stackArmor

Cloud Solutions for
Security Focused Customers

Continuous Cloud Threat Monitoring and Compliance

2018

CONTENTS

1. Continuous Threat Monitoring and Response

McAfee Cloud Adoption & Risk Report

Enterprise organizations have an average of 14 misconfigured IaaS/PaaS instances running at one time, resulting in an average of 2,269 individual misconfiguration incidents per month.

5.5% of AWS S3 buckets have world read permissions, making them open to the public.

stackArmor ThreatAlert™ is an **in-boundary** continuous cloud security monitoring and compliance solutions for compliance focused customers. Organizations in healthcare, public sector and financial services are constantly worried about data breaches and cybersecurity threats due to constant configuration changes due to devops and the dynamic nature of cloud services. stackArmor ThreatAlert™ provides a holistic security event monitoring and management service that is based on US Federal Government security standards embodied in the NIST Special Publication 800-53 that is the underlying basis for the NIST Cybersecurity Framework, HIPAA, MARS 2.0 E, and other similar compliance frameworks.

Figure: stackArmor ThreatAlert™ service for threat monitoring, management and incident response for security focused customers in Public sector, Healthcare and Financial Services industries.

stackArmor ThreatAlert™ provides comprehensive full-stack threat monitoring and incident response support. The solution has been developed by stackArmor's Security and Cloud Solution Architects that have supported cloud migrations and security operations since 2009 for US Federal and Department of Defense customers. stackArmor is a AWS validated Advanced Consulting Partner and was 1 of 10 firms worldwide selected by AWS as an inaugural launch partner for the security competency.

2. Bulletproof Cloud Security and Operations (SecOps)

The US National Institute of Standards and Technology (NIST) has developed a comprehensive information systems security requirements framework for protecting the confidentiality, integrity and availability of digital systems. stackArmor's cloud architecture, security and compliance experts have distilled these requirements into a cloud-specific SecOps framework for organizations looking to meet or exceed FedRAMP, FISMA, HIPAA, MARS 2.0 E or similar security and compliance standards. The infographic below provides a comprehensive set of requirements for security and operations on AWS.

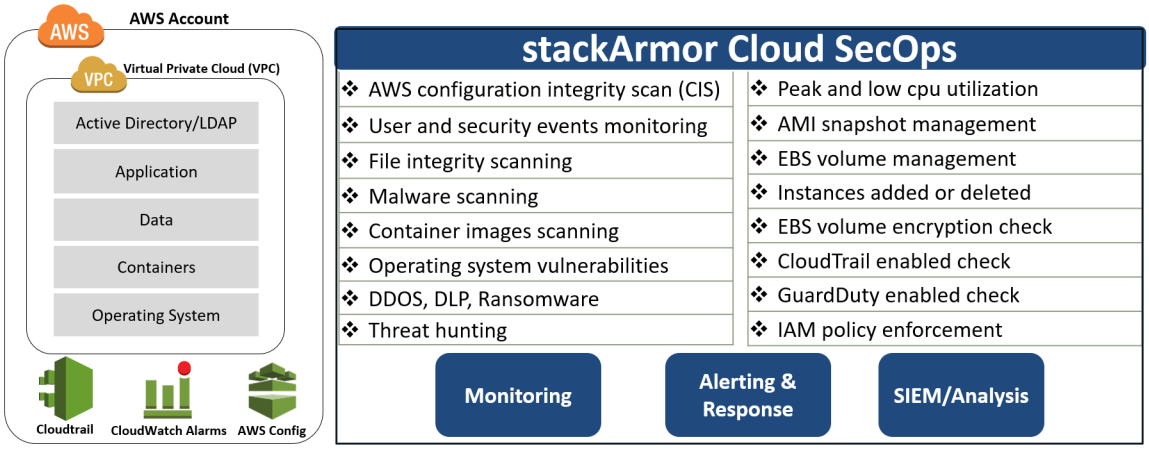

Figure 2: Comprehensive cloud security and operations framework for security focused customers in healthcare, financial services, and public sector organizations.

stackArmor has developed a comprehensive solution for organizations looking for an effective security and compliance service for AWS hosted applications and data. The stackArmor cybersecurity and compliance platform provides a tailored solution that meets security and compliance needs of organizations. The infographic below provides an overview of the solution. The platform has three integrated components for security operations and compliance – stackArmor ThreatAlert™, stackArmor OpsAlert™ and stackArmor RapidSSP™.

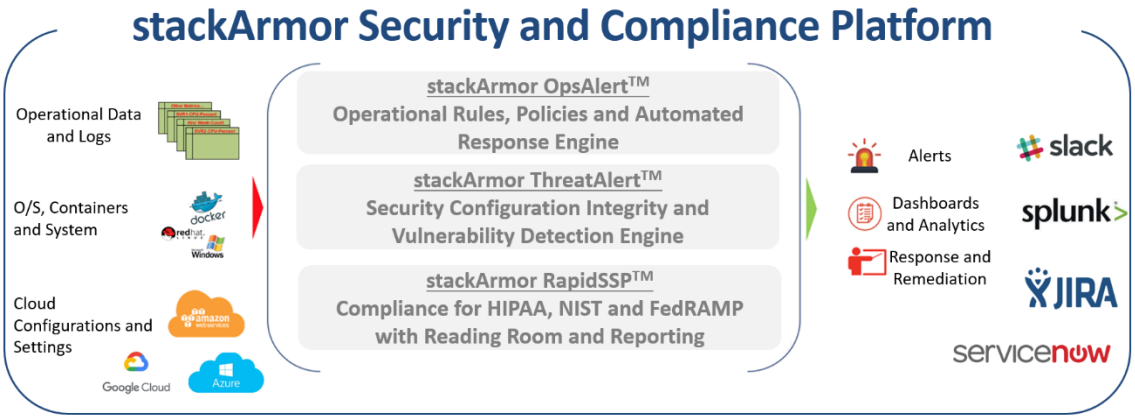

Figure 3: Integrated cloud security operations, incident response and compliance solution

The stackArmor Cybersecurity and Compliance platform is bundled with leading commercial solutions including Splunk and offers optional integrations with ServiceNow and Jira as well as Slack based alerting.

3. Cloud Threat Management with stackArmor ThreatAlert™

stackArmor ThreatAlert™ is an integrated security operations, logging, monitoring and findings management solution specifically geared towards NIST SP 800-53 compliance based environments. The stackArmor ThreatAlert™ service provides the following services and capabilities:

Threat Category	Measure or Capability	Description	Frequency of Check/Scan
AWS Configurations	Findings scored on a scale of 1-10	This scan includes common misconfiguration and security best practices that are recommended for protecting data and access including VPC, IAM, S3, RDS and others.	Daily scan with report in stackArmor ThreatAlert
Operating System Vulnerabilities	Findings scored based on the NIST CVSS score	The data is provided by a vulnerability scanner similar to AWS Inspector, OpenSCAP or similar.	Recommended atleast monthly but could be more frequent
Container Images	Findings scored on a scale of Critical, High, Medium and Low	Deep image scan of container image for common vulnerabilities using Anchore.io	Recommended as part of the CI/CD pipeline
Operational Intelligence for the Environment	Categorized as High, Medium and Low.	Aggregated collection of findings from common AWS services such as CloudTrail, GuardDuty for DDOS, Account, Instance scanning and unauthorized access.	Continuous Scan
File Integrity Scanning	Categorized as High, Medium or Low	Provided using AIDE; customization with a client provided service can be done assuming the data is readily available	Dependent on frequency of scan
Malware Scanning	Categorized as High, Medium or Low	Provided using open source version of ClamAV (only for Linux) and will use Bitdefender for Windows (which is the default service)	Dependent on frequency of scan

The screenshot below shows the dashboard and alerting for security findings in the environment with a single aggregated view of AWS configuration integrity findings, vulnerability scans, container vulnerabilities, Amazon GuardDuty alerts, and findings management for NIST Plan of Actions & Milestones (POAM) reporting.

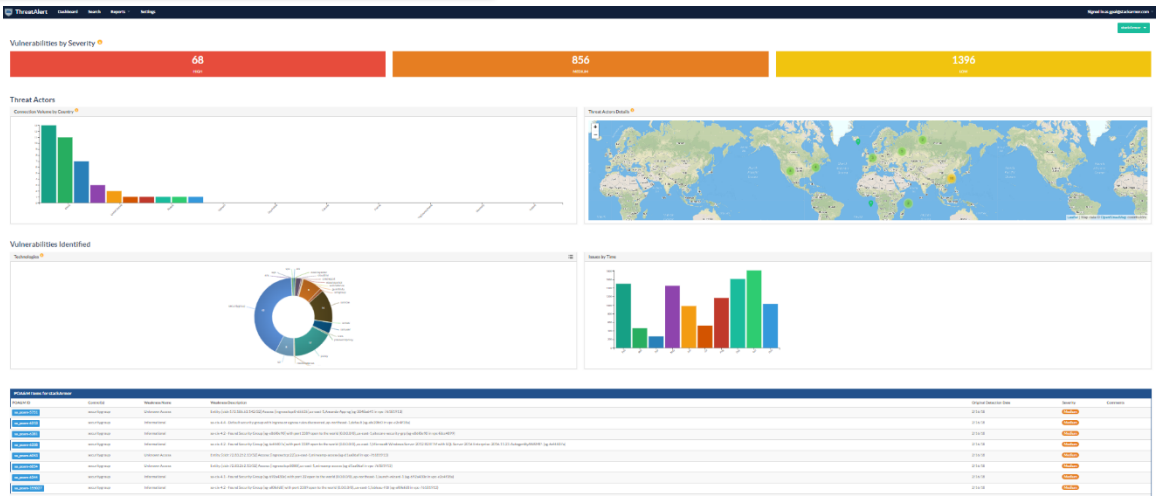

Figure 4: Screenshot of stackArmor ThreatAlert Dashboard and POAM Management System for compliance and continuous monitoring with incident response management

4. Cloud Operations Management with stackArmor OpsAlert™

stackArmor OpsAlert™ is an adaptive system operations and security governance policy engine for ensuring compliance with requirements and policies. The stackArmor OpsAlert policy engine generates alerts to policy deviations and allows the security and platform operations team the ability to enforce automated governance for shared services platfirms. The screenshot below provides a high level overview of the dashboard and alert provided from the system.

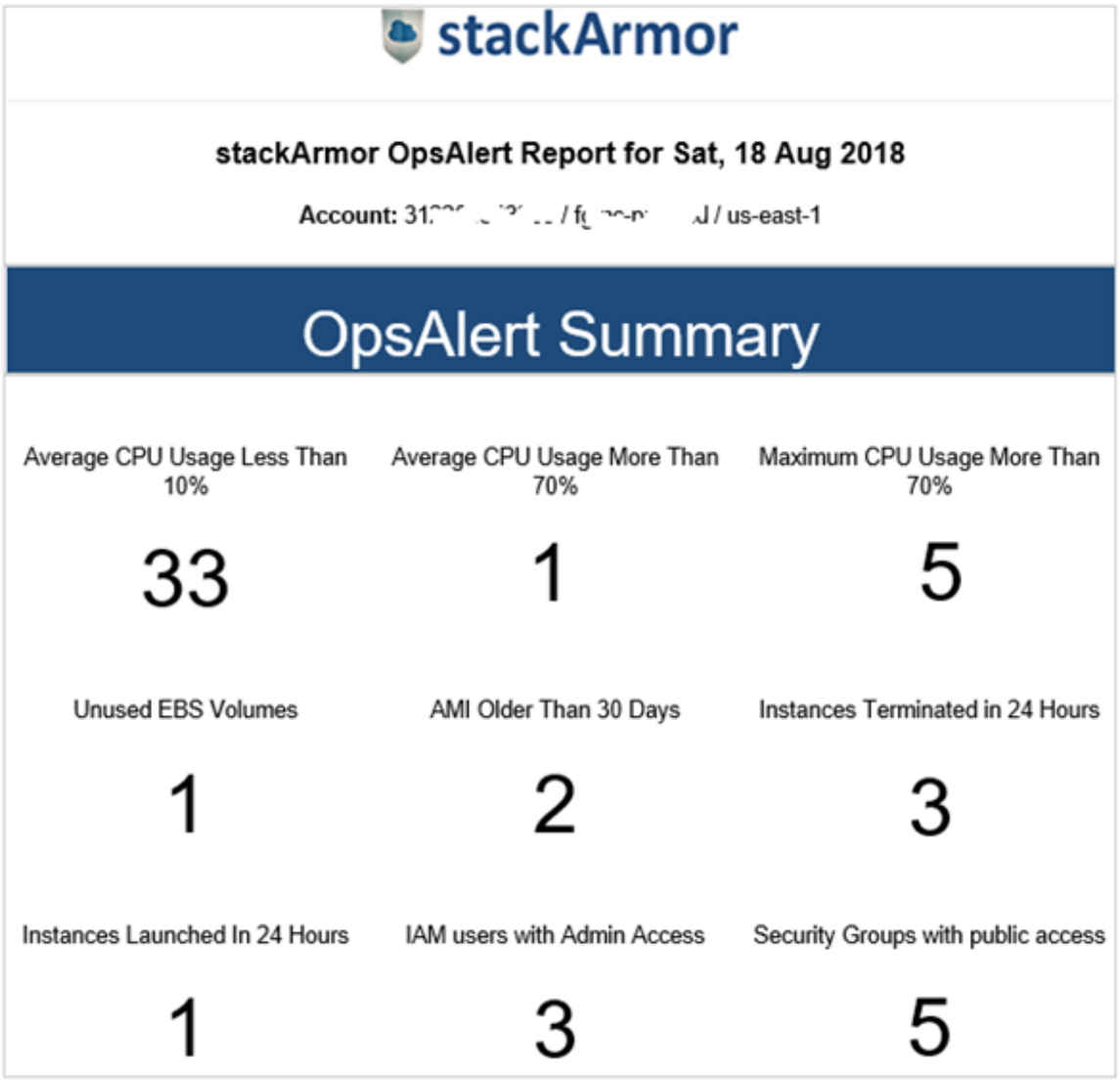

Figure 5: Screenshot of stackArmor OpsAlert Dashboard Summary for enforcement of governance policies and operational rules at-scale.

The stackArmor OpsAlert™ currently offers capability to build rules for 132 AWS resources, such as ec2, vpc, security-groups, ids etc. using with a combination of 500 plus filters, and 700 plus actions. Siemens Government can meet its compliance requirements by implementing a policy-based security and governance framework to reduce costs and oversight. The service is designed to help save money and optimize operations. We offer following policies as part of our quick-start pack, and more can be developed on customer requirements:

- List Instances with CPU utilization < 10% in last 1 Day(s) [Cost]

- List Instances with CPU utilization > 80% in last 1 Day(s) [Performance]

- Checks to make sure CloudTrail is enabled on the account for all regions [Compliance]

- List accounts with missing cloudtrails [Compliance]

- List of unencrypted EBS volumes [Security and Compliance]

- Unused AMI's older than 30 days [Garbage Collection]

- Unused EBS Volumes [Garbage Collection]

- Unused EBS Snapshots [Garbage Collection]

- Verify if MFA is enabled for root user [Security and Compliance]

- Verify if MFA is enabled for IAM users [Security and Compliance]

- Report on all images older than 120 days which should be de-registered. [Garbage Collection]

- Report running instances older than 60 days [Reporting]

- List unencrypted ids [Security and Compliance]

- Verify root access keys don't exist anymore [Security and Compliance]

- List IAM users with Admin access policy [Security and Compliance]

5. System Security Plan with stackArmor RapidSSP™

stackArmor RapidSSP™ solution is designed to be a light-weight service to help customer rapidly implement and comply with NIST requirements. The RapidSSP™ service allows the user to execute the following functions:

- Creation of System Security Plan with Security Controls based on NIST

- Creation of Plan of Actions & Milestones (POAM)

- Creation of Security Assessment Report (SAR)

The screenshot below shows the stackArmor RapidSSP solution to help customers implement SSP, SAR and POAM items for NIST compliance.

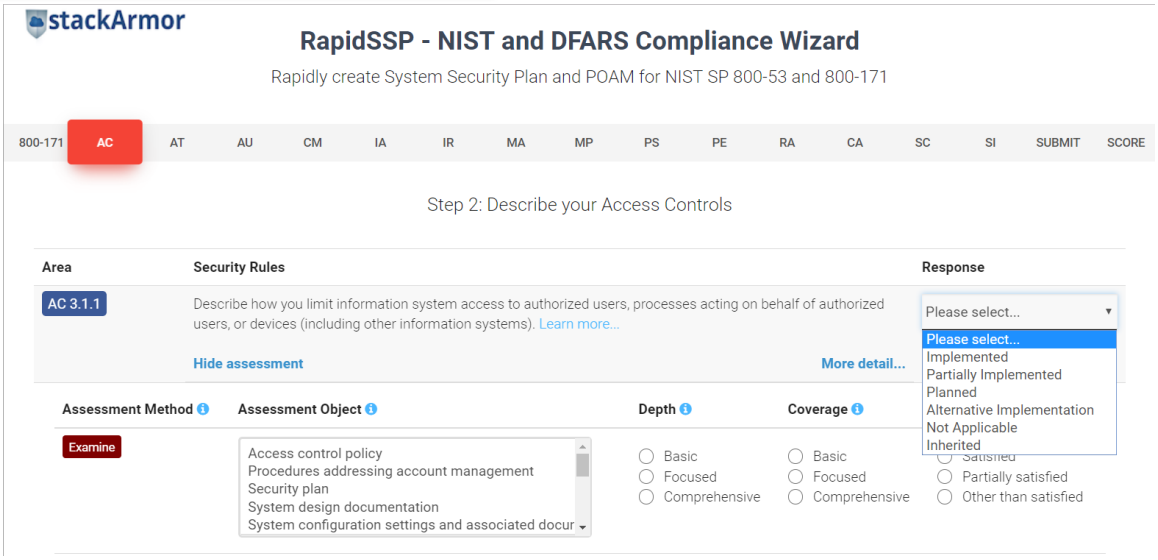

Figure 6: Screenshot of NIST SP 800-171 compliance wizard for developing and maintaining SSP, SAR and POAM templates in digital format.

6. In-Boundary Deployment Architecture

The stackArmor ThreatAlert™ solution is hosted within the customers' AWS account in a dedicated virtual private cloud (VPC) based on AWS security best practices. The infographic below provides an overview of the proposed high-level architectural approach.

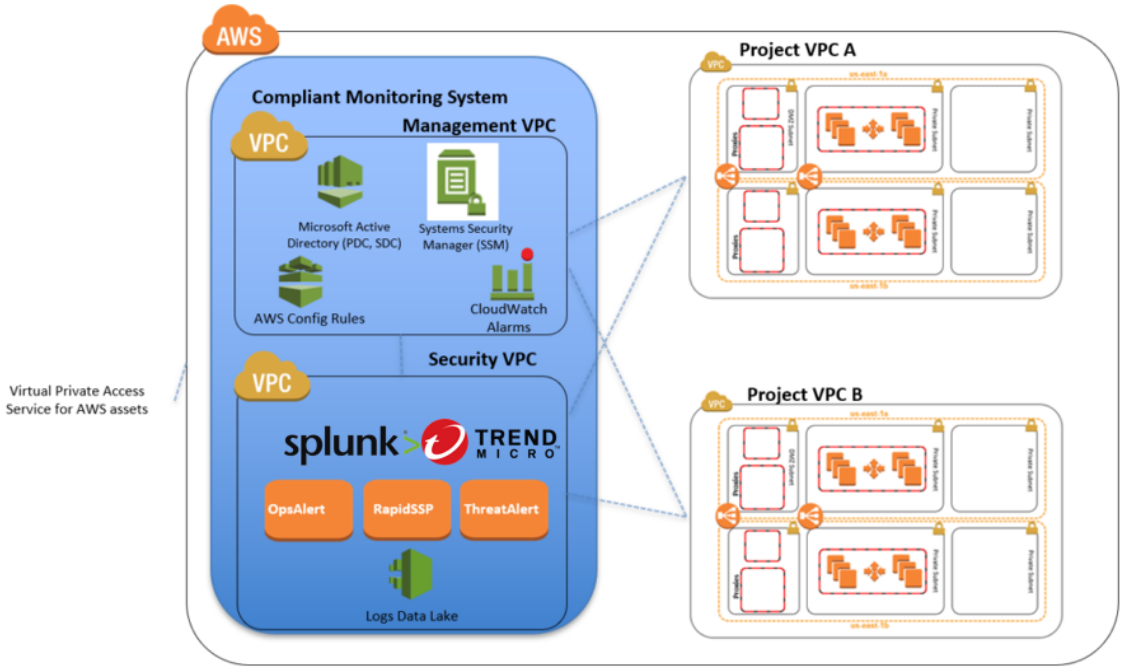

Figure 7: The stackArmor cybersecurity and compliance platform is deployed within the customers' AWS account within a segregated virtual private cloud (VPC).

The in-boundary deployment model helps reduce the complexity of the compliance framework and ensures that the customer controls their operational and security data. The security boundary is not breached and external services are not required to be accredited reducing dependencies.

7. About stackArmor

stackArmor is an Advanced AWS certified provider of Security & Compliance, Cloud migration and management, DevOps enablement, Cloud-native IOT and Data Analytics solutions. As an AWS Authorized Reseller, AWS Public Sector Partner and AWS GovCloud competency holder, stackArmor specializes in delivering secure and compliance-oriented IT solutions to regulated industries including Government, Education, Financial Services, Healthcare, Non-profits and Energy. Our certified experts help protect customers from cyberthreat challenges through systems engineering best practices developed over decades while working with US Federal Agencies requiring compliance with ISO 27001, NIST, FFIEC, FISMA, FedRAMP, DHS and DISA standards. stackArmor is recognized by Amazon Web Services (AWS) for strong Government, Public Sector and Security competencies and was selected as 1 of 10 inaugural launch partners globally for the AWS Security Competency. Our current AWS competencies and service delivery proficiencies as certified by AWS include:

- AWS Advanced Consulting Partner
- AWS Government Competency Partner
- AWS Public Sector Competency Partner
- AWS Security Competency Partner
- AWS GovCloud Competency Partner
- AWS Well Architected Framework Partner
- AWS Microsoft Competency Partner
- AWS Non-Profit Competency Partner
- AWS Government and Commercial Value-Added Reseller (VAR)

Additionally, stackArmor has a strong track record of performance in supporting Commercial, Public sector and US Government customers including but not limited to:

- Whitehouse Office of American Innovation (WHOAI) Cloud Adoption Center of Excellence
- Department of Education
- Department of Transportation
- District of Columbia, Health Benefits Exchange
- District of Columbia, Health Benefits Exchange
- SAP NS2
- General Dynamics
- Siemens Government

Washington DC Office
1775 Tysons Boulevard
5th Floor
Tysons VA 22102
United States of America

Email: solutions@stackarmor.com
Website: www.stackArmor.com

CONNECT WITH US


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


https://twitter.com/stackArmor

stackArmor has deep 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 Federal Agencies requiring compliance with NIST, FFIEC, FISMA, FedRAMP, DHS and DISA.

We enable your company's transition to secure cloud computing through the lifecycle that 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