The First Line of Defense for the Hybrid Cloud

Dynamically Identify, Proactively Monitor, and Fix Cloud Misconfigurations

Introduction

Cloud-based systems provide rapid development and scalability benefits, yet they are more susceptible to attacks. It is essential to maintain continuous monitoring and remediation practices to enhance security. Cavirin offers agentless Discovery, OS assessments, and AI-driven security solutions for ongoing monitoring and early threat identification on the following platforms.

- Amazon Web Services (AWS)
- Google Cloud Platform
- Microsoft Azure
- Oracle Cloud
- On-premise Data Centers
- OS containers
- Kubernetes
- Networking equipment

This is made possible through up-to-date standards-based policies and threat data, facilitating prompt threat detection and automated remediation.

Cavirin's solution features a CISO dashboard for both Cloud and On-premise environments. It provides an in-depth look at the Cyber Posture of cloud-based systems, identifies crucial vulnerabilities, and offers tools for rapid remediation.

Remediation of security and compliance issues can be launched directly from the Dashboard's home screen. Slack, Pager Duty, Jira, and ServiceNow are fully supported by the system.

AI Powered Cyber Posture Intelligence

AI technology for posture management offers predictive posture scoring by analyzing historical data and current trends. Through examining patterns in hybrid cloud infrastructure alterations, the AI system functions as an early warning system, forecasting posture score trends up to 180 days ahead.

The predictive score trend forecasts the potential percentage deviation from the current trend, signaling both positive and negative changes in frequently utilized policy packs, including CIS, NIST, PCI, and HIPAA.

Use Cases

Secure Cloud

- Misconfigurations in cloud data resources have resulted in significant breaches in recent years. To prevent vulnerabilities in your cloud assets, secure your critical resources by establishing the proper baseline.

Secure Compute

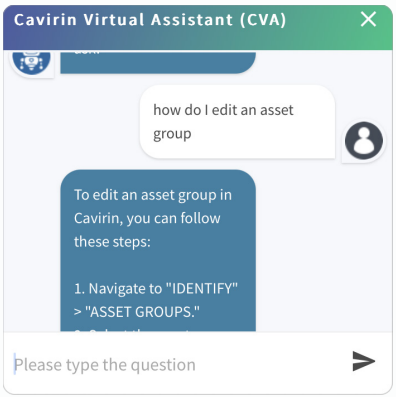
- Evaluate computing systems that include host machines, Docker engine, Docker images, and Kubernetes orchestrator by utilizing Cavirin-developed configuration checks, guided by industry standards.

Cloud Compliance

- Offer technical evidence to your auditors for smoother audit clearance.
- Speed up your cloud compliance process with pre-defined policies for HIPAA, PCI, AICPA SOC2, GDPR, and more.

AI Powered Chatbot

The new GenAI-powered Cavirin Virtual Agent (CVA) provides intelligent support for users. This chatbot enables users to ask questions in plain language, offers comprehensive system assistance, and acts as a substitute for user manuals, and reduces the learning curve for operators.



Network Device Support

In our most recent update, we have introduced network device support. This feature aims to assess the vulnerability of network device operating systems. Initially, we have incorporated support for Cisco Firepower Series and Cisco Meraki Series Devices. Expect future updates to expand this list to include more networking products.

Features

Remediation Policy Correlation Alerts: Specify which policies are impacted by the findings and the potential percentage improvement in posture through addressing these policies.

AWS Baseline: Cavirin's security and compliance solution provides users with detailed system vulnerability information, while CSIOs benefit from a comprehensive overview of threats and strengths in the AWS environment through the AWS Baseline report.

Terraform Automation for AWS Cloud Policies: Terraform is an open-source tool for managing cloud services efficiently through declarative configuration files. It automates policy execution and integrates predefined policies like CIS benchmarks to scan cloud services via APIs.

Lightweight OS Container Pods: allow quick OS Container scans, reducing network bandwidth. They facilitate efficient resource discovery and assessment across various platforms.

AWS Security Hub and Inspector 2.0 Integration: SAWS Security Hub users can benefit from the Cavirin dashboard, which merges policy-based discoveries with Amazon Inspector vulnerability findings (CVEs) to provide organized and actionable results for remediation.

Comprehensive Security Standards and Compliance Coverage:

- Security policies throughout your infrastructure are essential for meeting industry-standard benchmarks for compliance.
- Cavirin provides pre-configured support for various industry-standard security and compliance benchmarks such as NIST, HIPAA, PCI, SOC2, GDPR, and ISO.
- Moreover, Cavirin's solution is linked with the national exploits database to detect and report known exploits in operating systems.

Actionable reports: Prioritized top issues and remediation reports offer a clear path for your administrators to address these issues. Resource reports offer documented evidence for your compliance needs. Delta reports show the differences from the previous evaluation.

Cyber posture scoring: assigns a score from 0 to 100, focusing on risk areas for targeted responses. Scores are based on resource importance and policy violations seriousness, using NIST standards and machine learning for weight assignment. Asset group scores are calculated by averaging individual resource scores with relevant weights.

Kubernetes Content: Classification and aggregation of Kubernetes related policies across all cloud platforms.

Network Device Vulnerability Assessment Scans networking equipment to highlight vulnerabilities in the device OS.

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

Configurable Policies: Configurable policies allow you to ensure compliance with your security standards & configurations (e.g., security, encryption, administrative settings).

Custom Policies: offer an easy way to add custom policies to the system. Policy suppression allows the deactivation of policies not relevant to 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 reflects the correct resources.

Integration with the NIST national exploits database: Cavirin's solution is integrated with the national exploits database to identify and prioritize known exploits in operating systems.

Enterprise Integration: Cavirin is linked with ServiceNow and JIRA for ticket creation, as well as with Slack and PagerDuty for notifications. Moreover, our integration extends to Splunk, SIEM, Google Security Command Center (GSCC), and RSA Archer.

Cavirin's API-first architecture: is DevOps-friendly, and facilitates seamless integration into the DevOps pipeline. With our Jenkins integration, you can evaluate containers prior to deploying them in your CI/CD pipeline.

Features

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
  - AmazonElastiCache
  - AWSBackup
  - EBS
  - AmazonElastiSearch
  - WAF- WebApplicationFirewall
  - Kinesis Data Firehose
  - AmazonFSx
  - AmazonCloudWatchLogs
  - AmazonInspector
  - AmazonManagedStreaming forApacheKafka
  - AWSOrganizations
  - AmazonDocumentDB
  - AmazonDataLifecycleManager1
  - AWSDatabaseMigrationService
  - AmazonAthena
  - AmazonAccessAnalyzer
  - AWSElasticBeanstalk
  - AWSGlue
  - AmazonNeptune
  - AWSShield
  - AmazonWorkSpaces
  - AWSX-Ray
- 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 Baseline Policies

- Data Protection
  - Data at rest
  - Data in Transit
  - Customer Key Management
- Logging and Monitoring
- Network Boundaries
- IAM

Monitoring and Remediation

AWS	Google Cloud	Microsoft Azure	Oracle Cloud
S3	Compute Engine Firewall Rules	Storage Accounts	Account
RDS	Subnets	Key vaults	IAM
EBS	Cloud Virtual Networks	Virtual Machines	Object storage
Instance Images	Compute Engine	Network security groups,	File storage
Security Groups	Google Kubernetes Engine	Log profiles	Block volumes
Classic Load Balancer	Cloud SQL	Activity Log	Logging
Amazon Application Load Balancer	Projects	Azure Auto-Remediation	Compute
VPC (Virtual Private Cloud)	Key Ring	Network Security Group, Storage	security groups
KMS	StackDriver Monitoring	Account, Security Center.	Keys
CDN (Content Delivery Network)	Google Cloud Auto-Remediation		
IAM	Firewall Rules		
CloudTrail	IAM		
SNS	Virtual Network,		
Amazon Auto-Scaling Groups	Subnet		
CloudWatch	Instance		
SSL Certificates	Cloud SQL		
IAM Certificates	GKE (Google Kubernetes Engine)		
AWS Auto-Remediation			
Security Group			
IAM			
S3			
Cloud Trail			
Lambda			
KMS			
RDS			

Operating System Based Policy Packs

- Amazon Linux and AWS Linux 2
- Ubuntu (14.04, 16.04, 18.04, 18.04 Pro, 20.04)
- 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
- ServiceNow
- PagerDuty
- Slack
- Google Cloud Security Command Center

Cavirin SaaS

- In addition to the installation options below, Cavirin's solution is delivered as a fully functional multi-tenant SaaS solution.

Deployment Options and Details

- For deployments in VMware and KVM, use Cavirin's OVA format
- Launch Cavirin from AWS, Google Cloud, and Oracle Cloud Marketplaces

About Cavirin

Cavirin offers an Enterprise-Class Cyber Security framework that provides real-time insights into the overall security status of systems. Whether it's in the cloud or the corporate data center, our agentless CyberPosture Intelligence solution allows for cross-platform security monitoring, reporting, remediation, and compliance. Our aim is to offer clear insights into the security framework of Enterprise systems, empowering CSIOs and their teams to quickly and effectively address threats.

Cavirin Systems, Inc.
2114 Ringwood Ave
San Jose, CA 95131
USA.
sales@cavirin.com
www.cavirin.com