Centrify

A CLEAR PATH TO THE CLOUD

Privileged Access Security for the Hybrid Cloud
6 Best Practices

Migrating to the cloud presents challenges. Partnering with a cloud provider like Amazon Web Services (AWS) simplifies some of these, but their "Shared Responsibility Model" requires customers to handle some of the security themselves.

Fortunately, with Centrify, you can implement and extend AWS security **best practices** that make delivering a secure hybrid cloud easier than you think.

93%
of organizations store sensitive data in the cloud.[1]

BEST PRACTICE #1

Establish a common security model

Make sure your apps and infrastructure are protected by applying conventional security and compliance concepts in the cloud.

60%
of enterprises implement appropriate cloud visibility and control tools. These companies will experience **1/3 fewer security failures by 2018 than their counterparts who don't have the correct tools**, according to Gartner.[2]

BEST PRACTICE #2

Consolidate identities

Minimize attack points with a privileged identity management solution that consolidates identity.

95%
of security incidents **involve stolen credentials** according to Verizon's 2015 Data Breach Investigations Report.[3]

BEST PRACTICE #3

Ensure accountability

Have users login as themselves or federate access to services and resources in AWS.

95%
Gartner predicts that through 2020, 95% of **IaaS security failures will be the customer's fault.**[4]

BEST PRACTICE #4

Grant just enough privilege

Granting privileged access increases the risk of a security breach. Grant just the access needed in the AWS console on EC2 instances, and to apps.

50%
More than 50% of IaaS security failures will be attributed to **inadequate management of identities, access and privileges.**[5]

BEST PRACTICE #5

Audit everything

Having a small number of highly privileged AWS admin accounts can limit your risk via EC2 access, but be sure to enable monitoring of these privileged sessions by leveraging enterprise identities for account access. That way, you can capture high-risk activities and proactively identify and mitigate insider threats.

80%
of security breaches **involve** privileged credentials according to Forrester Research's Q3 2016 Wave report on Privileged Identity Management.[6]

BEST PRACTICE #6

MFA everywhere

Passwords just don't cut it anymore, especially with EC2 instance logins. Apply Multi-Factor Authentication (MFA) everywhere to thwart in-progress attacks in AWS.

Gartner advocates, **at minimum,** the use of an MFA tool supported by your cloud provider.[7]

Learn more about securely migrating to a hybrid cloud environment in our new eBook, ***5 Myths about Privileged Access Security for AWS:*** *Separating AWS cloud security fact from fiction*

LEARN MORE ›

1. http://www.csc.com/article/3018156/cloud-computing/cloud-adoption-soars-but-integration-challenges-remain.html
2. http://www.gartner.com/smarterwithgartner/is-the-cloud-secure/
3. http://www.verizonenterprise.com/verizon-insights-lab/dbir/
4. http://www.gartner.com
5. http://www.gartner.com
6. https://www.forrester.com/report/The+Forrester+Wave+Privileged+Identity+Management+Q3+2016/-/E-RES123903
7. http://www.gartner.com/technology/topics/cloud-computing.jsp

Centrify