stackArmor

Cloud Solutions for
Security Focused Customers

Creating a NIST/FedRAMP Compliant Architecture

Security by Design

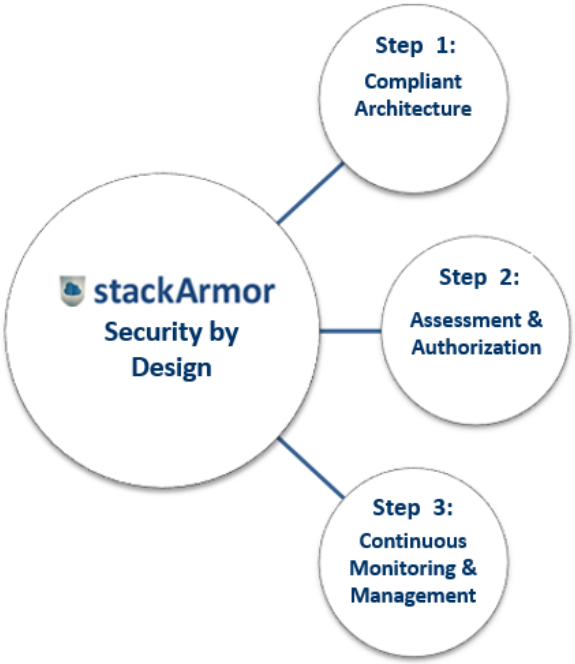
2018

CONTENTS

1. Security by Design 1
2. Compliant Architecture 2
2.1 Well-engineering Landing Zone 4
2.1.1 Boundary Protection with Web Application Firewall 5
2.1.2 Network Segmentation and Separation of Servers & Data 5
2.1.3 Network and Access Management 6
2.1.4 Database Encryption 6
2.1.5 Logging and Monitoring 6
2.1.6 System Hardening and Compliance with Industry Best Practices 6
2.1.7 Vulnerability Management and SCAP compliance scanning 7
3. About stackArmor 7

1. SECURITY BY DESIGN

Organizations in regulated markets such as the federal government, public sector, healthcare or financial services must meet specific compliance standards for IT systems. Amazon Web Services (AWS) provides all the necessary tools to allow the creation of compliant architectures meeting NIST, FedRAMP, HIPAA or PCI-DSS standards. stackArmor has developed the **Security by Design** methodology with three simple steps to ensure that the developed solution can meet regulatory compliance requirements.



Step 1 consists of creating an architecture composed of AWS services that meet the specific compliance standard. The architecture must meet the baseline security requirements as codified in NIST Special Publication 800-53 or similar.

Step 2 is creating the governance and compliance evidence codified in the form of policies, procedures and security control implementations.

Step 3 is the on-going monitoring, operations and security management of the system. These on-going activities include logging, monitoring, vulnerability management and security operations.

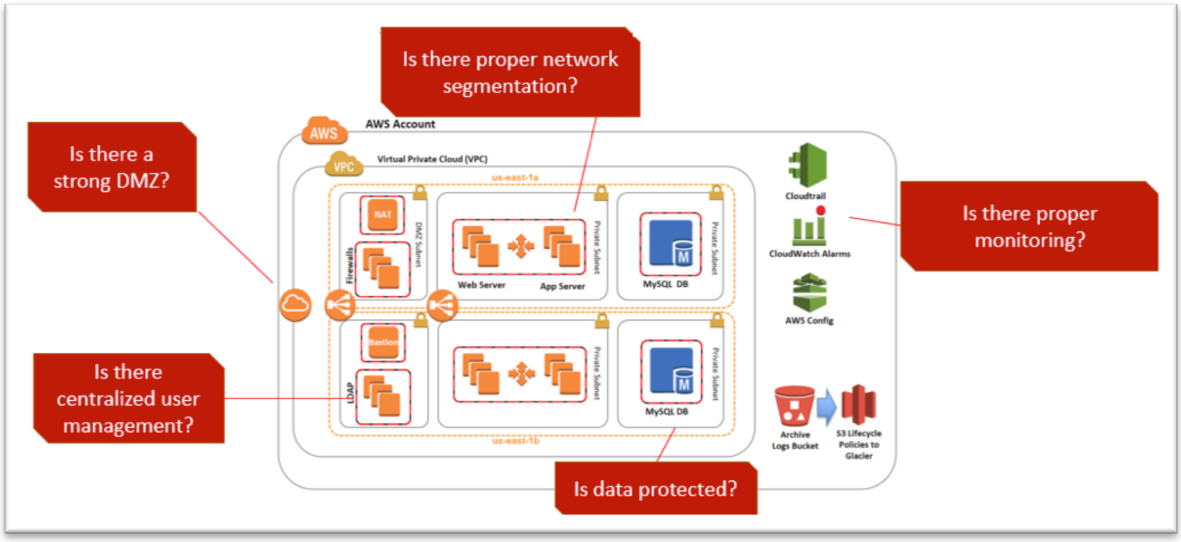
2. DEVELOPING A COMPLIANT SOLUTION ARCHITECTURE

A compliant solution architecture is based on a set of specific security and compliance requirements that are codified as part of an accepted standard such as NIST Cybersecurity Framework, NIST SP 800-53, FedRAMP, HIPAA or PCI-DSS. Cloud service providers such as AWS provide a wide variety of services to meet the needs of a diverse range of use cases and deployment scenarios. However, developing a compliant architecture begins with limiting the solution architecture to only accredited services listed. AWS publishes the accreditation level of their services on their Compliance in Scope resource page. Developing the compliant architecture requires mapping security requirements to specific solution components. The table below shows common NIST-specified security control families with corresponding services that help meet the requirement.

Control Family	Applicable AWS Services
Access Control	IAM
Awareness and Training	AWS Training Courses on Security, Operations
Audit and Accountability	Multi-Accounts, CloudWatch, CloudTrail
Configuration Management	Config, Service Catalog, Marketplace
Identification and Authentication	Cognito, Directory Service
Incident Response	Lambda, SNS, CloudWatch Logs & Metrics
Maintenance	Systems Manager, Inspector
Media Protection	EBS, S3 Encryption, KMS, Macie
Personnel Security	*Only worry about Application and Data*
Physical Protection	*Leverage AWS FedRAMP ATO*
Risk Assessment	Trusted Advisor, Artifact
Security Assessment	ELK, SplunkCloud

System & Comm. Protection	IDS, IPS, WAF, VPC, Security Groups, Sub-nets
System & Information Integrity	Multi-Region, Multi-VPC, Multi-AZ, ASG, ELB

Once the appropriate services have been selected, we must take a holistic approach to incorporating best practices as codified in a compliance standard. Based on multiple production deployments and common design flaws we have observed over the past 8 years, we have created an infographic that shows some very common errors and architectural security "hotspots." See below.

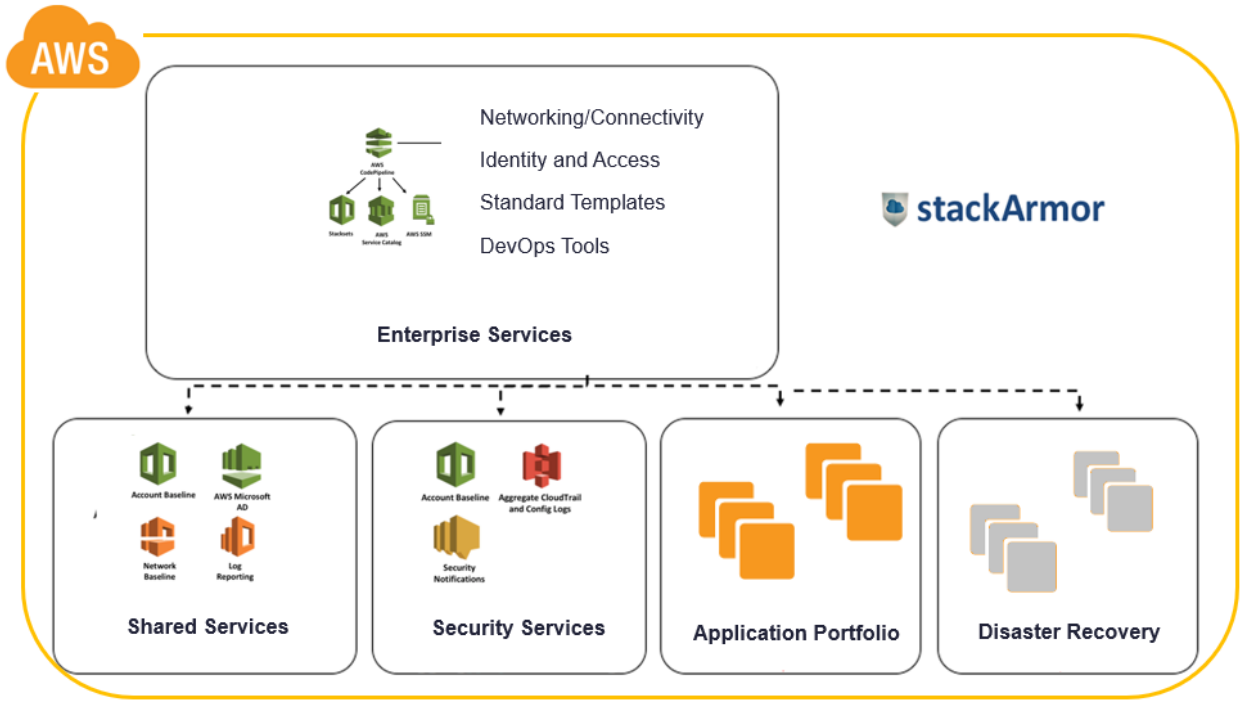


Logical view of common security hotspots that must be addressed by a compliant architecture that meets security standards such as PCI-DSS, HIPAA, NIST or FedRAMP.

Following proper systems engineering principles that address these key security hotspots is critical. For example, the boundary must be protected using a Next Generation Firewall as well as having a centralized Microsoft Active Directory/LDAP solution to allow for Privileged user access and centralized authentication. Further, the developers must access the environment using protected and encrypted means. Given the sensitivity of the data, there are data encryption requirements for data at rest and in motion.

2.1 TRUSTED LANDING ZONE

The output of the architecture definition phase is the creation of a blueprint commonly referred to as a landing zone. Based on industry best practices and real world deployment experience, a Trusted Landing Zone (TLZ) incorporates systems engineering and security practices, including resilience, separation of roles and responsibilities, security services, foundational enterprise services and disaster recovery. The diagram below provides an overview of a Trusted Landing Zone (TLZ) and its components.



stackArmor Trusted Landing Zone architecture includes in-built scalability, resilience and security engineering features for consistency across applications and business *services.*

The architectural components of a Trusted Landing Zone (TLZ) are further described below.

Enterprise Services: These are foundational services that allow for network connectivity, identity and access management, hardening templates and platform tools for DevSecOps. Each one of these services must be architected based on the specific needs of the organization. For example, there are primarily three connectivity pathways 1) point to point IPSEC VPN over the internet 2) Cloud native services, such as AWS DirectConnect and 3) Cloud Connectivity Hub solutions, such as AT&T Netbond or something similar.

Shared Services: Ensuring cost-efficient operations by using common services is critical to reducing complexity and promoting agility. Selecting and implementing shared services for code repositories such as Github or publishing standardized machine instances using AWS Service Catalog are good examples of Shared Services.

Security Services: The ability to continuously monitor and respond to security and systems incidents and events is a critical requirement for ensuring the security of the environment. The security services stack covers compute, storage, network, and application as well as data monitoring. The ability to monitor file changes, anti-virus, cloud configuration integrity and vulnerability management are just common examples of services that are part of Security Services.

Application Portfolio(s): Application and data are segregated from the rest of the system components to allow for maximum security through separation of roles and responsibilities. Segregated application and data enclaves allow for efficiencies by allowing the consumption of common security, management and enterprise services.

Disaster Recovery: Creating a DR or COOP environment is a critical requirement for resilient operations. There are various models to choose from, including cold, pilot-light or "hot-hot" models. Each one of these variations have varying levels of cost and, depending on the SLA for RTO and RPO, the right architecture must be implemented.

2.1.1 Boundary Protection with Firewall

The state-of-the-art firewall layer will protect the security and integrity of the application and prevent malicious traffic at the edge. AWS offers a variety of solutions, including third-party solutions, such as Palo Alto Networks, Cisco, Sophos and Fortinet and others. AWS native services such as Web-Application Firewall, and Cloudfront Shield also offer edge protection.

Typically, all traffic to a website, including registered users, anonymous and administrative traffic, is controlled by security groups and a Web Application Firewall-enabled (WAF) Application Load Balancer (ALB).

2.1.2 Network Segmentation and Separation of Servers & Data

Creating well-defined trust zones using sub-nets and security groups helps ensure public and private traffic is well managed. Separate enclaves for Production, Test and Dev should be

provisioned, segregated by Virtual Private Cloud (VPC), subnets and security groups (network access control). The web application(s) and data should be segregated through private subnets.

2.1.3 Network and Access Management

All access to the environment shall be through secure means, including the use of centralized authentication and access management, using Microsoft Active Directory (AD)/LDAP, Bastion or VPN based access to servers for administrators and developers.

2.1.4 Data Encryption

The data should be protected at rest and in motion. Data in motion typically is protected using SSL/TLS protocols for both internet and internal communications. All data at rest should be encrypted using AES-256 in the EBS volumes and S3 buckets, including archival and staging data. Additional database protection can be enabled using TDE, which is supported by most database programs.

2.1.5 Logging and Monitoring

In compliance with NIST, HIPAA, PCI-DSS or FedRAMP/FISMA requirements, continuous monitoring and compliance are implemented using Amazon GuardDuty, CloudWatch, Config, CloudTrail and VPC Flow logs. These are cloud-native services for tracking activity, configuration changes and access control/tracking for any changes within the AWS environment configured for the application.

2.1.6 System Hardening and Compliance with Industry Best Practices

The hosted environment should be hardened and configured based on industry best practices, such as CIS (Center for Internet Security), DISA STIG, or similar benchmarks. Multiple options are available in the marketplace for hardening and compliance that must be tailored to meet specific enterprise requirements.

- Creating custom images using DISA STIGs

- Applying CIS (Center of Internet Security) benchmarks
- Buying CIS-hardened images from the AWS Marketplace

Typically, a government-focused environment will use a DISA STIG standard for hardening the environment. However, commercial customers may use the CIS standards. If there are specific customization requirements, buying an off-the-shelf image may not be the right option and creating a custom hardened gold image is the right path.

2.1.7 Vulnerability Management and SCAP compliance scanning

Periodic vulnerability scanning using SCAP-compliant third-party commercial services or cloud-native services, such as AWS Inspector, must be implemented. The environment should be patched and scanned for vulnerabilities on a monthly basis at least, preferably as part of a CI/CD pipeline. In the event that serverless or container-based deployments are made, then special security scans for code and containers are required. Technologies such as Anchore.io, Twistlock and Docker Trusted Registry are commonly used third-party technologies.

3. ABOUT stackArmor

stackArmor is a provider of Cloud Advisory, Cloud Implementation, and Cybersecurity and Compliance services for healthcare, financial services and public sector customers. As an AWS Authorized Reseller, AWS Public Sector Partner and AWS GovCloud competency holder, stackArmor specializes in delivering secure and compliance-oriented AWS solutions, including cloud strategy, platform architecture, devops implementation, migration services, managed services and managed security services. Our experts help protect you from the cyberthreat challenges through systems engineering best practices developed over decades while working with US government agencies that require compliance with ISO 27001, NIST, FFIEC, FISMA, FedRAMP, DHS and DISA standards.

AWS Advanced Partner

AWS Public Sector Partner

AWS Security Competency Partner

AWS GovCloud Partner

AWS NoSQL Partner

We are a member of the AWS Partner Network and have trained and certified AWS Solution Architects to enable our customers' transition to secure cloud computing. We are **1 of only 10 firms selected by AWS** from around the world for the Security Competency launched in July 2017. Our cybersecurity services include design of secure environments; implementation of automated intrusion detection, vulnerability and log management services; and helping modernize Enterprise IT operations through automation of cybersecurity, development and operations activities, as well as FISMA/FedRAMP security authorization and accreditation support.

Our customers include US government agencies such as DOT, HUD, US Treasury, DOD, OSD, HHS, DHS, USCIS, and commercial customers such as SAP, Ricoh, Verizon and others. The company's principals have won Industry awards such as the Fed 100 and GCN Rising Star, and are recognized thought leaders in the Cloud and security space, with membership in prominent organizations such as the Digital Innovation Technology Strategy (DIGITS) at the University of Maryland's Robert H Smith School of Business, Technology Council of Maryland and the Northern Virginia Technology Council (NVTC).

CONNECT WITH US

https://www.linkedin.com/company/stackarmor-inc-/

https://twitter.com/stackArmor

stackArmor has extensive professional experience in delivering secure and compliance-oriented IT solutions to regulated industries in Government, Financial Services, Healthcare and Energy. Our experts help protect you from the cyberthreat challenges through systems engineering best practices developed over decades while working with US government agencies that required compliance with NIST, FFIEC, FISMA, FedRAMP, DHS and DISA.

We enable your company's transition to secure cloud computing through the lifecycle, which includes the design of secure environments; implementation of automated intrusion detection, vulnerability and log management services; and helping modernize Enterprise IT operations through automation of cybersecurity, development and operations activities.

THANK YOU

stackArmor

Cloud Solutions for
Security Focused Customers

gpal@stackArmor.com
www.stackArmor.com