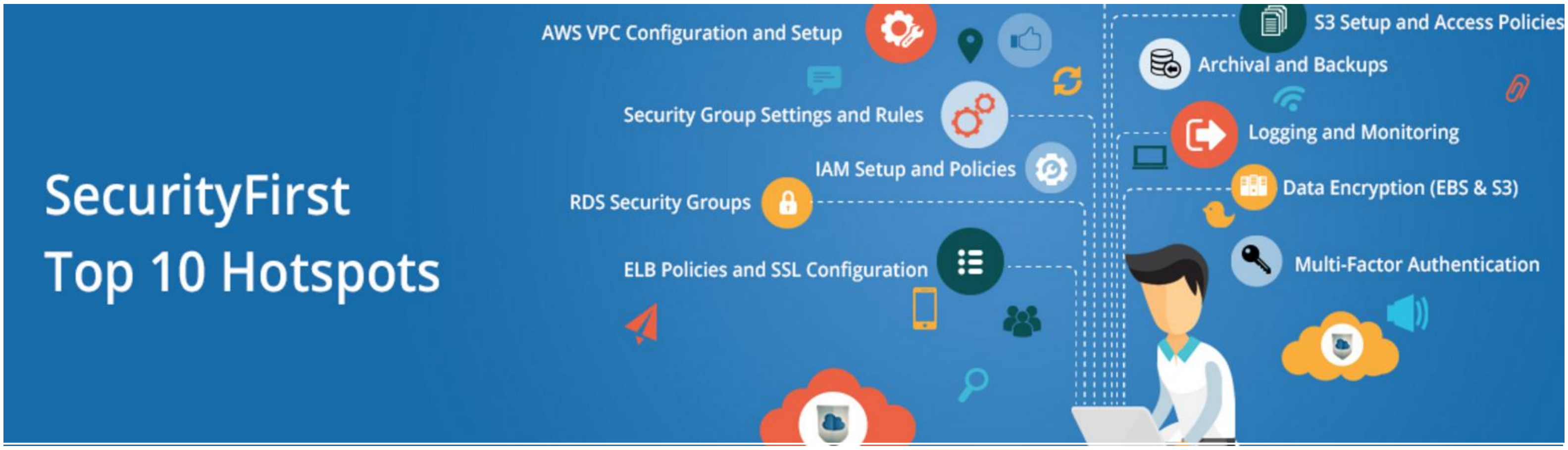
stackArmor


SecurityFirst
Top 10 Hotspots
AWS VPC Configuration and Setup
Security Group Settings and Rules
IAM Setup and Policies
RDS Security Groups
ELB Policies and SSL Configuration
S3 Setup and Access Policies
Archival and Backups
Logging and Monitoring
Data Encryption (EBS & S3)
Multi-Factor Authentication

Cloud Security Best Practices
White Paper
February 2016

Prepared by:
stackArmor
10411 Motor City Drive, Suite 410A
Bethesda MD 20817
Phone: 571-271-4396
www.stackArmor.com

The information in this document is the property of FedCEO LLC (DBA stackArmor) and may not be copied or redistributed without written permission. The contents of this document are for informational purposes only. No liability or warranty is expressed or implied.

Contents

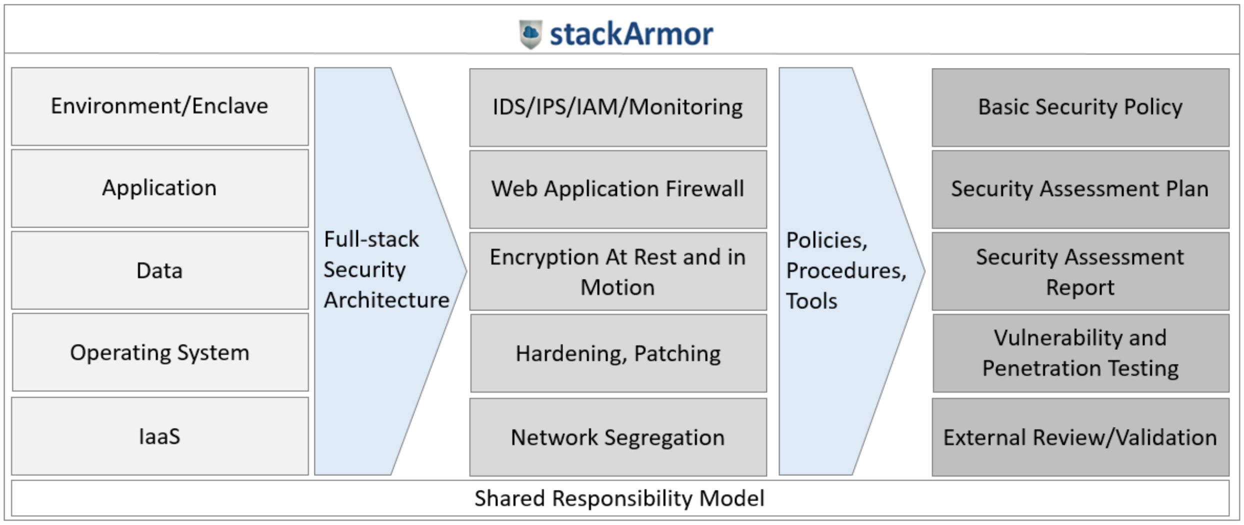
1 Introduction

stackArmor specializes in full-stack cloud solutions for security focused customers. stackArmor engineers are experts in designing, building and operating highly automated cloud platforms for enterprise workloads with stringent performance and security requirements. The company's principals have supported large cloud-based modernization programs at organizations such as Department of Defense, US Treasury, Coca-Cola, and SAP as well as fast-paced start-ups and SaaS providers. Our security practices have been developed based on real-world implementation experience of large cloud environments based on FISMA, FedRAMP, NIST, HIPAA and ISO 27001 requirements.

1.1 Full-stack Cloud Security Architecture and Operations

As more businesses operate online using cloud computing platforms such as Amazon Web Services (AWS), it is critical to implement a full-stack security architecture. The diagram below depicts a typical "stack" consisting of the environment, application(s), data, operating system and the cloud platform that must be protected.

stackArmor Full-stack Cloud Security Architecture


stackArmor
Environment/Enclave
Application
Data
Operating System
IaaS
Full-stack Security Architecture
IDS/IPS/IAM/Monitoring
Web Application Firewall
Encryption At Rest and in Motion
Hardening, Patching
Network Segregation
Policies, Procedures, Tools
Basic Security Policy
Security Assessment Plan
Security Assessment Report
Vulnerability and Penetration Testing
External Review/Validation
Shared Responsibility Model

It is critical for the security architecture to take into consideration the shared responsibility model of the underlying cloud platform that clearly defines roles & responsibilities. The architecture must be supported by policies, procedures and tools for secure operations.

2 Changing Business and Technology Landscape

Cybersecurity attacks have increased manifold with nearly daily news about data breaches that are stressing consumer confidence and causing regulators to take notice. The Securities and Exchange Commission (SEC) recently fined an Investment Advisor with failing to adoption proper cybersecurity policies and procedures prior to a data breach that comprised PII for 100,000 individuals. Similarly, the Federal Trade Commission (FTC) charged a Dental Practice software provider for misleading claims about securing patient data. Recent court judgements have established the rights of Federal regulatory agencies to "police" cybersecurity practices of firms. This is causing wide spread changes in the business landscape right from increased scrutiny of security practices as part of the due diligence process, increasing business insurance premiums for online businesses, and Board level interest in a firms' cybersecurity exposure.

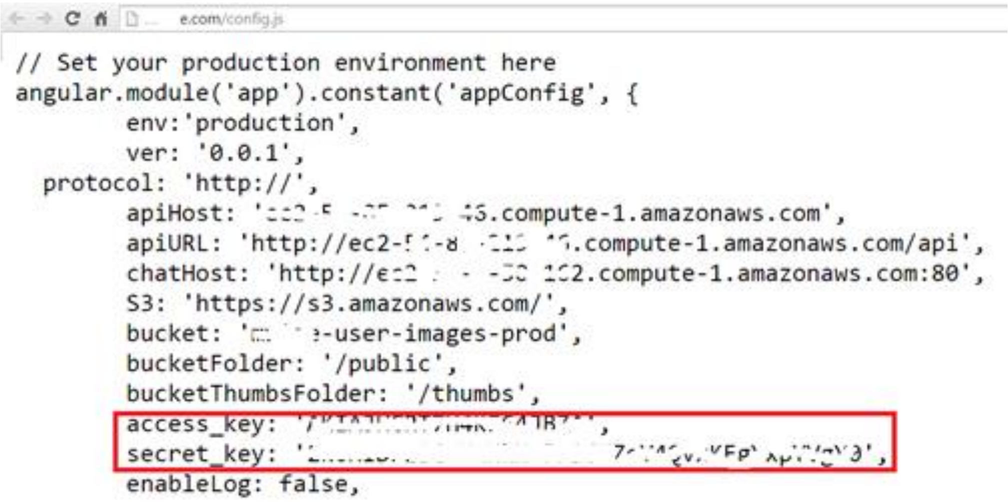
Furthermore, as more software is bought "as-a-service" instead of being shrink-wrapped, more businesses must get into the cloud operations business that traditionally do not have cloud and security operations experience. In practice, most SaaS businesses tend to be stronger on the development practices and weaker on operations. Cloud operations requires taking into consideration patching. vulnerability management, boundary protection, enclave hardening, micro-segregation, and continuous monitoring. In order to operate safely, management attention to strong cloud and security operations is critical.

2.1 Some real-world examples

Operating an online business requires an understanding of the Shared Responsibility Security Model and well trained resources to help create a secure and compliant hosting environment. We have seen some real challenges that demonstrate a lack of rigor and focus on security. Here are some examples:

"…while doing cloud hosting cost analysis for a venture funded start-up with $8 million of VC capital, we noticed heavy data egress charges. A simple analysis revealed that a hacker from China penetrated the platform and downloaded the firms' database and IP". The vulnerability was traced to a web application vulnerability.

"…a SaaS startup exposed their access secret key in their web application in plain view for anyone to access. This could have caused someone to wipe out the firms' entire production and operational platform…"



```
// Set your production environment here
angular.module('app').constant('appConfig', {
        env:'production',
        ver: '0.0.1',
  protocol: 'http://',
        apiHost: '[redacted].compute-1.amazonaws.com',
        apiURL: 'http://ec2-[redacted].compute-1.amazonaws.com/api',
        chatHost: 'http://[redacted].compute-1.amazonaws.com:80',
        S3: 'https://s3.amazonaws.com/',
        bucket: '[redacted]-user-images-prod',
        bucketFolder: '/public',
        bucketThumbsFolder: '/thumbs',
        access_key: '[redacted]',
        secret_key: '[redacted]',
        enableLog: false,
```

Organizations must take a SecurityFirst approach to their online business to contain increasing business risk that can cripple the entire firm.

3 Security Best Practices

stackArmor engineers have been migrating and managing workloads on AWS since 2009 for security conscious customers. Our **SecurityFirst** design approach begins with understanding the security posture with regard to confidentiality, integrity and availability. The nature of the data and the potential threat vectors, help create a customized security architecture and operations framework.

3.1 Environment/Enclave Protection

The hosting environment must be designed to be resilient and secured to protect the applications and data from malicious internal and external threats. Specific best practices include:

- Ensure boundary and enclave protection by installing an **Intrusion Prevention Systems/Intrusion Detection System (IDS)**. There are multiple solutions that exist in the market place from leading providers such as Sophos, Fortinet and many others. There are open source solutions such as Snort for IDS.
- Establish **secure connectivity** to the environment for privileged users such as administrators and developers accessing the underlying servers and applications. Creating VPN based access is ideal especially, when the user community is distributed. There are multiple options from providers such as Cisco and open source providers such as OpenVPN and pfSense amongst others.
- Create **policy based access management framework** for accessing cloud resources using the Identity and Access Management (IAM) module. The IAM policies should ensure that access is controlled and avoids leaving wide-open rules. Additionally, a clear separation of roles should be established e.g. production instance access should be limited to a specific set of users ensuring that any other users in the system cannot terminate these instances. Please refer to Appendix A for a sample list of common IAM configuration conditions and alerts.

3.2 Application Protection

Applications hosted in the cloud environment should be tested for specific vulnerabilities using scanning tools such as Acunetix, HP Webinspect or Nessus amongst others. The hosting environment must be designed to be resilient and secured to protect the applications and data from malicious internal and external threats. Specific best practices include:

- Install a **Web Application Firewall (WAF)** to provide continuous protection against common cross-site scripting (XSS) and SQL injection attacks amongst others. Common tools include Fortinet’s Fortiweb, Sophos UTM or AWS Web Application Firewall (WAF) amongst others.
- Perform **web application vulnerability** scans prior to releasing the software into production. This activity can be integrated into the Continuous Integration/Continuous Deployment pipeline through tools such as Acunetix, Webinspect or Nessus amongst others. Additionally, in the event that sensitive data is accessed by the application, static code scanning prior to deploying the code should be performed. Tools such as Checkmarx amongst others are available options.

3.3 Data Protection

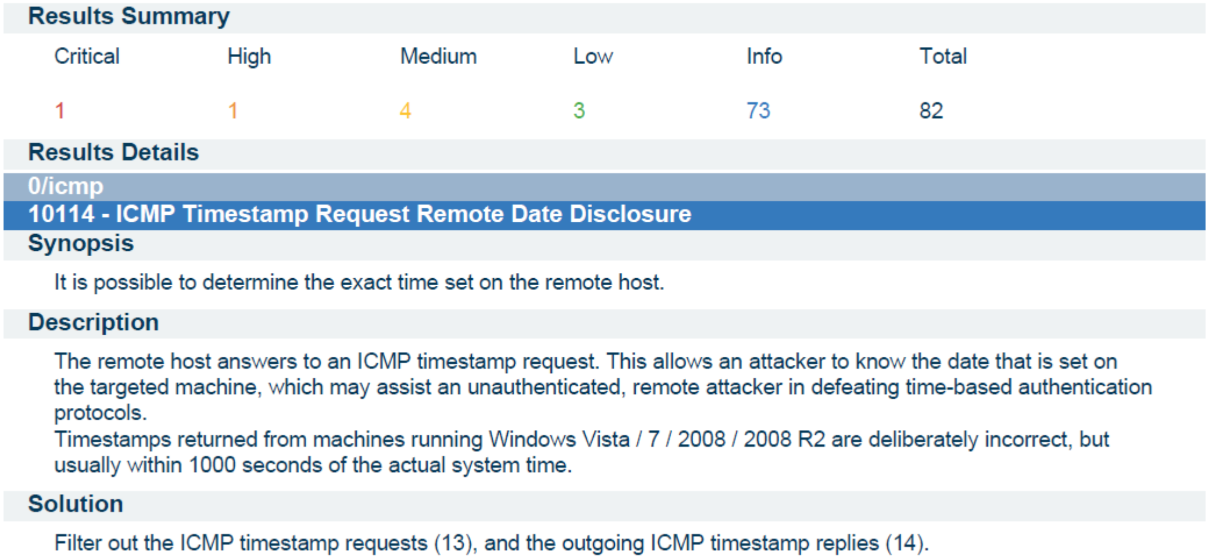
The emerging best practice is to encrypt data both at rest and in motion. Data protection should be viewed holistically and include data in the database, data residing on disk and backup data. Cloud platforms such as AWS provide a wide variety of encryption options including EBS-boot volume encryption, AWS s3, EBS volumes and various data services such as Aurora amongst others. Specific best practices include:

- Protecting **Data in Motion (DAM)** should be strongly considered between various system components including client browser and web server as well as between application server and database servers.
- Establish **Data at Rest (DAR)** policies that cover all data source including archives, backups, data on disk and persistent storage like s3, and EBS volumes. AWS offers multiple Key Management Services (KMS) options including CloudHSM. Data resident in databases should take into consideration using Transparent Data Encryption (TDE). TDE can be used in conjunction with encryption at rest, although using TDE and encryption at rest simultaneously might slightly affect the performance of your database.

3.4 Operating System and Installed Components

Most cloud platform have a well defined Shared Responsibility Model that requires customers of the platform to ensure the integrity of their environment. Most IaaS platform require operating system and above to be maintained by the user. Specific best practices include:

- **Harden the environment** by using configuration settings prescribed by Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG). Also, organizations such as the Center for Internet Security (CIS) provide hardening guides.
- Establish a **patching policy** for the operating system and all installed software components such as application servers, database servers and supporting components. The patching policy and procedure should ensure a robust change management process with testing of the application prior to rolling into production.
- Perform **periodic vulnerability scans** to check for vulnerabilities in the system. Tools such as Retina, Nessus, and OpenVAS are common examples of software packages for vulnerability scanning. The screenshot below shows the output from a vulnerability scan run.



Results Summary

Critical	High	Medium	Low	Info	Total
1	1	4	3	73	82

Results Details

0/icmp

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

3.5 IaaS Platform Operations

Cloud computing platforms provide powerful management and operation tools that make it easy to operate a secure and robust environment. It is critical to follow security and operational best practices to allow for proactive detection of issues. Specific best practices include:

- Architect micro-segmentation of enclaves through the proper of zoning through **private and public sub-nets**. Proper zoning through sub-nets allows for segregating network traffic and black-holing requests in the event of an attack.
- Implement strong **continuous monitoring** and establish key metrics of interest. Services such as AWS VPC Flow Logs provide insight into network traffic, and by tracking metrics such as Rejected Traffic, Most Talkers anomalous traffic can be detected. AWS CloudTrail provides visibility into actions performed by users in the environment e.g.,Who deleted my instances? Who is asking for old or deleted keys? Also, AWS Config helps track changes to configuration settings in the environment.

4 Compliance

As cybersecurity issues become more urgent and important for customers of outsourced IT and software services, compliance with security standards such as ISO 27001 is expected. Most buyers of hosted solutions are looking for ways to contain third-party risk. It is critical for cloud platform operators to have a formal compliance program to contain business liability and risk as well as ensure the ability to attract security conscious customers.

SaaS and cloud platform operators should put in place a formal compliance program that is right sized for their business. At a minimum the following activities should be performed:

- Complete an information security risk assessment with an executive summary report to identify any deficiencies in administrative, physical, and technical safeguards;
- Document current information security posture for executive and technical leadership;

- Document mitigation activities required to address administrative, physical, and technical risks identified during the risk assessment;

stackArmor has developed a simple and effective methodology that adapts from FISMA and NIST standards for cybersecurity and is called A.R.M^{TM} (Assess.Remediate.Monitor). The methodology and security controls assessed are drawn from NIST Special Publication 800-53 rev 4, and additionally map to international ISO/IEC 27001/27002 standards to address administrative, physical, and technical security controls. The path to an effective compliance framework begins with the creation of a risk model.

4.1 Risk Model

The risk model identifies the risk factors (threats, vulnerabilities, impact, likelihood, and predisposing conditions) to be assessed and defines the relationships among them. A *threat* is any circumstance or event with the potential for adverse impact to operations, assets, or personnel. The source of a threat can be human, environmental, or a structural failure and may be intentional or accidental in nature. A *vulnerability* is a weakness in an information system, security procedure, internal control, or implementation that may be exploited by a threat source. A *predisposing condition* is a condition that exists within the organization, its business processes, enterprise architecture, or operating environment that affects the likelihood that initiated threat events result in an adverse impact. The *likelihood* of occurrence is a weighted risk factor based on the probability that a given threat is capable of exploiting a given vulnerability. The *impact* of a successful exploitation of a vulnerability or predisposed condition is a measure of the magnitude of harm that could be expected to the firm, its assets, or personnel.

4.2 Assessment Approach

A hybrid assessment approach that combines the measurable aspects of a traditional quantitative assessment with the flexibility of a qualitative assessment. This provides meaningful risk results that allow for prioritization. In order to provide improved rigor and effectiveness of risk analysis, a vulnerability-oriented analysis with an impact-oriented analysis to provide a more complete risk picture that identifies vulnerabilities in policy, process, and technology as well as critical assets and the impact of successful attacks against those assets.

4.3 Documents

Following is a complete list of all project deliverables that help in creating a tangible compliance model and framework for a typical organization.

Document	**Description**
Basic Security Policy	This document provides a basic set of high level security policies that allow client to state that they have a security policy in place that can serve as an initial baseline.
Assessment Plan	This is a checklist security assessment, basically a self-assessment with questions asked by an experienced Information

	Assurance Analyst to demonstrate understanding and maturity of Cybersecurity posture.
High Level Security Assessment Report	Security Assessment Report (SAR) that summarizes the scope, approach, high level findings and recommendations. The high-level recommendations are for any security controls found to be “not in place” and include description of actions necessary to show the security control is “in place”.
Vulnerability and Penetration Testing	Automated scans with basic parameters with provided auto-generated reports. This effort will include working with the App47 team to perform a re-test to ensure that any technical remediation that have been applied adequately addressed the vulnerabilities found.
Letter of Attestation	Executive summary of assessment signed by an experienced and certified Cybersecurity Specialist. The letter will attest to the overall level of risk (Low, Moderate, High) based on the security controls found to be “not in place” and it will include a reference to the methodology utilized to categorize the system being assessed, selection of security controls assessed.

5 References

- **SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach**

  https://www.sec.gov/news/pressrelease/2015-202.html

- **Dental Practice Software Provider Settles FTC Charges It Misled Customers About Encryption of Patient Data**

  https://www.ftc.gov/news-events/press-releases/2016/01/dental-practice-software-provider-settles-ftc-charges-it-misled

- **FTC has power to police cyber security: appeals court**

  http://www.reuters.com/article/us-wyndham-ftc-cybersecurity-idUSKCN0QT1UP20150824

- **Contractor breach gave hackers keys to OPM data**

  http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/23/keypoint-usis-opm-breach/28977277/

- **NIST Cybersecurity Framework**

  http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

6 About stackArmor

stackArmor is staffed with experienced professionals that have many years of experience in providing full lifecycle systems development and maintenance services including infrastructure and cybersecurity. The company's principals have worked with large and small organizations in various sectors including Government, Financial Services, Healthcare, Non-profits and SaaS markets. Learn more by visiting https://www.stackarmor.com or send us an email at solutions@stackarmor.com

DevOps and Process Automation	**Cybersecurity Engineering**	**AWS Migration and Managed Services**	**Training & Support**

stackArmor deploys integrated teams of certified Solution Architects and Senior Engineers with real-world deployment experience and expertise. Our full-stack approach integrates systems engineering and operations, networking and routing, cybersecurity engineering and compliance, and performance engineering to support large and mission critical cloud platforms operating at scale with stringent SLA's.

DevOps and Process Automation

We accelerate development and deployment processes by implementing DevOps and Agile Development practices using tools such as CHEF, Ansible, Puppet and Atlassian's Agile Development Suite.

Cybersecurity Engineering and Vulnerability Management

We support Federal, Healthcare and Defense customers requiring compliant solutions and expertise with boundary protection, system hardening (DISA STIG's), continuous compliance and vulnerability management.

AWS Cloud Migration and Managed Services

Migrating and managing an AWS cloud environment requires a deep understanding of virtual private cloud, networking, environment configuration and cost optimization as well as managed services.

Training and Custom Support

We provide customized training delivered by trainers with real-world implementation experience helps our customers become self-sufficient. We also offer Cloud Coaches to help with continued mentoring and assistance.

Send us an email at solutions@stackarmor.com to schedule a free security architecture review and consulting call.

7 Appendix A: Common IAM Configuration Alerts and Conditions

Sub-System	Configuration	Comment
IAM	User has full admin privileges.	User has full admin privileges.
IAM	User has full IAM privileges.	User has full IAM privileges.
IAM	User has IAM privileges.	Alert when an IAM Object has a policy allowing 'iam:XxxxxXxxx'
IAM	User has iam:PassRole privileges.	Alert when an IAM Object has a policy allowing 'iam:PassRole'. This allows the object to pass any role specified in the resource block to an ec2 instance.
IAM	User policy contains NotAction.	Alert when an IAM Object has a policy containing 'NotAction'. NotAction combined with an "Effect": "Allow" often provides more privilege than is desired.
IAM	User can change security groups.	Alert when an IAM Object has ec2:AuthorizeSecurityGroupEgress or ec2:AuthorizeSecurityGroupIngress.
IAM	Allows assume-role from anyone.	Alert when an IAM Role has an assume_role_policy_document but using a star instead of limiting the assume to a specific IAM Role.
IAM	Cert size is less than 1024 bits.	Alert when a cert is using less than 1024 bits
IAM	Cert size is less than 2048 bits.	Alert when a cert is using less than 2048 bits
IAM	Cert uses an MD5 signature Algorithm	Alert when a cert is using md5 for the hashing part of the signature algorithm
IAM	Cert uses an SHA1 signature Algorithm	Alert when a cert is using sha1 for the hashing part of its signature algorithm. Microsoft and Google are aiming to drop support for sha1 by January 2017.
IAM	Cert will expire soon.	Alert when a cert's expiration is within 30 days
IAM	Cert has expired.	Alert when a cert has expired
IAM	Cert may have been compromised by heartbleed.	Alert when a cert was uploaded pre-heartbleed.
IAM	User has active accesskey.	Alert when an IAM User has an active access key.
IAM	Active accesskey has not been rotated.	Alert when an IAM User has an active access key created more than 90 days go.
IAM	User with password login and no MFA devices.	Alert when an IAM user has a login profile and no MFA devices. This means a human account which could be better protected with 2FA.
IAM	User with password login and API access.	Alert when an IAM user has a login profile and API access via access keys. An account should be used Either for API access OR for console access, but maybe not both.
RDS	POLICY - Redshift cluster not in VPC.	Alert when not running in a VPC.
S3	ACL - AuthenticatedUsers USED.	ACL - AuthenticatedUsers USED.
S3	ACL - AllUsers USED.	ACL - AllUsers USED.
S3	ACL - Unknown Cross Account Access.	ACL - Unknown Cross Account Access.

Use or disclosure of data contained on this page is subject to the restrictions on the cover page of this proposal

S3	POLICY - This Policy Allows Access From Anyone.	POLICY - This Policy Allows Access From Anyone. Note: There's two conditions under which this code may be logged - both imply access from everyone hence not duplicating the log code.
S3	POLICY - Unknown Cross Account Access.	POLICY - Unknown Cross Account Access.
S3	POLICY - This policy has conditions.	POLICY - This policy has conditions.

Please note the list above provided is a starting point for helping detect and remediate policy configurations for securing access to cloud resources. The list is not exhaustive or complete and must be adopted by reviewing the specific security posture and requirements of the application and data.