Architecting 'Security-First' Into Cloud Strategy

CloudAcademy

contents

written by Stuart Scott

Stuart Scott is the AWS Security Lead at Cloud Academy, where he has authored more than 10 courses and learning paths on security-related topics for AWS. He covers the latest AWS security services and updates on the Cloud Academy blog, and he is the author of the ebook, “The Complete Guide to AWS Security for Developers and Sysadmins.” Stuart has more than two decades of IT industry experience in data center and network infrastructure design and cloud architecture and implementation. He is certified as a Data Centre Design Professional (CDCDP) and as an AWS Certified Solutions Architect, and is accredited as an AWS Business and Technology Professional. Stuart was recognized for his contributions to the cloud services community with the Expert of the Year Award from Experts Exchange in 2015.

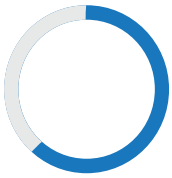
SECURITY MUST REMAIN THE CORNERSTONE OF ANY ORGANIZATION'S CLOUD DEPLOYMENT STRATEGY.

introduction

There are several forces driving organizations toward public clouds as quickly as possible—including reduced costs, faster time to market, and the ability to attract and retain technical staff. But the success or failure of any project is often measured by the level of security that is integrated to safeguard an organization's data and that of its customers.

In the past two years, several high-profile security breaches have resulted in the theft or exposure of millions of personal customer data records. The headlines are a constant reminder of the disruptive (or calamitous) impact on a business in the wake of a breach.

Concern about the security of public cloud technology itself, however, is misplaced. Most vulnerabilities can be traced back to a lack of understanding of cloud security and a shortage of the skills necessary to implement effective security measures. Consider the finding that 60% of engineering firms have slowed their cloud adoption plans due to a lack of security skills.[1] Consider, more worryingly, what happens at firms where similar skill gaps exist, but where adoption plans have not slowed.



60% of engineering firms have slowed their cloud adoption plans due to a lack of security skills.[1]

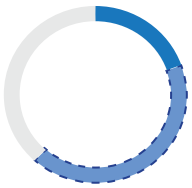
Security must remain the cornerstone of any organization's cloud deployment strategy. Security should need not altogether be viewed as an impediment to migration efforts, but it must not be swept aside due to pressure or demands from business units. While companies cannot prevent every attack, building cloud security awareness at the right levels of the organization from the outset is a first line of defense for blocking the malicious activity that often precedes a breach.

This whitepaper serves as a guide for organization leaders and managers. It begins with an examination of the state of cloud security, lays out the costs of poor security, then addresses common questions about cloud security. Finally, it outlines best practices that de-risk the likelihood of preventable vulnerabilities and enable organizational confidence in cloud initiatives.

IT'S NOT A FAILURE OF TECHNOLOGY, BUT A LACK OF UNDERSTANDING ABOUT THE IMPORTANCE OF SECURITY **AND A LACK OF SKILLS THAT PUT YOUR BUSINESS AT RISK.**

The State of Cloud Security

Companies in every industry are eager to leverage the benefits of the cloud and leave data center management and legacy technologies behind.



57% of enterprises are running hybrid architecture

*In the past year, the shift from on-premises to hybrid cloud in the enterprise has increased from **19% to 57%**.*[1]

Requirements to optimize costs, increase efficiency, and scale to reach new markets are driving cloud adoption from the inside. Competitive changes in markets and the need for innovation are driving adoption efforts externally. Inside the enterprise, migration timelines are often underestimated in the push to deliver cloud solutions quickly. This is especially true for organizations with no prior experience migrating to the cloud.

As a result, business deliverables often take priority over taking the time to establish a comprehensive cloud security strategy. This means that production applications and sensitive data are being deployed to meet key business milestones but without the best practice security principles and methodologies to govern these solutions.

This rush to move to the cloud is one of the factors that make it most vulnerable to security threats.

36% are adopting cloud even without the right security skills

*Despite a lack of cybersecurity skills, **36%** of organizations report that they are continuing to migrate, adopt, and utilize cloud security solutions.*[1]

Some of 2017's largest security breaches were caused by poorly configured security settings or careless human errors. High-profile data breaches at companies like Dow Jones, Verizon, and Scottrade occurred due to improperly configured settings in services like Amazon Simple Storage Service (S3), leaving millions of customer records and other sensitive data exposed. Researchers at RedLock found that 40% of organizations using cloud storage have accidentally exposed one or more of these services to the public.[2]

Hackers are fully aware of human fallibility, and they are perfectly positioned to exploit security vulnerabilities when a business takes shortcuts.

In these instances,

it's not a failure of technology, but a lack of understanding about the importance of security and a lack of skills that put your business at risk.

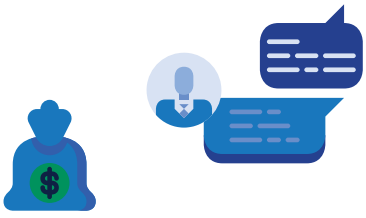
Security must be the top-most priority for any cloud deployment. It is crucial to invest the time and resources required to train your internal cloud teams to correctly and effectively design safe, secure, auditable, and traceable cloud solutions that also meet the demands of your business.

The Cost of Poor Cloud Security

A cloud security breach is more than just the loss of data. When security is treated as an afterthought, or anything less than first-level importance, the result can impact the entire organization.

FINANCIAL IMPACT:
Lost revenue while the business tries to remediate and isolate the attack. You may need to terminate services and systems until the source of the attack has been identified.
Additional internal resources may be required to help resolve and close the point of entry to block the malicious attacker. Employees may need to work additional hours until the issue is resolved.
New software and toolsets may need to be implemented. This includes time to re-architect existing infrastructure to block further attacks and increase your threat detection and prevention measures with additional monitoring.
New security specialists may need to be onboarded to provide expert-level coverage for security and governance.
Once the incident has been resolved, additional training may be required to remediate and strengthen the skills of existing employees.
Procedures and process will need to be evaluated to prevent future attacks or breaches.
Compensation may be required for customers affected by the breach.
Fines may be levied for compliance violations.

REPUTATIONAL IMPACT:
Being publicly *'named and shamed'* in the media.
Loss of customer trust.
Lack of confidence from users, partners, and shareholders.
Potential customers may look upon the broader products and services offered by the business as unsafe, knowing a breach occurred.
The organization may no longer be seen as an industry leader within its field of expertise.
Customers may leave and source their services from a competitor.
Employees may leave, should the incident start to impact company performance.
Re-branding may be required to disassociate the breach from the business.



Data Security in the Cloud

Data security—for any quantity or type of data—is a leading concern when it comes to the cloud. While trust in the public cloud grew from 13% to 18% in 2016, 19% of organizations still distrust the effectiveness of security in the cloud.[1]

These are some of the most common questions that organizations have about storing their data and confidential information in the cloud.

Q. Where does my data physically reside?

As a customer, you can choose where you'd like to store your data. For example, with Amazon Web Services' S3 (Simple Storage Service), you would specify the region where you'd like to store your uploaded data. As a part of the managed S3 service, AWS will automatically replicate your data across several different availability zones within that same region for resilience. The data will then be stored within at least two AWS data centers in undisclosed locations within that region.

Q. Who has physical access to my data?

Physical access to the disks that hold your data are only accessible by the cloud service provider's data center staff. Customers do not have physical access to these data centers. Cloud service providers use external vendors to conduct a rigorous auditing process across a range of controls to ensure compliance for a wide scope of governance categories and standards. Reports and compliance certifications can be obtained directly from the cloud vendor.

Q. Can my data be encrypted in the cloud?

Yes, and encryption should be used where possible for any data at rest and in transit. The leading cloud service providers offer specific services that allow you to manage encryption of your data in the cloud:

CLOUD SERVICE PROVIDER	SERVICE NAME
Amazon Web Services	Key Management Service (KMS)
Microsoft Azure	Key Vault
Google Cloud Platform	Cloud Key Management Service (KMS)

Encryption in transit should be used when transferring data to and from the cloud and when moving data between internal cloud services using protocols such as TLS (Transport Layer Security).

Q. How can I manage access controls for my data?

It is your responsibility to enforce access controls for any data you store in the cloud. The cloud service provider offers security services and features for controlling this access. However, as a customer, it is your responsibility to implement the correct level of security to protect your data at an access level. Identity and access management (IAM) mechanisms allow you to provide granular levels of permissions to any given user, group, and service. Multi-factor authentication should also be used for any user with an elevated set of permissions.

Q. How reliable and resilient is my data?

The cloud generally offers greater resiliency for data compared to storage in most on-premises data centers. Cloud vendors offer a number of managed features to attain this level of availability. Many services automatically duplicate data for resiliency on the customer's behalf, such as Amazon EBS (Elastic Block Store) and Amazon S3, which offers 99.999999999% durability. However, your cloud vendor is not solely responsible for the durability of your data. Customers are also responsible for ensuring that data is protected against potential disasters, including for earthquakes or fire. As the customer, you can choose how much resiliency to build into your solution, and you will be responsible for architecting a failover approach to ensure operation if an entire region fails.

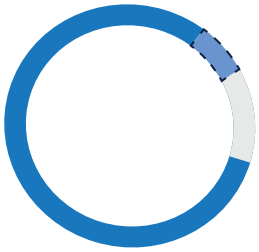
CLOUD ADOPTION IMPACTS YOUR ENTIRE BUSINESS.

Best Practices in Cloud Security

Implement a Security-First Culture.
Security must be part of your business strategy, and it must be reinforced from the very top of your organization.

Cloud adoption impacts your entire business, from technical changes at the infrastructure level, to cultural changes that touch everyone from the board of directors to the teams operating in the cloud.

86% of senior management understand the risks



*The understanding of risk within the public cloud at a senior management level has risen from **80% to 86%** since last year[1].*

Senior management can help drive the cultural change of the cloud by ensuring an understanding of the importance of security at every layer of deployment. This is essential for ensuring that security is at the forefront of all corresponding methodologies, practices, processes, and procedures.

This message must be fed down through the hierarchy of management to all employees. Simultaneously, a clear plan for training and education must run in parallel, allowing employees who need to upskill and learn new technologies, frameworks, and techniques to keep pace with the evolving business demands. If a business moves too fast without an adequate training plan to support its employees, best practices can be overlooked, mistakes can occur, shortcuts may be made, and vulnerabilities will be quietly designed into solutions.

By issuing a 'security-first' directive and backing it up with action across all areas of the business, your organization will more confidently operate in the cloud.

Understand Your Security Responsibility.
Amazon Web Services, Microsoft Azure, and Google Cloud Platform offer a range of services and tools that your teams can use to design, implement, and architect the proper level of security to protect your data and applications in the cloud. The entire security framework operates under a shared responsibility model between the provider and the customer. For this model to be effective, a clear understanding of each side's roles and responsibilities is an essential starting point.

From an infrastructure perspective, the cloud service provider is responsible for ensuring sufficient levels of physical security at their data centers. The service provider manages security throughout their entire global infrastructure, from their physical presence, to the underlying foundational resources that provide compute, storage, database, and network services. Together, these features provide a secure cloud environment.

Customers who import data and utilize the provider's services are responsible for using those services and features provided to design and implement their own security mechanisms. This may include access control, firewalls (both at the instance and network levels), encryption, logging and monitoring, and more.

Train Teams on Governance & Compliance.
Moving services to the cloud impacts how a business maintains compliance with various certifications and governance controls. Traditionally, all resources were maintained within an on-premises data center that an organization could access as needed. This allowed teams to maintain a solid understanding of their infrastructure. When an organization migrates these services to the cloud, this luxury no longer exists. Internal and external auditors are no longer be able to walk around the data center to assess physical controls relating to security and asset management that may be needed for PCI-DSS or ISO 27001.

Similar levels of compliance can be achieved in the cloud. Cloud service providers cover worldwide assurance programs across an extensive list of certifications, attestations, laws, regulations, alignments, and frameworks. The level of certification and compliance attained typically far exceed those held by organizations otherwise running resources on-premises.

Best Practices in Cloud Security

As part of an audit process, an organization can request to see their chosen provider's certifications, and these can be passed to their own auditors to cover any required controls. In addition, there are several cloud services that can be used to help achieve specific compliance. Many of the managed services offered meet the basic controls for programs such as HIPAA or PCI-DSS. Using services that have already been ratified by external auditors can significantly help you achieve the required certification.

Your chosen cloud provider will also have a range of compliance, auditing, monitoring, and recording services in place. Your teams should understand and leverage these where possible in support of your own compliance objectives.

Implement Security at Every Level of Deployment.
Your infrastructure is only as secure as its weakest link. Threats are not limited to external sources. Your teams must be prepared to correctly architect against risks from non-malicious internal breaches or loopholes in user privileges to the most sophisticated attacks, and everything in between.

By implementing security measures across your deployments, you are minimizing the attack surface area of your infrastructure.

Below, we have created a sample multi-level security architecture for a web application deployed on AWS. This example is meant to illustrate the importance of understanding security from a multilayer, cloud-first perspective. In the enterprise, it is unlikely that a single team would implement each of these security services across each layer. Instead, separate teams need to architect the relevant security safeguards within their respective parts of the development and deployment lifecycle.

The services listed below are just some of the AWS security services that you can deploy to protect your environment. Where possible, your teams should use the managed security services offered by your cloud service provider.

It's important to have a full understanding of the services available to protect your infrastructure, applications, and data. And it's critical for teams to show that they know how to can use them for each deployment across the infrastructure stack.

A sample multi-level security architecture for a web application deployed on AWS.

LAYER	AWS SERVICE/FEATURE
Network Edge	Amazon CloudFront (Content Delivery Network) AWS WAF (Web Application Firewall) and Route53 (DNS)
Internal Network	Virtual Private Clouds (VPCs) VPC Flow Logs, Network Access Control Lists (NACLs), network gateways, public/private subnet architecture and route tables
Instance	O/S hardening best practices and Security Groups
Database	Encryption mechanisms and Amazon RDS security groups
Storage	Amazon S3 - Encryption mechanisms, lifecycle rules, MFA delete and bucket policies
Application	Amazon API Gateway, automation, encryption and best practices
Access Control	Identity & Access Management (IAM), users, groups, roles, policies ad MFA (Multi-Factor Authentication)
Monitoring, Auditing & Governance	AWS CloudTrail, AWS Config, Amazon CloudWatch, Amazon SNS, AWS Lambda, Amazon GuardDuty, Amazon Inspector, AWS Trusted Advisor

KEY TAKEAWAYS

- **Concern about the security of public clouds in and of themselves is misplaced;** the real concern lies with organizational, team, and individual security awareness, processes, and practices.

- **Enterprises tend to fall into two cloud security traps:** (1) those that delay migration projects due to lack of cloud skills, or (2) more threateningly, those that rush to deploy workloads due to business pressure, despite an identified cybersecurity skill gap.

- **The risks of an ill-defined security strategy remain very serious** and real to the financial and reputational success of your business.

- **Security must be a core part of your business strategy;** a 'security-first' culture must be reinforced from the very top of your organization.

- **Your organization must clearly understand the shared responsibility model.** This dictates which security responsibilities sit with the provider and which sit with you, the customer.

- **Make teams responsible for architecting the relevant security safeguards** within their respective parts of the development and deployment lifecycle.

- **At minimum, support any 'security-first' strategy by investing time and resources into ongoing training.** Ideally, build your own internal certification that ensures teams understand how to effectively design and deploy solutions that are safe, secure, auditable, and traceable.

conclusion

Although cloud security as a topic is still the biggest concern for enterprises migrating services to the cloud, public clouds are considered far more secure than traditional on-premises data centers.

With a range of tools, services, features, and enhancements it's possible to secure your environment at every layer while at the same time providing the ability to generate extensive logging capabilities that could be used to automatically trigger self-protecting measures should a breach be detected.

Cloud security should not be reason to shy away from running services on the cloud. Start by instilling a culture of transparency around adherence to security best practices in each organizational unit that touches any cloud initiative.

Through a continuous training strategy, ensure that teams stay current on vendor updates, security vulnerabilities, and evolving best practices. When teams are enabled to move confidently in the context of a 'security-first' implementation strategy, the more commonly referenced reasons in favor of managing infrastructure on public clouds–cost optimization, flexibility, scalability, elasticity–become a reality.

Source: [1]McAfee 2017 Report: Building Trust in a Cloudy Sky
[2]RedLock Cloud Infrastructure Security Trends, May 2017 Edition

Cloud Academy is the leading enterprise training platform that accelerates teams and digital transformation.

Companies trust Cloud Academy to deliver multimodal training on the leading clouds (AWS, Azure, Google Cloud Platform), on the essential methodologies needed to operate on and between clouds (DevOps, Security), and on the capabilities that are unlocked by the cloud (machine learning, IoT).

From the fundamentals to advanced scenario training, Cloud Academy empowers organizations with the knowledge, critical thinking, and hands-on experience needed to adopt, operate, and optimize the multi-cloud.

cloudacademy.com

UPDATED: 1/10/2018