SOLUTION BRIEF

Centrify
THE BREACH STOPS HERE

aws partner network
Advanced Technology Partner

Increase Security for Amazon Web Services (AWS) Environments

Centrify offers the benefit of tremendous flexibility and elasticity. However, as organizations migrate to the cloud, they face new considerations as they try to maintain their risk posture and prove compliance. It's important for a business to understand that flexibility requires a focused approach to maintaining centralized management of privileged access security for infrastructure and apps. Amazon Web Services (AWS) is quickly becoming one of the most popular options for enterprises who want to extend their data center infrastructure to the cloud, providing best practices to help ensure security as they move to the cloud. Centrify delivers a solution for AWS that implements and extends their best practices by securing access, controlling privilege and auditing activity across hybrid environments.

Challenges in Adopting Infrastructure-as-a Service

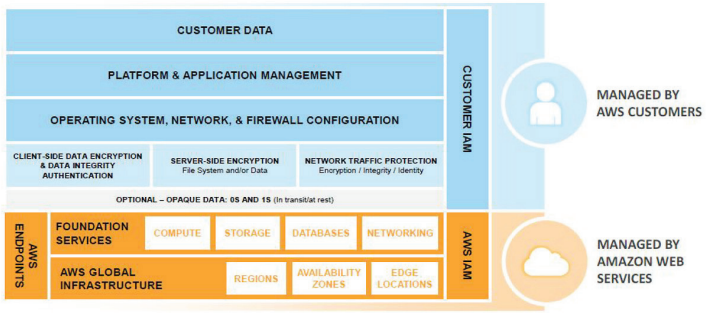
Enterprise IT organizations are increasingly extending their data centers with a cloud environment. According to a recently commissioned Forrester survey, 93% of decision-makers surveyed said that their organization stores sensitive data in the cloud. This adoption of cloud-based infrastructure and apps drives the need to secure privileged access across on-premises, private-cloud and public cloud environments with a single solution.

Centralized IT organizations cite cloud security as one of the top concerns, along with integration complexities, access and privilege management and app authentication.

Gartner predicts that "through 2020, 95% of IaaS security failures will be the customer's fault, and more than half of those will be attributed to inadequate management of identities, access and privileges."

Organizations adopting IaaS want to realize the benefits of the cloud, while maintaining the same level of privileged access security they currently have on-premises. They need to secure access to the IaaS management services, server instances and hosted applications.

To ensure their customers understand their security responsibility, AWS has established security best practices outlining their Shared Responsibility Model.

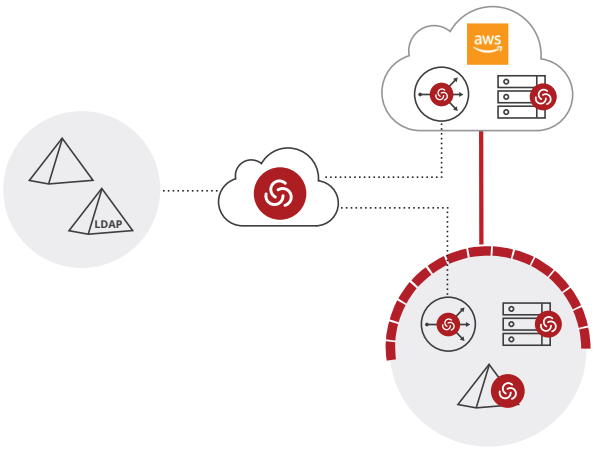


Source: Amazon Web Services Security Best Practices, August 2016

Leveraging built-in IaaS security is a great start, but this approach only covers a portion of the AWS' Shared Responsibility Model. AWS provides an excellent layer of foundational security for services, but their shared responsibility model is clear — "businesses are still responsible for the confidentiality, integrity, and availability of their data in the cloud."

Centrify Solutions for AWS

Centrify simplifies and streamlines adoption of IaaS by implementing and extending AWS security best practices by vaulting the built-in root account, controlling access to the AWS Management Console leveraging AWS IAM roles, and securing privileged access to Amazon Elastic Compute Cloud (Amazon EC2) instances and the applications that run on them.



Centrify's solutions ease the move of an organization's infrastructure and apps to AWS so they can take advantage of the benefits of the cloud, while allowing them to maintain the same level of privileged access security and enterprise access they currently have on-premises.

Centrify Application Services and Infrastructure Services provide the following capabilities aligned with AWS' best practices:

- Secure built-in AWS root accounts and federated SSO access to all AWS accounts leveraging corporate credentials
- Secure remote access to Amazon EC2 instances and identity brokering for authentication to Linux servers from a directory of your choosing (Active Directory, LDAP, G-Suite, Centrify Cloud Directory)
- Comprehensive bridging and policy enforcement of non-Windows Amazon EC2 instances leveraging Active Directory
- Granular role-based access with dynamic and policy driven, privilege elevation, session auditing and monitoring

Secure AWS Service Management

Centrify enables secure access to the AWS console by vaulting the built-in AWS root account, precluding the need for long-lived access keys. For break glass access, enforce workflow approval and enforce multi-factor authentication as an additional layer of security.

Secure Privileged Access for Amazon EC2 Instances

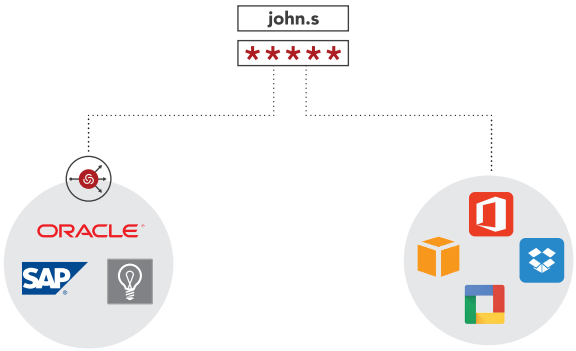
Securely extend your enterprise authentication services to AWS without replicating identities or identity infrastructure. Broker identities from a directory service of your choice — Active Directory, LDAP and cloud directories such as Centrify's and G-Suite. Users log in as themselves to perform their daily tasks, and IT users elevate privilege only when needed. This least privilege approach is highly recommended for reducing the attack surface.

Federated Access to AWS and Business Apps

Centrify enables federated authentication to the AWS console and business applications for employees, business partners and customers. Automatically provision access to one or more AWS accounts with role based access while securing AWS and other business applications with adaptive MFA and risk aware policy driven access controls. Reduce the attack surface by providing per-app VPN-less access to internal applications.

Multi-factor Authentication

To prevent unauthorized access, it's important to ensure a second factor of authentication is implemented when the need arises, especially for remote and third party users. Centrify provides multi-factor authentication across the enterprise for access to infrastructures and apps, at password checkout, endpoint login, session initiation, server login or when elevating privilege.



Privileged Activity Auditing and Compliance

Centrify's privileged access security solutions provide session auditing, video replay, search capabilities and comprehensive reporting for Amazon EC2 instances to effectively establish accountability and streamline regulatory compliance.

Centrify and AWS — Better Together

As customers move to cloud architectures to complement their existing investments, there has been a big focus at Centrify to enable support for dozens of AWS use cases to support customers on their journey.

As a result, it was important for Centrify to build Privileged Access Security and Active Directory integration solutions for AWS. These integrations are in production at some of the largest Centrify and AWS customers, such as a major U.S. credit card issuer.

The combination of Centrify solutions with the power of AWS has helped customers save millions in operating expense while increasing security for end users and privileged users which Centrify and AWS can bring you.

Centrify
THE BREACH STOPS HERE

As the only industry recognized leader in both Privileged Identity Management and Identity-as-a-Service, Centrify provides a single platform to secure every user's access to apps and infrastructure in today's boundaryless hybrid enterprise through the power of identity services. This is the Next Dimension of Security in the Age of Access.

Founded in 2004, Centrify is enabling over 5,000 customers, including over half the Fortune 100, to defend their organizations. Centrify is a privately held company based in Santa Clara, California. To learn more visit www.centrify.com. The Breach Stops Here.

SANTA CLARA, CALIFORNIA +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
EMAIL sales@centrify.com
WEB www.centrify.com

BRF003739EN-12202017