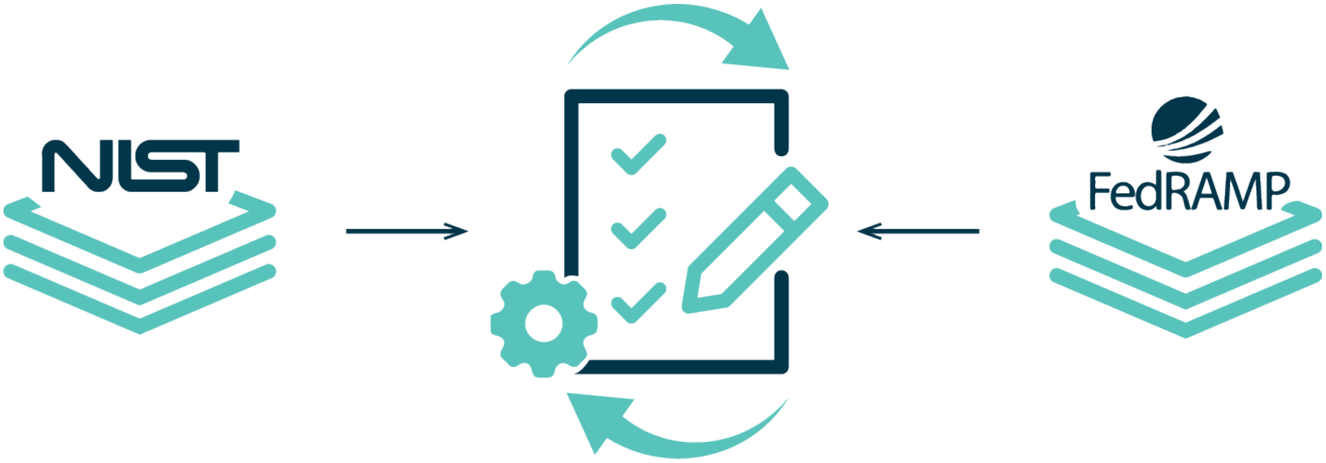
Check Point
SOFTWARE TECHNOLOGIES LTD

COMPLY WITH NIST 800-53 / FEDRAMP STANDARDS USING THE COMPLIANCE ENGINE FROM CLOUDGUARD DOME9

The National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev 4) provides a catalog of security controls for all U.S. federal information systems. These systems must go through a formal assessment and authorization process to ensure sufficient protection of confidentiality, integrity, and availability of information and information systems, based on the security category and impact level of the system (low, moderate, or high), and a risk determination. Since NIST 800-53 is a comprehensive security standard, it is common even for unregulated organizations to use it for guidance, if they have a simple and cost-effective tool they can utilize.



The Compliance Engine from CloudGuard Dome9 ensures continuous compliance automation of federal standards across your cloud accounts with pre-established compliance bundles for NIST 800-53 Rev. 4 and FedRAMP.

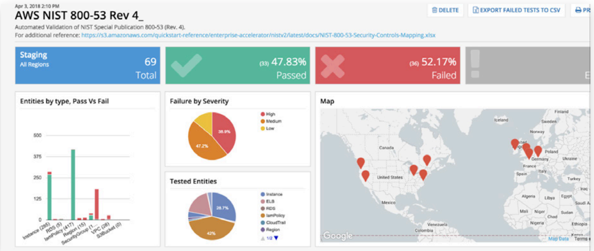
Key Considerations on Managing NIST 800-53 Standards in the Cloud

Most of the NIST SP 800-53 controls can be categorized as being either procedural or technical. Procedural controls are usually policy procedures and process related. Technical controls typically relate to configuration of your cloud environment and should be implemented and assessed using cloud security tools. Design and implementation of technical security and privacy controls in the cloud present some unique challenges that are listed below:

1. **Lack of Visibility** – with hundreds of security groups, projects, entities, instances and accounts across several regions, it is difficult to keep track of security policy configurations and ensure that these policies are being enforced.
2. **Ever Changing Cloud Technology** – legacy on-premise security solutions are not designed to support dynamic cloud infrastructure that is rapidly changing.
3. **Knowledge Gap** – one big cloud computing challenge is lack of specific cloud security knowledge in the DevOps/ Compliance teams.
4. **Large Amounts of Data** – legacy security and compliance tools built to reactively analyze big volumes of data are not designed to visualize cloud activity or configurational data.
5. **Remediation is a Pain** – complex cloud architecture makes it difficult to remediate known issues immediately when discovered.

The Compliance Engine from CloudGuard Dome9 Provides Comprehensive Compliance

The Compliance Engine from CloudGuard Dome9 provides an automation framework that allows customers to automatically assess their cloud environments against regulatory standards and security best practices. You can use the pre-packaged CloudGuard Dome9 NIST 800-53 / FedRAMP compliance bundle to accelerate your checks for recommended security controls in helping federal agencies ensure compliance with other regulations. Additionally you can easily create your own test bundle that captures your organization's unique requirements using CloudGuard Dome9's concise Governance Specification Language (GSL).



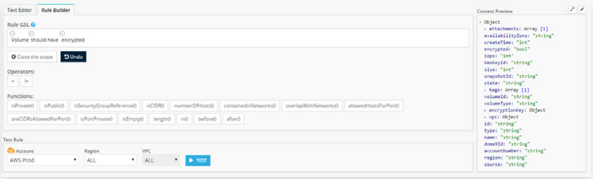
Apr 3, 2018 2:10 PM

AWS NIST 800-53 Rev 4_

Automated Validation of NIST Special Publication 800-53 (Rev. 4).

For additional reference: https://s3.amazonaws.com/quickstart-reference/enterprise-accelerator/nistv2/latest/docs/NIST-800-53-Security-Controls-Mapping.xlsx

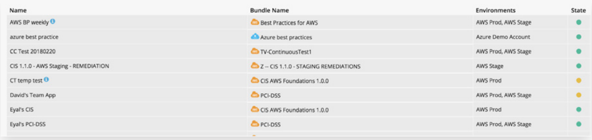
Staging All Regions 69 Total | (33) 47.83% Passed | (36) 52.17% Failed



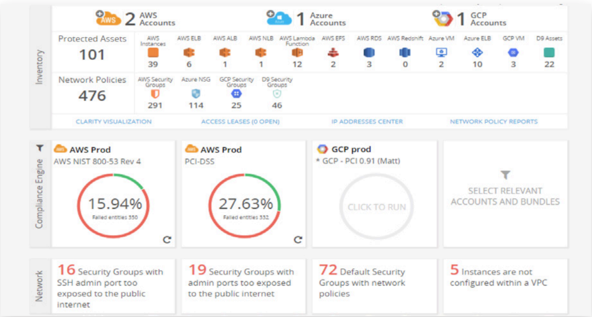
Volume should have encrypted

Account: AWS Prod | Region: ALL | VPC: ALL

```
Object
  attachments: Array [1]
  availabilityZone: "string"
  createTime: "int"
  encrypted: "bool"
  iops: "int"
  kmsKeyId: "string"
  size: "int"
  snapshotId: "string"
  state: "string"
  tags: Array [1]
  volumeId: "string"
  volumeType: "string"
  encryptionKey: Object
  vpc: Object
  id: "string"
  type: "string"
  name: "string"
  dome9Id: "string"
  accountNumber: "string"
  region: "string"
  source: "string"
```



Name	Bundle Name	Environments	State
AWS BP weekly	Best Practices for AWS	AWS Prod, AWS Stage	●
azure best practice	Azure best practices	Azure Demo Account	●
CC Test 20180220	TV-ContinuousTest1	AWS Prod, AWS Stage	●
CIS 1.1.0 - AWS Staging - REMEDIATION	Z -- CIS 1.1.0 - STAGING REMEDIATIONS	AWS Stage	●
CT temp test	CIS AWS Foundations 1.0.0	AWS Prod	●
David's Team App	PCI-DSS	AWS Prod, AWS Stage	●
Eyal's CIS	CIS AWS Foundations 1.0.0	AWS Prod	●
Eyal's PCI-DSS	PCI-DSS	AWS Prod, AWS Stage	●



16 Security Groups with SSH admin port too exposed to the public internet

19 Security Groups with admin ports too exposed to the public internet

72 Default Security Groups with network policies

5 Instances are not configured within a VPC

KEY BENEFITS

Compliance Engine. Real-time view of compliance and security posture for immediate risk mitigation. Use CloudGuard Dome9 compliance and best practices test suites such as HIPAA, PCI DSS, GDPR, CIS AWS Foundations Benchmark to quickly check your environment against these regulations and implement changes as needed.

Governance Specification Language (GSL) allows Compliance and Security teams to write and review any compliance checks easily without deep technical knowledge. This equates to fewer errors in translating regulatory and governance requirements to policy definitions for a faster time-to-compliance.

Continuous Compliance. Continuous Compliance allows CloudGuard Dome9 clients to automate and continuously run compliance assessment reports according to various compliance suites and deliver findings through the most convenient method such as email, SNS notification message or a PDF report.

Live Dashboard. Receive a compliance score that indicates where entities have passed or failed. Prescribed remediation can easily be done for each non-compliant entity using Cloud-Supervisor2.

CloudGuard Dome9 provides AWS NIST 800-53 Rev. 4 / FedRAMP standards assistance for the following federal security controls:

Security controls are selected from the NIST SP 800-53 Security Control Catalog, and the system is assessed against those security control requirements.The controls selected are based on the security category and impact level of the system (low, moderate, or high), and a risk determination. Below is the coverage CloudGuard Dome9 provides for AWS and each impact level of NIST 800-53 as well as FedRAMP requirements*:

	LOW	MODERATE	HIGH
CONTROLS	116	150	171
CLOUDGUARD DOME9 COVERAGE	41%	30%	28%

*Does not include non-applicable controls such as physical security, etc.

CONTACT US

Check Point Software Technologies Ltd.
959 Skyway Road, Suite 300
San Carlos, CA 94070
USA +1-800-429-4391
www.checkpoint.com

For a free security assessment or trial, please contact:
US Sales: +1-866-488-6691
International Sales: +44-203-608-7492