Centrify
THE BREACH STOPS HERE

SOLUTION BRIEF

# Increase Security in Amazon Web Services (AWS) Environments

amazon web services | Partner Network

**Infrastructure as-a-Service (IaaS) offers tremendous flexibility and elasticity, which results in complexity for enterprises trying to maintain their risk posture and prove compliance while moving to the cloud. It's important to understand that flexibility can slowly become chaos, especially for enterprises that have fought hard to consolidate processes around managing privileged access to 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 and Amazon Web Services have partnered to provide AWS customers with solutions to secure access, privileges and auditing within their AWS environment.**

## Challenges in Adopting Infrastructure-as-a Service

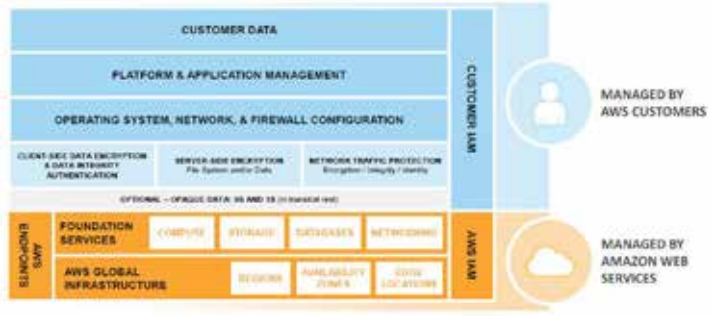
Enterprise IT organizations are increasingly extending their data centers to a hybrid cloud environment. According to a recently commissioned Forrester survey, 93% of decision-makers surveyed said that their organization stores sensitive data in the cloud. This adoption of cloud-based infrastructure 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 take advantage of the benefits of the cloud, while maintaining the same level of privileged access security they currently have on-premises. They need to consider securing both their access to the IaaS management services, servers and hosted applications.

To ensure their customers understand their security responsibility, Amazon Web Services (AWS) has established security best practices outlining the AWS Shared Responsibility Model.

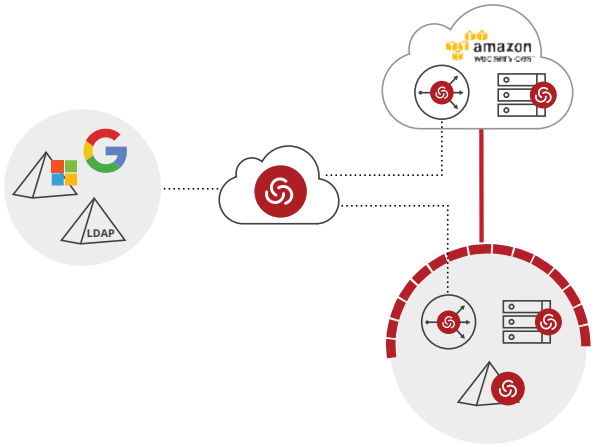



Source: Amazon Web Services Security Best Practices, August 2016

Leveraging built-in IaaS security is a great start, but not a complete solution according to 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 Amazon Web Services

Centrify simplifies and streamlines adoption of IaaS by implementing and extending AWS security best practices for vaulting the root account, controlling access and roles for the AWS console, and securing privileged access to EC2 instances and the applications that run on them.




Centrify's solutions ease the move of an organization's infrastructure and apps to AWS (IaaS) 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:

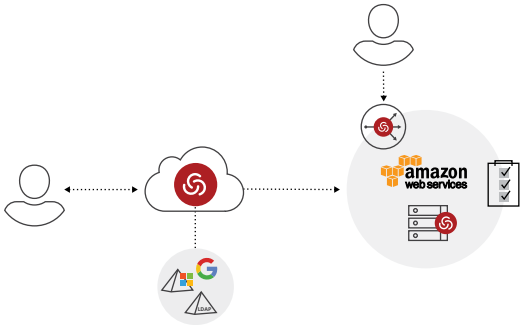
- Federated access to the AWS console and enterprise access to hosted applications
- Secure remote access to EC2 instances and identity brokering for authentication to Linux servers with your choice of identity provider (Active Directory, LDAP, Google G Suite Directory).
- Comprehensive bridging of EC2 instances to Active Directory
- Powerful, role-based granular privilege management and session monitoring

## Secure AWS Service Management

Centrify enables secure access to AWS by vaulting the password for the AWS root account and federating access to the console for service management, precluding the need for long-lived access keys. For break glass access, multi-factor authentication should be enforced for an additional layer of security.

## Secure Privileged Access for EC2 Instances

Securely extend your enterprise authentication services to AWS without replicating identities or identity infrastructure. Broker identities from your choice of directory services — Active Directory, LDAP and cloud directories such as Centrify's and Google's. 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.

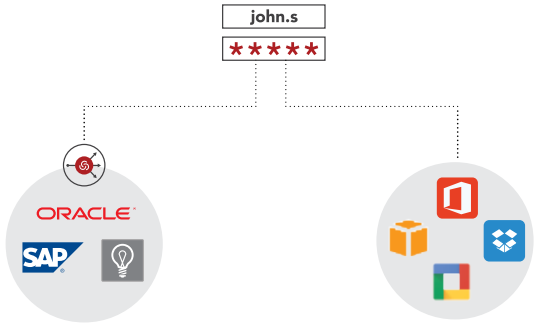



## Enterprise Access for Hosted Apps

Centrify enables federated authentication for employees, business partners and customers who need access to hosted applications on AWS, reducing the attack surface without requiring a VPN.

## 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, per-app policy, 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 EC2 instances to effectively establish accountability and streamline regulatory compliance.

### Centrify and AWS — Better Together

As customers have moved to cloud architectures to complement their existing investments, there has been a big focus at Centrify to enable support for dozens of Amazon Web Services (AWS) use cases to support customers on their journey.

As a result, it was important for Centrify to partner with Amazon Web Services to provide Privileged Identity Management and Active Directory integration for EC2 instances. 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 only 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 50, 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-06152017