cavirin

SOLUTION BRIEF

Closed-Loop Security Delivers Cybersecurity Posture Management for AWS

Cavirin's continuous protection, monitoring, and remediation, across hybrid infrastructures, automates compliance and secures organizations from possible cyberattacks. Powered by Cavirin's patent pending machine learning technology, our CyberPosture Intelligence provides users with the most accurate credit-like scoring view of their security posture, so they can make informative decisions when protecting their organization.

Cavirin's solution for AWS offers customers single-pane visibility into CyberPosture scoring and management for AWS services and resources. The CyberPosture score immediately alerts SecOps of top security issues that require attention due to the addition of new resources or configuration changes. A list of prioritized issues facilitates AWS Lambda Functions auto-remediation to bring the score back to the organization's 'golden posture'. CISOs can continually assess risk trends across their AWS or hybrid infrastructure, while Chief Compliance or Risk Officers can ensure audit-readiness.

Cavirin's up-to-the minute compliance and risk analysis supplies audit-ready evidence to comply with every major regulatory and security best practice framework and guideline (including CIS, NIST, DISA, GDPR, SOC, PCI, and HIPAA). Plus, our customizable policy framework provides flexibility for enterprises so users can craft their own combinations of benchmarks and set risk levels, to accommodate various compliance and security requirements.

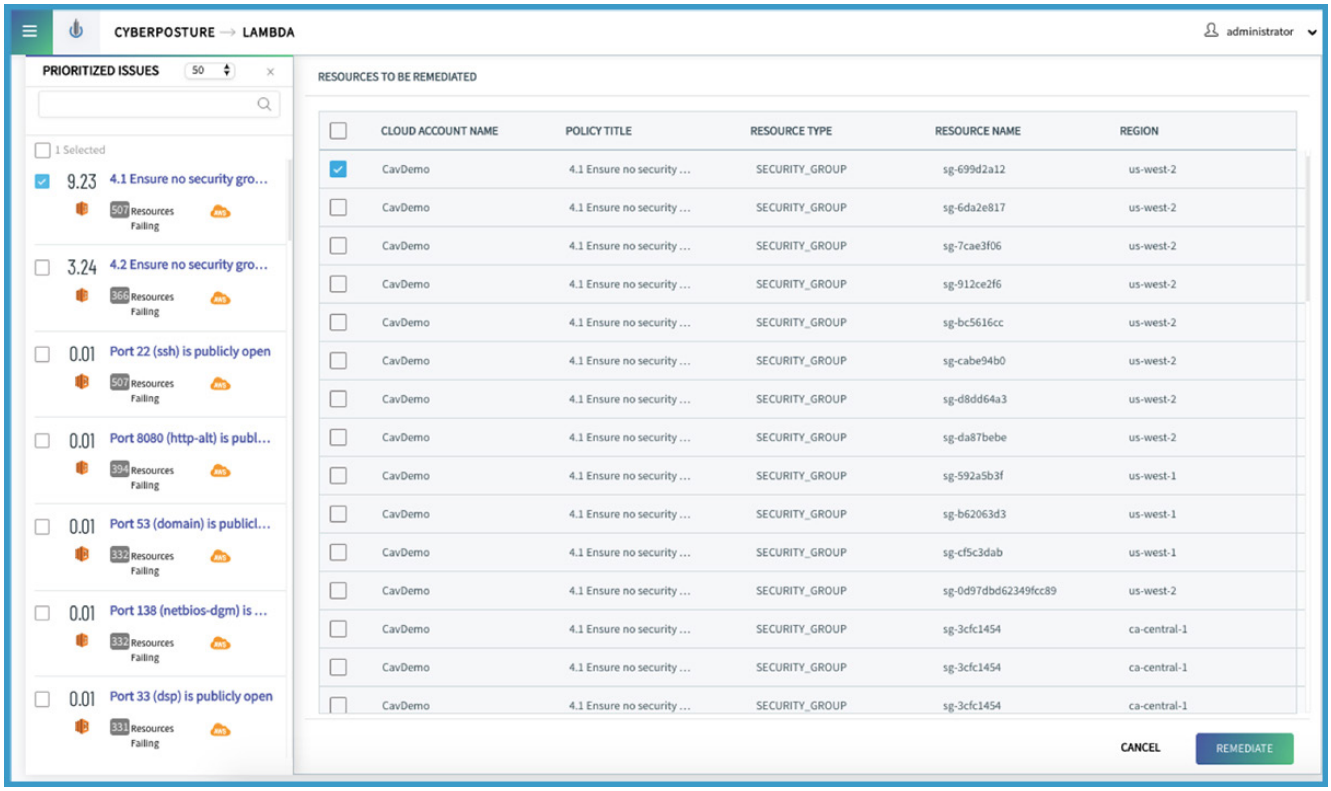
UNSURPASSED AWS VISIBILITY & CONTROL

- Visibility into AWS services and resources including Cloud Accounts, Compute Instances, Compute Images, Virtual Networks, Subnets, NAT Gateways, DNS, Audit Logs, Cloud Monitor, AutoScaling, PubSub, KMS, SSL and IAM Certificates, Security Groups, Classic and Application Load Balancers, CDN, Block Store, Object Store, and Databases. Additional services will follow in subsequent releases.
- Support for the CIS AWS Foundations Benchmark, the Cavirin AWS Web Applications Policy Pack, derived from the CIS AWS Three-tier Web Architecture Benchmark, as well as the Cavirin AWS Network Policy Pack that covers 522 of the most important TCP ports. These are a set of best-practices to establish a security posture baseline. Additional AWS-specific packs include the HIPAA and PCI DSS 3.2 QuickStarts.
- Discovery of and visibility into AWS workloads, both VM and container. The solution assesses and then scores these against a broad set of controls, including the NIST CSF, CIS, SOC2, PCI, HIPAA, and GDPR. All major OSs are supported, including Amazon Linux 2.
- Integration to AWS CloudTrail activity logs to detect new or changed resources, including RDS Keys SSL and IAM Certificates, Audit Logs, CloudWatch, SNS, and IAM. Set thresholds to be notified of potential security gaps.
- Simple operator workflow with powerful insights.
- Execute auto-remediation via Ansible Playbooks for workloads and AWS Lambda Functions for cloud services to remove identified security gaps.

95+% **CLOUD SECURITY FAILURES THROUGH 2022**
GARTNER PREDICTS WILL BE THE CUSTOMER'S FAULT.

Typical Operator Workflow

- Select cloud and host accounts via AWS integration wizards.
- Discover and assessment wizard for quick selection of AWS asset groups, control families to test or suppress, and creation of timed assessments with notifications.
- Create asset groups based on operator selections, for assessments.
- Identify monitored services that exceed configured thresholds and may be vulnerable.
- Search within resources database for more detailed analysis of AWS services.
- View CyberPosture score of security and compliance across the AWS environment, including pass/fails, trending, and top prioritized issues for remediation to a desired 'golden posture'.
- Plan for target CyberPosture and generate guidance report.
- Analyze CyberPosture via reports (xls, csv, pdf) that detail asset type, controls, & remediation guidance.
- Execute auto-remediation via Ansible Playbooks or AWS Lambda Functions.
- Activate monitoring of AWS services.



About Cavirin

Cavirin, headquartered in Santa Clara, Calif., is a privately-held, global provider of risk, cybersecurity, and compliance posture intelligence for the hybrid cloud. Founded in 2012, Cavirin's continuous protection, monitoring, and remediation, across hybrid infrastructure, automates compliance and secures organizations from possible cyberattacks. Powered by Cavirin's patent pending machine learning technology, our CyberPosture Intelligence, provides users the most accurate credit-like scoring view of their security posture, so they can make informative decisions when protecting their organization.

Find us on the AWS Marketplace, https://aws.amazon.com/marketplace/cavirin