

Velocity with Security

A Guide to Amazon Web Services (AWS)

Cloud Security Best Practices

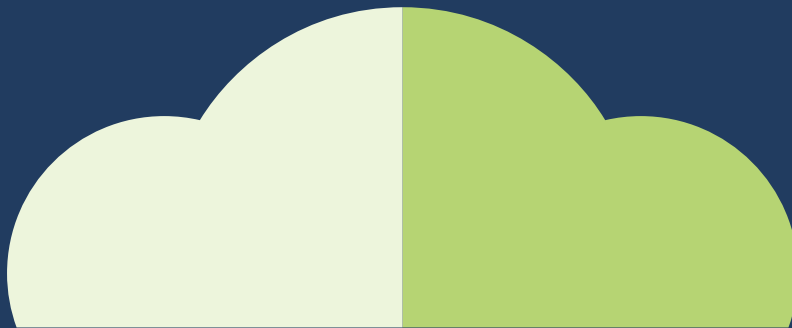
From the experts at Symantec and Amazon Web Services

Over the last decade, we've seen growing adoption of cloud computing running on Amazon Web Services (AWS).

Businesses and organizations are increasingly using AWS to launch new products and services, enter new markets, disrupt competitors and provide always-on customer service. Today, there are millions of active customers using AWS to provide better business agility and greater flexibility to build their own applications.

The wide adoption of AWS signals that we've entered the Cloud Generation era where computing has broken the boundaries of desktops and data centers to embrace the mobile, social, global, crowd-sourced, always-on realities of modern life. Not only has cloud computing altered the way people work, it has dramatically expanded the computing environment, upending traditional business and IT operations right along with their corresponding security requirements. Organizations are no longer just using AWS for their test and development environments. Increasingly, they are using AWS to migrate critical applications running on unsupported on-premises legacy platforms, as well as to deploy new cloud-native applications.

As cloud adoption increases within organizations and new agile development processes become widespread, new threats and vulnerabilities have emerged. It's important to create a culture of security across your organization and implement new approaches like the DevSecOps framework. The following guide from Symantec and Amazon Web Services provides best practices for helping secure your cloud environment and software development lifecycle, so your organization can experience all the advantages of AWS while mitigating security risks.





Securing the Cloud

While the cloud enables new levels of business productivity and agility, maintaining security and compliance remains paramount.

These are two primary considerations for customers adopting the cloud with an ever-evolving threat landscape and an expanding attack surface due to enterprises now needing security within their datacenters and for workloads in the cloud. Organizations should leverage a highly-secure cloud provider, like AWS, and then take the appropriate steps to help secure the data and workloads running in their environment.

Security and compliance in the cloud present new challenges for security, IT and DevOps teams. Applications in these environments are componentized, preconfigured and based on a library of templates. These applications are dynamic, mobile, orchestrated and automated. Architectural differences between workloads in the cloud and on-premises infrastructures make it difficult to retrofit on-premises security solutions for public cloud environments. Traditional security solutions may not work well in the cloud, where infrastructure configuration and security policies need to be applied and enforced dynamically and may be based on aggregating traffic at the perimeter for threat detection, rather than building security into a distributed cloud architecture. Understanding these differences and implementing security best practices that are optimized for AWS cloud architectures are critical to providing the agility the business needs, while maintaining security.

Security needs to change for the cloud. When you change parts of the architecture, you change the requirements. Organizations still want to use the same type of products that they use for perimeter security in the cloud, which may not have the same value. The key is to adopt a new security approach from the beginning of your move to the cloud rather than bolting it on at the end.

Shared Responsibility of Cloud Security

The concept of shared responsibility is a critical success factor for effective cloud security. Cloud security can't be "outsourced" – it requires collaboration across vendors and customers and collaboration across security, IT and DevOps teams. There are four foundational principles when rethinking the security of the AWS public cloud:



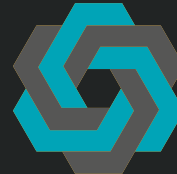
Democratize cloud infrastructure

The AWS shared responsibility model defines the role of the cloud provider and the customer in providing security in the cloud. When you move to the cloud, infrastructure responsibility essentially gets distributed to many different application teams that are consuming infrastructure directly from AWS. Security practices need to morph to incorporate this shared responsibility model, where AWS is responsible for securing the underlying infrastructure, and your teams are responsible for how you configure and use your AWS environment, including access controls, workload and storage configuration, user activity monitoring, threat protection, application security and data security.



Decentralize security responsibility

If you are moving to AWS, more than ever before you need to educate your application owners on how to secure their services – alongside the safety net that a centralized security function provides. It is wise to educate, instrument and engage different application owners that are going to be consuming AWS services, and provide them support from a centralized security model. You should engage your risk and compliance team to establish requirements for meeting regulatory compliance requirements. Involve your InfoSec team on how to include AWS into your cloud app security and data loss protection strategy.



Deploy DevSecOps

DevSecOps is all about how to reengineer your software development lifecycle (SDLC) and how to morph that into a security practice. Security needs to be embedded within whatever software development lifecycle process that you are going to use when migrating to AWS. Often, this cycle is referred to as continuous integration (CI) and continuous deployment (CD).



Address attack vectors

Cloud security isn't just about securing a specific machine or compute engine. It's about securing applications that run in your cloud environment. The entire fabric, ranging from where your information is stored, to compute, to different service components that you may consume from AWS – needs to be addressed in the context of a holistic cloud security approach. Also consider how AWS fits into your overall organizational security strategy and use of cloud services.

According to Hardeep Singh, Symantec's cloud security architect, "When moving to the cloud, the goal is to decentralize and democratize the security process. The more you bring developers into the operations model, the more you need to have a decentralized security model. Organizations can't have centralized security and decentralized operations."

The Rise of DevSecOps

DevOps is a culture not a function. It's a cultural framework where developers and production engineers are working closely together to deliver applications in a services environment.

"Organizations can't have centralized security and decentralized operations."

Hardeep Singh
Symantec Cloud Security Architect

Ops is an engineering discipline. Within that engineering discipline, there are three key modalities, including reliability, security and velocity. In the DevOps culture, the reliability cycle gets faster since these teams are working hand-in-hand. That same notion can be extended to security. Ultimately, it's about acceleration of remedial faults. If you make your DevOps team accountable, everything gets addressed faster in that framework – whether it be reliability, security or velocity. However, if security becomes a second-class citizen in the DevOps framework, it can weaken an organization's security posture.

DevSecOps is an emerging approach to close the gap between security and DevOps, especially when moving to the cloud. The DevSecOps framework brings these traditionally disparate constituencies a lot closer together in a more modular way. To ensure success, companies should reorganize and retrain around a DevSecOps framework, led strongly by a partnership between the CIO and CISO.

Today's organizations want the benefit of the velocity gain enabled by AWS but also want to improve their security posture as they move to the cloud. "Security is not absolute, but a gradient against the lever of velocity," says Raj Patel, vice president of Cloud Platform Engineering for Symantec. "The level of DevSecOps integration depends on an organization's appetite for risk and security posture in general. For Symantec as a cyber security leader, our applications teams are very security-aware by design. We found it more appropriate for them to be more educated and accountable for security in their own regard. Our Central security team provides strong guardrails and a safety net for our services. In cloud-native organizations, it's often more successful to embed security a lot closer to those applications."



DevSecOps

Either way, the DevSecOps framework relies on deep security experts to define security practices, policies and how to implement. It brings these practitioners who are implementing security capabilities much closer to the application teams. In some cases, these practitioners could be the application developers themselves or they could be embedded security engineers in the same scrum team as the developers.

DevSecOps requires companies to think about changes to their software development lifecycle (SDLC) to address their migration to the AWS. If you have an existing software development lifecycle methodology, you typically have a development pipeline, a QA cycle, a testing cycle and a deployment cycle – as well as some form of security testing within that lifecycle. As you move to the AWS public cloud, that SDLC typically tends to change to more of a continuous integration and continuous deployment type of approach.

If you make this change, you must integrate your suite of security services into that CI/CD pipeline. The cloud gives you the ability to rapidly iterate. To take advantage of this, you must integrate your security practices alongside that same pipeline. For example, if you are deploying to production multiple times a day, your security verification and testing needs to get built into that CI/CD pipeline versus engaging with a centralized security function as an adjunct. And security experts need to be embedded with the application teams to approach and achieve those tasks as one cohesive unit.

In DevSecOps, an important cultural change is making sure application owners know that they are responsible for the security posture of their applications. The centralized security function is there to enable them, and to provide them with security guidelines, tools and capabilities to secure their applications. But ultimately, they are accountable. It's particularly important to make that shift in application owner mindset in an organization that has not been providing a SaaS or cloud service where they may have relied on a different organization to secure their application after it's been developed.

It's critical to focus on culture and tools to drive change management to DevSecOps. "Symantec was in a position of strength when shifting our mindset to DevSecOps," said Patel. "We found it effective to create an internal cloud security forum made up of practitioners who are passionate about security to create best practices and approaches that we should implement as we moved to AWS. This was a grassroots way for us to implement some of the leading thoughts on security, while at the same time having application teams owning security."

Following these best practices enables cross-functional teams to integrate security with DevOps processes. In this framework, DevSecOps works together with the InfoSec and Risk & Compliance teams to deliver a balanced approach to security, with some security functions owned by DevSecOps and some security functions owned by these other teams. Organizations can then leverage automation to assure the right security measures are implemented at every step in the process and address a number of security challenges they are facing today.

“Security is not absolute, but a gradient against the lever of velocity.”

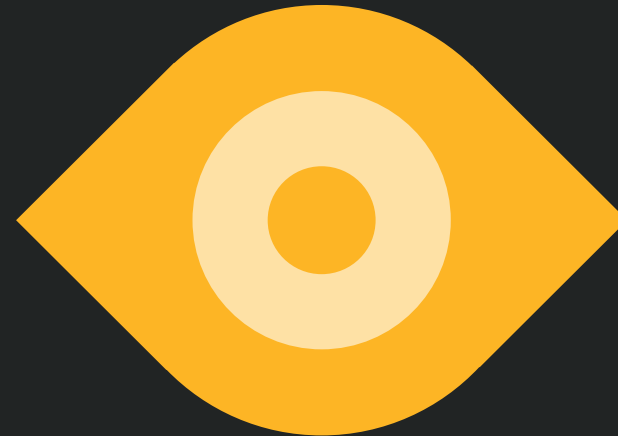
Raj Patel
Vice President of Cloud Platform Engineering, Symantec



Visibility

In many organizations, “shadow IT” runs rampant as users and departments embrace agility, often without consideration for data and access security. Where data once traveled along linear and predictable paths, today the flow of information is fluid, chaotic and complex. This puts security leaders and IT staff in a painful bind. Traditional security infrastructure, already hampered by blind spots and a lack of integration, can’t cope with this brave new world – where applications and data proliferate while people and information interact in ways that defy prediction and resist control.

As companies move data and applications to the cloud, it becomes even more difficult for security and DevOps teams to secure potentially thousands of cloud resources that are being spun up and torn down daily across their cloud environment by anyone with a credit card. And misconfigured cloud services can lead to data breaches and targeted attacks. Organizations must monitor and audit the configuration of their cloud services and security-related actions of their admins and users. This requires visibility and control of the cloud management plane, which is used to manage and configure cloud resources such as launching virtual instances or configuring virtual networks.



Compliance

While there have been some lingering concerns about the security of the cloud, the reality is that many cloud security failures are a result of misconfiguration. According to Gartner, “Through 2022, at least 95 percent of cloud security failures will be the customer’s fault.”*

Ensuring enforcement of critical policies and regulations on AWS requires governance, risk and compliance tools that can help customers inventory their IT assets, evaluate vulnerabilities, govern information access, and automate compliance reporting for more than 100 regulatory and best practice frameworks including GDPR, HIPAA, NIST, PCI DSS and SWIFT.

Configuration

While there have been some lingering concerns about the security of the cloud, the reality is that many cloud security failures are a result of misconfiguration. According to Gartner, “Through 2022, at least 95 percent of cloud security failures will be the customer’s fault.”*

“Companies with limited resources and budget should actually consider moving to the cloud in order to benefit from stronger security and compliance,” says Curt Dukes, executive vice president for Security Best Practices, CIS (Center for Internet Security, Inc). “Equipment is monitored, and access to the premises of data centers is heavily secured. The cloud is no less secure than servers managed internally by your company.” The non-profit organization CIS (Center for Internet Security, Inc.) recently worked with security experts like Symantec and others around the globe to publish the Amazon Web Services Foundations Benchmark that has become the industry benchmark for securing AWS environments.

To secure your AWS environment, you must correctly configure your cloud in key areas including identity and access management, logging, monitoring and networking. Based on our work with organizations worldwide, Symantec and Amazon Web Services have published a configuration checklist of the Top 10 most important and easiest steps for customers to take when moving their infrastructure to AWS.

“Companies with limited resources and budget should actually consider moving to the cloud in order to benefit from stronger security and compliance,”

Curt Dukes
Executive Vice President for
Security Best Practices, CIS
(Center for Internet Security, Inc).



Symantec and AWS Cloud Security Solutions

For organizations to succeed in their move to the cloud, it's critical to leverage advanced cloud security solutions like those from Symantec and AWS that help secure cloud access, cloud infrastructure and cloud applications, providing in-depth visibility and controls to safeguard users, information and workloads across public and private clouds.



Securing Cloud Access

Symantec VIP Access Manager is a next generation access control platform, the foundation for an information protection solution for the cloud, that integrates Single Sign-On (SSO) with strong authentication, access control, and user management. In AWS, where a traditional perimeter does not exist, VIP Access Manager fills the gap by helping organizations adopt cloud-based applications while maintaining proper risk management and compliance measures to help protect data and follow regulations. Virtually any cloud-based application is supported with easy-to-create connectors. Also included is a built-in user directory for self service provisioning and integration with common identity providers to enforce security and compliance for applications without getting in the way of productivity. AWS offers secure, scalable infrastructure to support VIP Access Manager as it scales with an organization's need to manage additional apps, devices and users.

While VIP Access Manager guards the login, Symantec CloudSOC CASB enables you to enforce granular access controls for both users and admins within an authenticated session. The solution provides continuous visibility and control over access to systems, settings and content based on granular contextual event attributes using multi-channel CASB functions leveraging both API integration and inline traffic inspection.



Securing Cloud Infrastructure

The AWS cloud infrastructure puts strong safeguards in place to help protect customer privacy. All data is stored in highly secure AWS data centers. Security scales with your AWS cloud usage. No matter the size of your business, the AWS infrastructure is designed to help keep data safe. AWS provides several security capabilities and services to increase privacy and control network access. These include:

- ◆ Network firewalls built into Amazon VPC, and web application firewall capabilities in AWS WAF let you create private networks, and control access to your instances and applications
- ◆ Encryption in transit with TLS across all services and encryption at rest with services like KMS and HSM
- ◆ Connectivity options that enable private, or dedicated, connections from your office or on-premises environment

In addition, Amazon S3 provides a highly durable storage infrastructure designed for mission-critical and primary data storage. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 region. Once the objects are stored, Amazon S3 maintains their durability by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums.

Symantec's solutions for securing the cloud infrastructure provide organizations with a comprehensive view into who is using the cloud and how they are using it. By utilizing Symantec CloudSOC CASB, Symantec Cloud Workload Protection and Symantec Cloud Workload Assurance, organizations can help protect their AWS environments from misconfigurations, misuse, attacks, threats and data loss. And together, these solutions automate security for DevOps teams by embedding it into the front-end of the development process.



Securing Cloud Applications

Symantec CloudSOC CASB empowers organizations to confidently leverage cloud applications and services while helping them stay safe, secure and compliant. CloudSOC enables you to detect and respond to security issues for your cloud apps and infrastructure all in one platform. With CloudSOC, you can protect sanctioned and unsanctioned use of AWS within your organization by:

- ◆ Monitoring, logging and analyzing user and admin activity
- ◆ Enforcing access controls to prevent misconfigurations
- ◆ Detecting and remediating risky exposures in S3 buckets
- ◆ Defending S3 storage from advanced malware and APTs
- ◆ Detecting compromised accounts with user behavior analytics
- ◆ Detecting and restricting misuse and "shadow" AWS instances



Securing Cloud Workloads

Symantec Cloud Workload Protection automates security for cloud workloads, enabling business agility, risk reduction, and cost savings for organizations, while easing DevOps and administrative burdens. Rapid discovery, visibility, and elastic protection of AWS workloads enable automated security policy enforcement to help protect applications from unknown exploits.

Cloud-native integration allows DevOps to build security directly into application deployment workflows, while support for Chef and Puppet automates configuration, provisioning, and patching. Access to the Symantec Global Intelligence Network helps protect workloads against the latest global attacks and vulnerabilities, providing peace of mind for large enterprises, mid-market companies and born-in-the-cloud businesses.

Organizations migrating workloads to AWS benefit from:

- ◆ Visibility and control of cloud workloads
- ◆ Elastic security for their dynamic cloud infrastructure
- ◆ Mitigation of risk associated with public cloud adoption

In addition, with potentially thousands of cloud resources deployed across multiple regions and multiple clouds, Symantec Cloud Workload Assurance provides organizations with visibility into their cloud environments, assesses your cloud security posture and helps enforce security and compliance policies. Organizations can have visibility and control of the AWS management plane, which is used to manage and configure cloud resources such as launching virtual instances or configuring virtual networks. The solution continuously monitors your cloud environment for resource misconfigurations that can expose your data to the public internet. It gives you the ability to resolve issues quickly with easy-to-follow, guided remediation steps developed by security analysts and compliance experts. And it generates compliance reports with a single click, while eliminating the taxing process of collecting evidence in spreadsheets.



Conclusion

Moving to the cloud is liberating. But security in public clouds is different. And the pitfalls of making a hasty move to the cloud are many.

Are you prepared? Symantec and Amazon Web Services have teamed up to offer these cloud security best practices and deliver cloud security solutions that are optimized for your AWS applications and instances.

For access to a Free Trial** of Symantec's cloud security solutions, please visit:

- ◆ [Cloud Workload Protection](#): Automatic discovery and visibility of cloud workloads
- ◆ [Cloud Workload Protection for Storage](#): Anti-malware scanning for S3 buckets
- ◆ [Cloud Workload Assurance](#): Cloud Security Posture Management (CSPM)

* Gartner, "Clouds Are Secure: Are You Using Them Securely?," Jay Heiser, January 31, 2018. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

** Free trial subject to applicable terms and conditions.

Amazon Web Services (AWS) Cloud Security A Configuration Checklist

From the experts at Symantec + Amazon Web Services



Many organizations believe that the security responsibility of their workloads lies entirely with the cloud service provider, when in reality it is a shared responsibility between the customer and provider. According to Gartner, “Through 2022, at least 95 percent of cloud security failures will be the customer’s fault.”*

The non-profit organization CIS (Center for Internet Security, Inc.) recently worked with security experts like Symantec and others around the globe to publish the CIS Amazon Web Services Foundations Benchmark that has become the industry benchmark for securing AWS public cloud environments. CIS Hardened Images™ are Amazon Machine Images of today’s most popular operating systems – pre-configured to meet the globally-accepted cybersecurity best practice guidelines of the CIS Benchmarks™ – to help you start secure and stay secure while working in the cloud. For more information, please visit www.cisecurity.org/cis-benchmarks/

Symantec’s new Cloud Workload Assurance solution enables customers to score the security posture of their AWS instances to ensure compliance against these benchmarks. In addition, based on our work with organizations worldwide, Symantec and Amazon Web Services have highlighted what we believe are the Top 10 most important and easiest steps for customers to take when moving their infrastructure to AWS. Use this hands-on, actionable checklist to ensure your cloud environments are secure and configured correctly – and avoid becoming part of the 95 percent.

* Gartner, “Clouds Are Secure: Are You Using Them Securely?,” Jay Heiser, January 31, 2018. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Identity and Access Management

- ❑ Avoid the use of the “root” account
- ❑ Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password
- ❑ Implement strong IAM password policies across accounts

Logging

- ❑ Ensure that CloudTrail is enabled all regions
- ❑ Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible

Monitoring

- ❑ Ensure a log metric filter and alarm exist for usage of the “root” account
- ❑ Ensure a log metric filter and alarm exist for IAM policy changes

Networking

- ❑ Ensure no security groups allow ingress from 0.0.0.0/0 to port 22
- ❑ Ensure the default security group of every VPC restricts all traffic
- ❑ Ensure routing tables for VPC peering are “least access”

