SOLUTION BRIEF

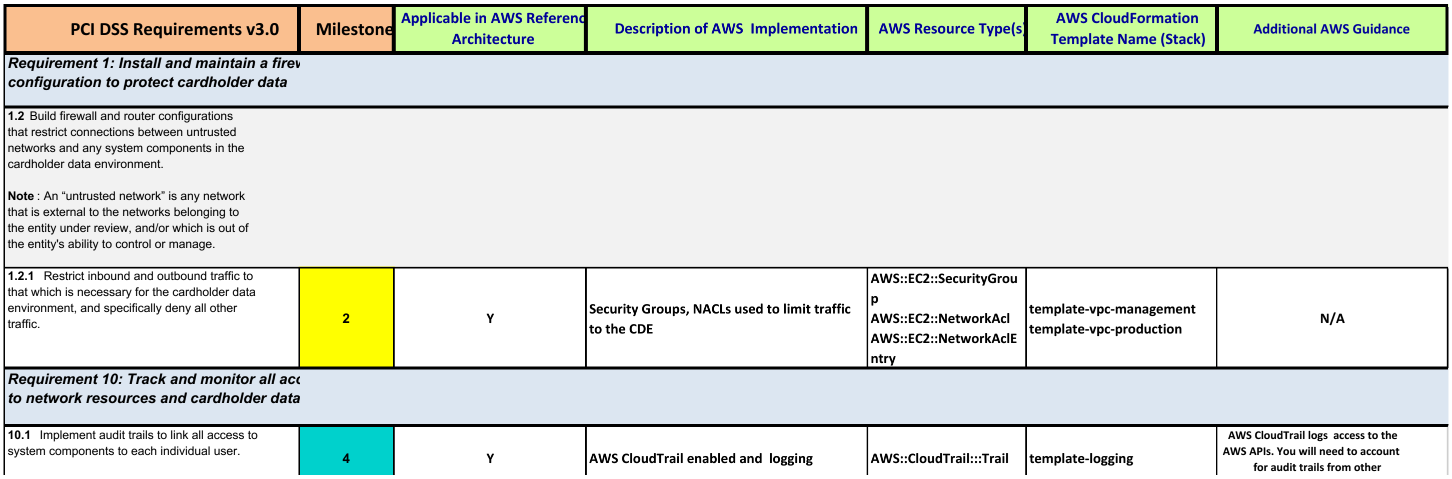
cavirin

CAVIRIN SUPPORT FOR AWS PCI DSS QUICKSTART

Separate from AWS CIS benchmarks and the different regulatory frameworks that apply to both on-premise and cloud, Cavirin is taking a leadership role within AWS by supporting the PCI DSS 3.2 for AWS Quick Start.

QUICKSTART

The Quick Start defines a standardized environment set of artifacts that helps organizations with deploy and operate PCI-compliant workloads on the AWS cloud. It consists of AWS CloudFormation templates, scripts, and spreadsheets that help build standardized environments and verify key security configurations against the PCI controls on a continuous basis. For example, one requirement mandates a firewall at each internet connection and between any DMZ and internal network. Another ensuring that auditing is in place via CloudTrail. The different tests called out consists of a focused subset of the total CIS PCI benchmark. With the requirements in-hand, the organization can easily properly audit their compliance, and if there is a gap, implement the suggested remediation steps.



PCI DSS Requirements v3.0	Milestone	Applicable in AWS Referenc Architecture	Description of AWS Implementation	AWS Resource Type(s)	AWS CloudFormation Template Name (Stack)	Additional AWS Guidance
Requirement 1: Install and maintain a firev configuration to protect cardholder data						
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. **Note** : An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.						
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	2	Y	Security Groups, NACLs used to limit traffic to the CDE	AWS::EC2::SecurityGroup AWS::EC2::NetworkAcl AWS::EC2::NetworkAclEntry	template-vpc-management template-vpc-production	N/A
Requirement 10: Track and monitor all acc to network resources and cardholder data						
10.1 Implement audit trails to link all access to system components to each individual user.	4	Y	AWS CloudTrail enabled and logging	AWS::CloudTrail:::Trail	template-logging	AWS CloudTrail logs access to the AWS APIs. You will need to account for audit trails from other

The Quick Start is part of the AWS Enterprise Accelerator – Compliance Jumpstart offering, providing security-focused, standardized architecture solutions to help Managed Service Organizations (MSOs), cloud provisioning teams, developers, integrators, and information security teams adhere to strict security, compliance, and risk management controls. Advantages include:

- A repeatable approach to compliance via reference architectures that meet stringent enterprise security requirements
- Simplified security accreditation via a Security Controls Matrix
- Detailed documentation that includes templates, tools, and reference diagrams
- AWS workshops covering objectives, requirements, and shared responsibility

SOLUTION

Cavirin’s unique approach to achieve PCI DSS 3.2 security compliance includes a rich set of well curated policies that can be tested automatically, and continuously against the infrastructure built using the Quick Start artifacts. The special Policy Pack targeted against the PCI DSS 3.2 AWS Quick Start requirements is a hybrid composition of Cavirin’s other popular Policy Packs such as the CIS AWS Three-tier benchmark, the CIS AWS Cloud Foundation Policy Pack, the PCI DSS 3.2 Policy Pack for OS security hardening.

With this security content, and the automation around it, any organization can quickly, and without error deploy their PCI workloads within AWS or even within a hybrid environment. Cavirin plans to introduce additional AWS Quick Start support that includes NIST, HIPAA, and others.

Links -

- AWS Enterprise Accelerator for Compliance background
- AWS blog on the PCI DSS Quick Start reference architecture
- Cavirin ‘Cloud Security - Are Your Assets Protected?’ - The shared responsibility model
- Cavirin blog ‘Agility in Security’ talks about CloudFormation and PCI

ABOUT CAVIRIN

Cavirin provides continuous security assessment and remediation across physical, public, and hybrid clouds, supporting AWS, Microsoft Azure, Google Cloud Platform, VMware, KVM, and Docker. The company’s solutions offer continuous visibility, are agentless and multi-tenant, and scale to the largest physical and virtual infrastructures. They offer up-to-the-minute compliance assessments, supplying audit-ready evidence as measured by every major regulatory and security best practice framework including CIS, DISA, PCI and HIPAA. With Cavirin, companies are empowered to make the right decisions faster and de-risk their cloud migrations.

FOR MORE INFORMATION, CONTACT US AT:

CAVIRIN SYSTEMS, INC. | 5201 GREAT AMERICA PKWY SUITE 419 SANTA CLARA, CA 95054 | 1-408-200-3544 | WWW.CAVIRIN.COM