The First Line of Defense for Hybrid Cloud Security

Identify, Proactively Monitor, and fix Cloud Misconfigurations

Introduction

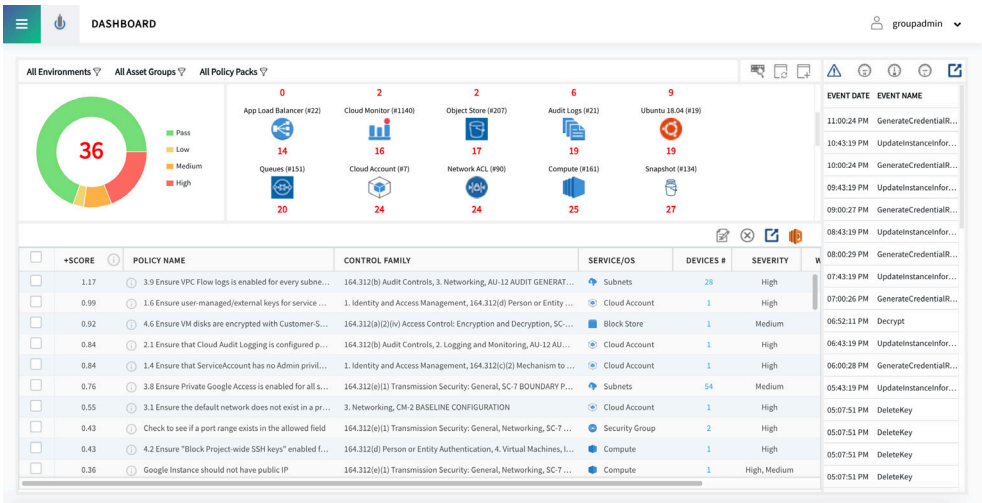
In today's world, where a data breach seems like a daily event, employing effective cybersecurity is critical. While cloud-based systems offer rapid development and instant scalability, the risk of unintentionally growing the attack surface on those systems increases significantly.

The key to managing your cloud security starts with identifying vulnerabilities and continues with rapid remediation. A critical first step to securing your cloud is to ensure proper configurations and standards compliance of your critical infrastructure and access management services.

Cavirin's solution offers real-time monitoring, threat detection, and auto-remediation across AWS, GCP, Azure, On-premises, OS, containers, and Kubernetes.

Cavirin's version 5 debuts a new interactive CISO dashboard that provides a detailed view of various components in both Cloud and On-premises environments. This new dashboard brings to the fore the cyber posture of your systems by delivering a score that reflects critical vulnerabilities.

Remediation of identified security and compliance issues can now be launched directly from the dashboard's home screen. The system is fully integrated with Slack, Pager Duty, Jira, and Service Now.



Also new in Version 5

- **Multi-tenant SaaS**
- **Real-time alert notifications**
- **Resource Whitelisting**

Use Cases

Secure Cloud

Single misconfigurations of cloud data resources have led to massive breaches in the past few years. Don't leave gaping holes in your cloud assets; lock down your critical assets by ensuring the correct baseline.

Secure Compute

Assess computing systems consisting of host machines, Docker engine, Docker images, and Kubernetes orchestrator with Cavirin-authored and industry-led configuration checks.

Cloud Compliance

Provide technical evidence to your auditors to make passing audits head-ache free

Accelerate your cloud compliance. Cavirin provides out-of-the-box policies for HIPAA, PCI, AICPA SOC2, GDPR, and more.

Cyberposture Intelligence for Continuous Cloud Security

Advanced cloud security with one-click policies, cloud monitoring, automated remediation, threat detection, and enterprise integrations Security does not end with configurations.

The end goal is continuous health checks, monitoring, threat detection, and automated remediation.

Features

Broad policy coverage across clouds, OS, containers, and Kubernetes: Cavirin offers the most comprehensive set of out-of-box policies for AWS, GCP, and Azure. Cloud security & compliance is incomplete without coverage for compute instances, operating systems, and containers. Cavirin offers extensive coverage of compliance & vulnerabilities for operating systems and containers. It also has policies for Kubernetes.

All-inclusive security standards and compliance coverage: Security policies across your infrastructure form the basis for compliance to industry standards benchmarks. Cavirin offers out-of-box support for a wide range of industry-standard security and compliance benchmarks, including NIST, HIPAA, PCI, SOC2, GDPR, and ISO.

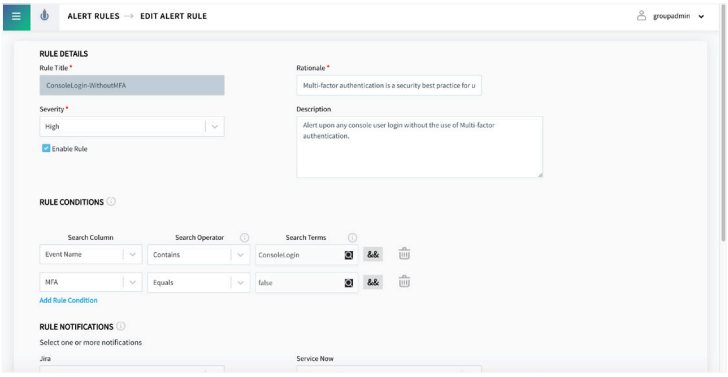
Actionable reports: Top issues reports and remediation reports provide a prioritized and actionable path for your administrators to fix these findings. Resource reports provide documented evidence to serve your compliance needs. Delta reports provide changes since the last assessment.

Cyberposture scoring: Cyberposture scoring provides you a score between 0 and 100 that highlights risk areas and empowers prioritized response plans. A score is computed for each resource based on the weights and severity of the failed policies. Cavirin has used the industry-standard NIST definition for score calculation and applied machine learning to derive weights for policies. An asset group score is calculated using the weighted average of the resource scores.

Discovery & assessment: Cavirin has built a high-performance and scalable architecture to discover & assess cloud services using cloud APIs in bulk. With this architecture, assessments finish fast without consuming a lot of network bandwidth. OS scanning is done without using any agents and supports bastion host and proxy server for instances that are not directly accessible from Cavirin instance.

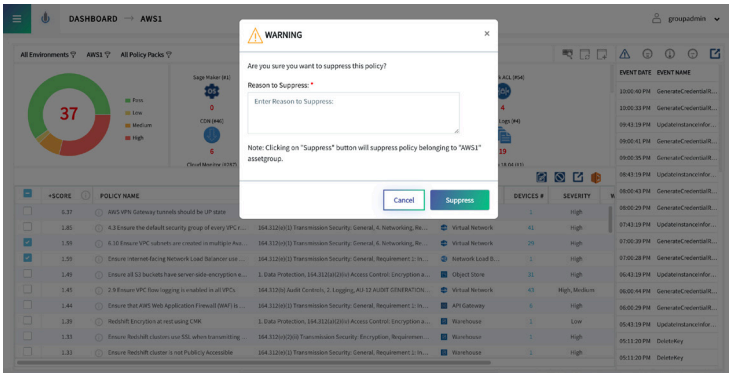
Proactive monitoring: Cavirin proactively monitors AWS CloudTrail, Google StackDriver, and Azure Audit logs to detect policy failures as changes are happening in your environment. After reaching a defined threshold for cloud resources, a full assessment is triggered automatically to ensure that you remain on top of your Cybersecurity Posture at all times.

Real-time alert notifications: The ability to focus on critical events by defining rules that initiate notifications through third-party apps and email integration.



Configurable and Custom Policies: Configurable policies allow you to ensure compliance with your secure standards & configurations (e.g., for your security, encryption, administrative settings). Custom policies offer an easy way to add custom policies in the system. Policy suppression allows deactivation of policies not relevant for your organization or a specific asset group.

Resource whitelisting: Delivers flexibility for the user, offering granular control over resource suppression to ensure the cyber posture score is reflecting the correct resources.



Threat detection integration: Cavirin integrates with many cloud provider's threat detection capabilities (e.g., AWS GuardRail). Threat detection allows customers to prioritize and address gaps in the environment more effectively. For the Operating System, Cavirin is integrated with the national exploits database to identify and prioritize known exploits.

DevOps friendly API first architecture: Cavirin offers DevOps friendly API first architecture that allows for easy integration into the DevOps pipeline. Our Jenkins integration enables you to assess containers before deployment into your CI/CD pipeline.

Enterprise Integration: Cavirin is integrated with ServiceNow and JIRA to open tickets and Slack and PagerDuty to send notifications. Additionally, we integrate with Splunk, SIEM, Google Security Command Center (GSCC), and RSA Archer.

Fast & Easy deployment: Cavirin delivers fast & easy deployment from across multiple platforms:

- Cloud marketplaces (AWS, Azure, and GCP)
- Offers OVA for on-premise deployments
- Multi-tenant SaaS environment that supports hybrid workloads across Public Clouds/Private Clouds or On-premises.

Cavirin offers agentless Discovery and OS assessments and implements cloud provider APIs to ensure fully comprehensive assessments.

Specifications

Control Frameworks (Cloud)

- CIS Foundation Benchmark for AWS, Azure, and GCP.
- Cavirin-authored AWS, Azure, and GCP policy pack designed with security best practices for cloud.
  - Configurable AWS, Azure, and GCP policy packs
  - Identity, access, and authorization policies
  - Networking boundaries
  - Security baseline
  - Data protection
- 1300+ AWS policies covering 30+ top AWS cloud services including but not limited to:
  - IAM Identity and Access Management
  - EC2 (Elastic Compute Cloud)
  - S3 (Simple Storage Service)
  - EBS (Elastic Block Store)
  - RDS (Relational Database Service)
  - EFS (Elastic File Store)
  - DynamoDB
  - SNS (Simple Notification Service)
  - SQS (Simple Queue Service)
  - Elastic Search
  - RedShift
  - CloudTrail
  - Lambda
  - ECR (Elastic Container Registry)
  - Kinesis
  - Snapshots
  - IAM Certificates
  - KMS (Key Management Service)
  - ACM Certificates
  - CloudWatch
  - AWS Config
  - VPC (Virtual Private Cloud)
  - Security Groups
  - Network ACL
  - Route 53
  - Auto-Scaling
  - Subnet
  - NAT Gateway
  - CloudFront
  - ELB (Elastic Load Balancing)
- 550 + Azure policies covering top seven services including:
  - Security Center
  - Storage Accounts
  - Logging and Monitoring
  - Networking
  - Virtual Machines
  - Service Bus
  - Azure Functions
  - Security Baselines
- 550+ Google Cloud policies covering top seven services including:
  - IAM (Identity and Access Management)
  - Logging and Monitoring
  - Networking
  - Virtual Machines
  - Storage buckets
  - Cloud SQL Database Services
  - Kubernetes
- AWS, Azure, and Google Network Policy Packs: 520 common ports For Containers

Container Security

- Cavirin Docker Image Hardening Policy Pack

Security (OS Level)

- NIST 800-53 R4 Policy Pack
- NIST 800-171 Policy Pack
- NIST Cybersecurity Framework Policy Pack
- CIS 7 Policy Pack
- DISA Policy Pack
- Cavirin Patches & Vulnerabilities Policy Pack
- Cavirin Operating System Exploits Policy Pack
- CIS Policy Pack for Database
- GuardDuty Threat Policy Pack

Compliance (OS Level)

- ISO 27002:2013 Policy Pack
- AICPA SOC 2 Type II Policy Pack
- PCI DSS 3.2 AWS Policy Pack
- HIPAA AWS Policy Pack
- CJIS Policy Pack
- GDPR Policy Pack

Cloud Frameworks (AWS/Azure/GCP)

- CIS Cloud Policy Pack
- NIST 800-53r4 Policy Pack
- HIPPA Policy Pack
- PCI DSS 3.2 Policy Pack
- Cavirin Web Application Policy Pack
- Configurable Security Policy Pack
- Network Policy pack

AWS Monitoring

- S3
- RDS
- EBS
- Instance Images
- Security Groups
- Classic Load Balancer
- Amazon Application Load Balancer
- VPC (Virtual Private Cloud)
- KMS
- CDN (Content Delivery Network)
- IAM
- CloudTrail
- SNS
- Amazon Auto-Scaling Groups
- CloudWatch
- SSL Certificates
- IAM Certificates

AWS Auto-Remediation

- Security Group
- IAM
- S3
- Cloud Trail
- Lambda
- KMS
- RDS

Google Cloud Monitoring

- Compute Engine Firewall Rules
- Subnets
- Cloud Virtual Networks
- Compute Engine
- Google Kubernetes Engine
- Cloud SQL
- Projects
- Key Ring
- StackDriver Monitoring

Google Cloud Auto-Remediation

- Firewall Rules
- IAM
- Virtual Network,
- Subnet
- Instance
- Cloud SQL
- GKE (Google Kubernetes Engine)

Azure Monitoring

- Storage Accounts
- Key vaults
- Virtual Machines
- Network security groups,
- Log profiles
- Activity Log

Azure Auto-Remediation

- Network Security Group, Storage
- Account, Security Center.

Operating System Based Policy Packs

- Amazon Linux and AWS Linux 2
- Ubuntu (14.04, 16.04, 18.04)
- Debian 7, 8, 9
- CentOS 6, 7 & 8
- RedHat Linux 6, 7 & 8, Japanese
- SUSE Linux 11, 12
- Windows 7, 8, 10,
- Windows Server 2008, 2012, 2012R2, 2016

Integrations

- JIRA
- Service Now
- PagerDuty
- Slack
- Google Cloud Security Command Center

Deployment Options and Details

- For deployments in VMware and KVM, use Cavirin's OVA format
- Launch Cavirin from AWS, and Google Cloud Marketplaces
- Create custom deployments in AWS, or GCP using AMI/VHD formats or use the Cavirin installer
- Create custom deployment in Azure using the Cavirin Installer
- XLS and PDF reports include both device and remediation including delta reports (the change in posture between two assessments).
- Support for proxy servers, bastion hosts, custom ports, SSO, and role-based access (RBAC)

About Cavirin

Cavirin delivers an Enterprise-Class Cyber Security framework that presents up-to-the-minute knowledge of system-wide security strengths and weaknesses. Whether in the cloud, or the corporate data center, our agentless CyberPosture Intelligence solution enables cross-platform security monitoring, reporting, remediation, and compliance. Our focus is to provide concise views into the security framework of Enterprise systems to empower CSIOs and their teams to respond to threats rapidly and decisively.

Cavirin Systems, Inc.
5201 Great America Pkwy, Suite 419, Santa Clara
CA 95054
sales@cavirin.com
www.cavirin.com