of creating individual IAM accounts for admins that will have to be managed, and implementing the principle of least privilege.

For organizations seeking to enable secure access to cloud instances and containers, there are three considerations as well: protecting shared accounts and remote access, enforcing multi-factor authentication, and extending enterprise authentication to the cloud. Some IaaS providers have offerings to help organizations migrate Active Directory (AD)-aware, on-premises workloads.

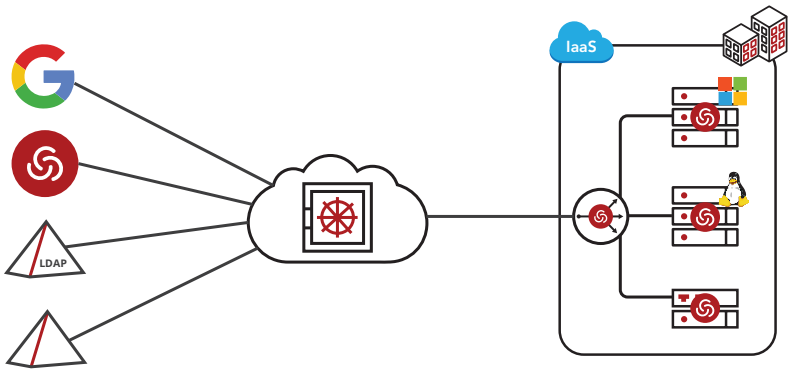
Many organizations attempt to address their needs with a homegrown hack — for example, a self-managed version of AD deployed on a cloud instance. Here, AD is duplicated in the cloud and can be protected by a site-to-site VPN connection with the cloud provider's virtual network. It also can create its own set of problems, such as the cost of having site-to-site VPN, a lack of centralized management, and limited migration opportunities if the enterprise decides to switch IaaS providers. In addition, this approach would have to be duplicated any time a new cloud service is added.

Another strategy is to leverage an on-premises password vault for local admin accounts. In practice, this approach means no directory access to user accounts for authentication and separate secrets management. It also requires a VPN for remote SSH or RDP sessions. While this is a more strategic way to address security concerns, it comes with drawbacks. For example, this approach will require constant synchronization across the different system elements, leading to increased latency.

Multi-Directory Brokering: Scalability and Security

There is a strategy, though, that solves many of the challenges enterprises face regarding identity in the cloud: multi-directory brokering. Brokered authentication enables organizations to migrate workloads into the cloud while still leveraging their preexisting corporate directory. This approach, in effect, eliminates the need for IT to replicate their enterprise directory infrastructure for the cloud. Rather than replicate on-premises AD for every new cloud platform that is adopted, enterprises can leverage a connected gateway to broker access.

In this model, users could log into Windows or Linux compute instances using their corporate account without the instances needing direct visibility into the corporate user identity store. This strategy avoids exposing the directory externally and removes the need to pay for a site-to-site VPN. Access decisions can be made based on a single identity instead of having to manage user identities across multiple directories. As a result, if an enterprise using Active Directory acquires a company using a different identity repository or with multiple cloud platforms, a multi-directory brokering approach can scale and handle authentication across the different environments.



From the standpoint of security, leveraging this approach reduces the attack surface by eliminating local accounts and decreasing the number of passwords. It is also scalable and supports multiple cloud environments and directories without requiring synchronization.

Migrate to the Cloud Securely

Cloud computing has ushered in new opportunities for businesses to increase agility, cut costs, and scale to seize the possibilities offered by digital transformation. For enterprises to move to the cloud with confidence, IT must maintain the appropriate security levels across its entire infrastructure, and implement the same rules, roles, and permissions in the cloud. Doing so not only reduces complexity, it significantly increases your compliance posture. Dynamic, context-aware security controls that enforce least privilege and enable privileged access decisions based on behavioral analytics offer an additional layer of security to bolster best practices around identity.

As cloud adoption continues, unifying IAM efforts across hybrid environments through strategies such as multi-directory brokering while maintaining the visibility and audibility companies need remains more vital than ever. Implemented properly, secure access controls empower businesses to migrate to the cloud safely.

Discover Identity-Centric PAM for Cloud Transformation

Centrify's Identity-Centric Privileged Access Management (PAM) solution empowers organizations to deal with the security and operational challenges surrounding moving existing workloads into hybrid or even multi-cloud environments. Instead of creating new identity silos or managing local accounts with cloud provider IAM, cloud-centric organizations can leverage their existing enterprise directories with the help of Centrify Brokered Authentication Service.

Taking advantage of these capabilities, users can now log into Windows or Linux cloud instances using their corporate account without the instances needing direct visibility to the corporate directory. This method is not only quick and easy, but more secure than the alternatives. Since the Centrify Gateway Connector maintains a persistent outbound connection to the Centrify Platform, there's no need to poke additional holes in the firewall.

Through its hub-and-spoke architecture, Centrify is uniquely positioned to secure access to systems hosted in DMZs, LANs, private clouds, and public cloud environments. And all of it at hyper-scale and without any additional cost impact.

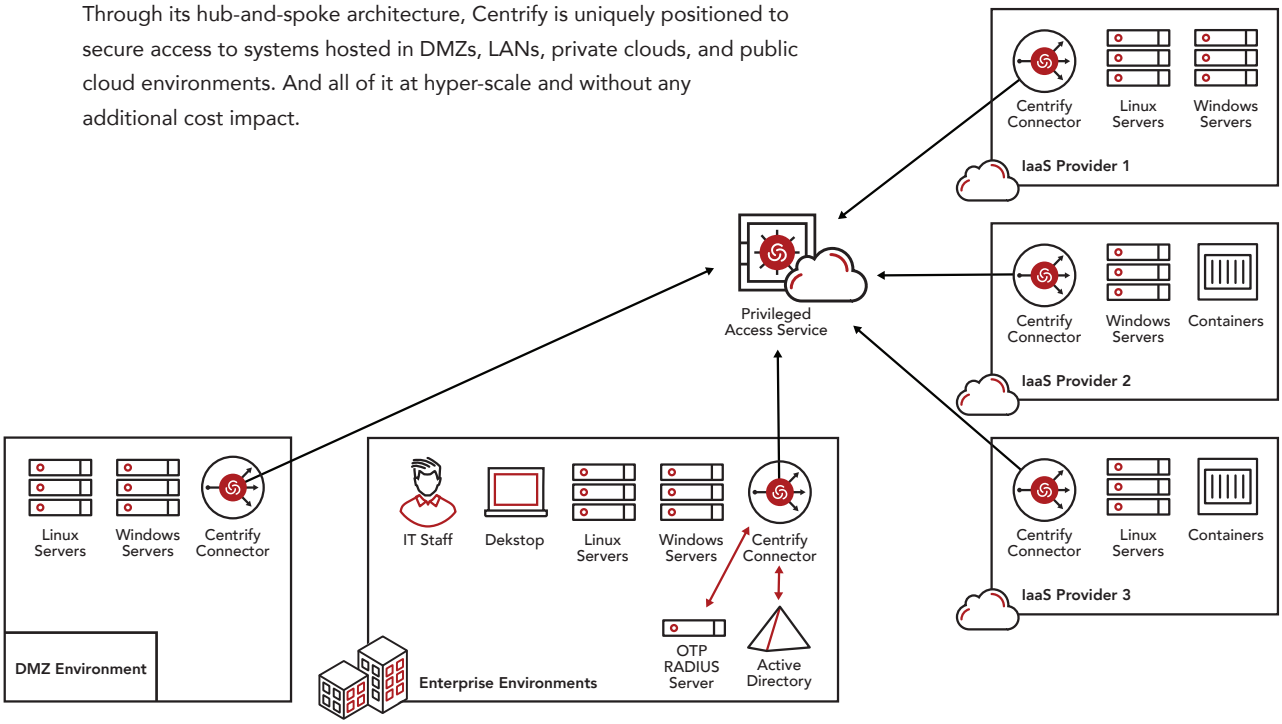


FIGURE 2: Centrify Centralized Authentication Service with Multi-Directory Brokering Capabilities

In the context of securing access to the hybrid or multi-cloud environments, Centrify's Identity-Centric PAM solution delivers

- Centralized vaulting for local admin accounts
- Authentication brokering service for enterprise directory user login
- Service account management with authentication services
- Centralized secrets management service
- Multi-factor authentication brokering service
- Remote SSH or RDP sessions without VPN

In turn, organizations can easily extend corporate security policies and best practices to cloud environments, while reducing costs (e.g., by avoiding site-to-site VPN for identity directory synchronization purposes), improving scalability across multi-VPCs/VNets, -SaaS, and -directory environments, and minimizing security blind spots through centralized management.

Centrify enables digital transformation at scale, modernizing how organizations secure privileged access across hybrid- and multi-cloud environments with Identity-Centric PAM based on Zero Trust principles. To learn more, visit **www.centrify.com**.

US Headquarters +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Asia Pacific +61 1300 795 789
Brazil +55 11 3958 4876
Latin America +1 305 900 5354
sales@centrify.com

www.centrify.com