CHEAT SHEET

McAfee
Together is power.

51-Point AWS Security Configuration Checklist

Amazon Web Services (AWS), the leader in the public cloud infrastructure-as-a-service (IaaS) market, offers a broad set of global compute, storage, database, analytics, application, and deployment services that help organizations move faster, lower IT costs, and scale applications. According to Amazon, over one million active AWS customers are reaping the cost and productivity advantages they have to offer. Like most cloud providers, AWS operates under a shared responsibility model. AWS takes care of security 'of' the cloud while AWS customers are responsible for security 'in' the cloud. This document guides customers on how to ensure the highest level of protection for their AWS infrastructure and the sensitive data stored in AWS with a 51-point security configuration checklist to ensure that AWS services are configured with the highest level of security while still allowing employees to fulfill their job responsibilities.

AWS Security Challenges

Threats to applications running on AWS and the data stored within them can take many forms:

- **Compromise of AWS.** Amazon has made significant investments in security to protect its platform from intrusion. However, the small possibility remains that an attacker could compromise an element in the AWS platform and either gain access to data, take an application running on the platform offline, or permanently destroy data.
- **Denial of Service (DoS) attack on an application.** Amazon has developed sophisticated DoS prevention capabilities delivered in AWS Shield for all customers. However, it's possible a large attack could overwhelm Amazon's defenses and take an application running on the platform offline for a period of time until the attack is remediated.

Connect With Us

- **Insider threats and privileged user threats.** The average enterprise experiences 10.9 insider threats each month and 3.3 privileged user threats each month. These incidents can include both malicious and negligent behavior— ranging from taking actions that unintentionally expose data to risk, to employees stealing data before quitting to join a competitor.
- **Third-party account compromise.** According to the Verizon Data Breach Investigations 2016 Report, 63% of data breaches, including the breach that sunk Code Spaces, were due to a compromised account where the hacker exploited a weak, default, or stolen password. Misconfigured security settings or accounts that have excessive identity and access management (IAM) permissions can increase the potential damage.
- **Sensitive data uploaded against policy/regulation.** Many organizations have industry-specific or regional regulations, or internal policies, that prohibit certain types of data from being uploaded to the cloud. In some cases, data can be safely stored in the cloud, but only in certain geographic locations (for example, a data center in Ireland but not in the United States).
- **Software development lacks security input.** Unfortunately, IT security isn't always involved in the development or security of custom applications. IT security professionals are only aware of 38.6% of the custom applications in use in their organizations. This means when it comes to their development, IT security is often circumvented, making the task of securing these applications more difficult.

As enterprises continue to migrate to or build their custom applications in AWS, the threats they face will no longer be isolated to on-premises applications and endpoint devices. While the move to the cloud transfers some responsibility for security from the enterprise to the cloud provider, as we will see in the next section, preventing many of these threats falls on the shoulders of the AWS customer.

Shared Responsibility Model

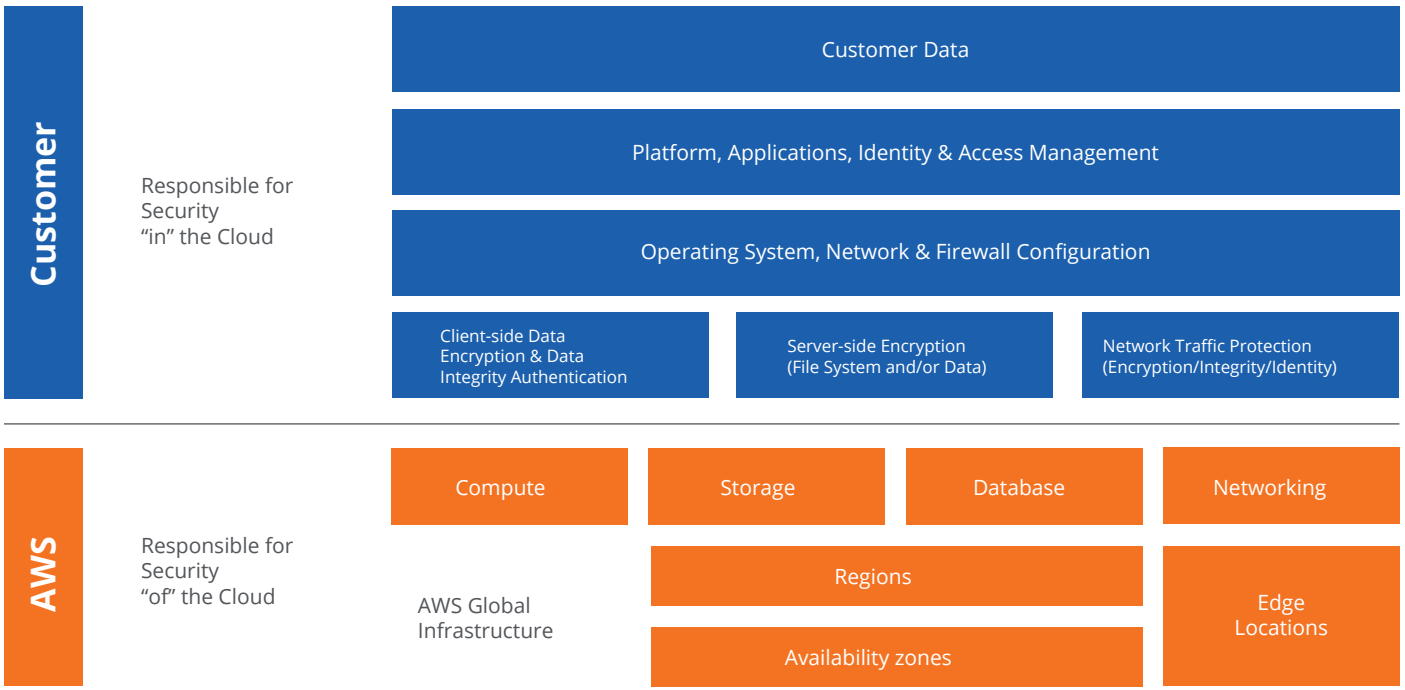
Amazon takes responsibility for the security of its infrastructure and has made platform security a priority in order to protect customers' critical information and applications. Amazon detects fraud and abuse and responds to incidents by notifying customers. However, the customer is responsible for ensuring their AWS environment is configured securely, data is not shared with someone it shouldn't be shared with inside or outside the company, identifying when a user misuses AWS, and enforcing compliance and governance policies.

Amazon's responsibility

Since it has little control over how AWS is used by its customers, Amazon has focused on the security of AWS infrastructure, including protecting its computing, storage, networking, and database services against intrusions. Amazon is responsible for the security of the software, hardware, and the physical facilities that host AWS services. Amazon also takes responsibility for the security configuration of its managed services such as Amazon DynamoDB, RDS, Redshift, Elastic MapReduce, WorkSpaces, and others.

Customer's responsibility

AWS customers are responsible for secure usage of AWS services that are considered unmanaged. For example, while Amazon has built several layers of security features to prevent unauthorized access to AWS, including multifactor authentication, it is the responsibility of the customer to make sure multifactor authentication is turned on for users, particularly for those with the most extensive IAM permissions in AWS.



CHEAT SHEET

	Customer	AWS
Preventing or detecting when an AWS account has been compromised	•	
Preventing or detecting a privileged or regular AWS user behaving in an insecure manner	•	
Preventing sensitive data from being uploaded to or shared from applications in an inappropriate manner	•	
Configuring AWS services (except AWS Managed Services) in a secure manner	•	
Restricting access to AWS services or custom applications to only those users who require it	•	
Updating guest operating systems and applying security patches	•	
Ensuring AWS and custom applications are being used in a manner compliant with internal and external policies	•	•
Ensuring network security (DoS, man-in-the-middle (MITM), port scanning)	•	•
Configuring AWS Managed Services in a secure manner		•
Providing physical access control to hardware/software		•
Providing environmental security assurance against things like mass power outages, earthquakes, floods, and other natural disasters		•
Database patching		•
Protecting against AWS zero-day exploits and other vulnerabilities		•
Business continuity management (availability, incident response)		•

Table 1. Shared responsibility model at a glance

AWS Security Checklist

Amazon has invested heavily in building a powerful set of security controls for its customers to use across AWS services and it is up to the customer to make the most of these built-in capabilities. Here are the top 51 best practices security experts recommend you follow:

- [ ] Enable CloudTrail logging across all AWS.
- [ ] Turn on CloudTrail log file validation.
- [ ] Enable CloudTrail multi-region logging.
- [ ] Integrate CloudTrail with CloudWatch.
- [ ] Enable access logging for CloudTrail S3 buckets.
- [ ] Enable access logging for Elastic Load Balancer (ELB).
- [ ] Enable Redshift audit logging.
- [ ] Enable Virtual Private Cloud (VPC) flow logging.
- [ ] Require multifactor authentication (MFA) to delete CloudTrail buckets.
- [ ] Turn on multifactor authentication for the “root” account.
- [ ] Turn on multi-factor authentication for IAM users.
- [ ] Enable IAM users for multi-mode access.
- [ ] Attach IAM policies to groups or roles.
- [ ] Rotate IAM access keys regularly, and standardize on the selected number of days.
- [ ] Set up a strict password policy.
- [ ] Set the password expiration period to 90 days and prevent reuseCustomer Visualforce pages with standard headers.
- [ ] Don’t use expired SSL/TLS certificates.
- [ ] User HTTPS for CloudFront distributions.
- [ ] Restrict access to CloudTrail bucket.
- [ ] Encrypt CloudTrail log files at rest.
- [ ] Encrypt Elastic Block Store (EBS) database.

CHEAT SHEET

- [ ] Provision access to resources using IAM roles.
- [ ] Ensure EC2 security groups don't have large ranges of ports open.
- [ ] Configure EC2 security groups to restrict inbound access to EC2.
- [ ] Avoid using root user accounts.
- [ ] Use secure SSL ciphers when connecting between the client and ELB.
- [ ] Use secure SSL versions when connecting between client and ELB.
- [ ] Use a standard naming (tagging) convention for EC2.
- [ ] Encrypt Amazon's Relational Database Service (RDS).
- [ ] Ensure access keys are not being used with root accounts.
- [ ] Use secure CloudFront SSL versions.
- [ ] Enable the require_ssl parameter in all Redshift clusters.
- [ ] Rotate SSH keys periodically.
- [ ] Minimize the number of discrete security groups.
- [ ] Reduce number of IAM groups.
- [ ] Terminate unused access keys.
- [ ] Disable access for inactive or unused IAM users.
- [ ] Remove unused IAM access keys.
- [ ] Delete unused SSH Public Keys.
- [ ] Restrict access to Amazon Machine Images (AMIs).
- [ ] Restrict access to EC2 security groups.
- [ ] Restrict access to RDS instances.
- [ ] Restrict access to Redshift clusters.
- [ ] Restrict access to outbound access.
- [ ] Disallow unrestricted ingress access on uncommon ports.
- [ ] Restrict access to well-known ports such as CIFS, FTP, ICMP, SMTP, SSH, Remote desktop.
- [ ] Inventory and categorize all existing custom applications by the types of data stored, compliance requirements and possible threats they face.

- [ ] Involve IT security throughout the development process.
- [ ] Grant the fewest privileges as possible for application users.
- [ ] Enforce a single set of data loss prevention policies across custom applications and all other cloud services.
- [ ] Encrypt highly sensitive data such as protected health information (PHI) or personally identifiable information (PII).

Are You Ready to Secure Your AWS Environment?

McAfee Skyhigh Security Cloud for Amazon Web Services offers a comprehensive monitoring, auditing and remediation solution for your AWS environment and custom applications.

www.skyhighnetworks.com

Download a data sheet to learn more about our product capabilities.

- **McAfee Skyhigh Security Cloud for AWS**

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com