The First Line of Defense for Cloud Security

Identify, Proactive Monitor, and fix your Cloud Misconfigurations

Introduction

Security starts with building a moat for your IT assets. But what is a “moat” in the context of cloud computing? Traditional, on-prem security focused on “locking down” the perimeter. However, resources in the cloud are consumed as-a-software-service, accessible by cloud APIs, across multiple clouds over the public internet. There is no physical boundary in your control.

Security in the cloud requires a complete mind-shift. Without a physical perimeter, each software service itself must be “locked down.” Therefore, the first step in securing your cloud is to ensure proper configurations of your critical infrastructure (compute, data, and network), platform (databases) and access management services (identity access cloud services) to protect against exploitable vulnerabilities, e.g., access management, encryption (at rest and in transit), network ports, and database services.

What should the configurations be for each of these services, across different clouds? How do you go about determining the 1000s of configurations, across 100s of services, across multiple clouds? It’s a daunting task, and there is no one prescriptive answer to import into your CI scripts.

Cavirin’s expertise is cloud-native security. We are the leaders in developing cloud configuration policies based on industry best practices. Cavirin has built and co-authored the most comprehensive policy packs for foundational IaaS (storage, compute, network services, e.g., S3, EC2, VPCs, security groups, etc.), PaaS (e.g., IAM, databases), and compute (OSs and containers) services across all 3 major clouds – AWS, GCP, and Azure.

Customers use our “one-click” configuration assessments to start their cloud journey and continue with Cavirin’s Cyberposture Intelligence - delivering continuous IT health checks through real-time monitoring, threat detection, and auto-remediation.

Use Cases

Secure Cloud:

Build your first line of defense for cloud security

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:

Build your first line of defense for all your workloads (OS or containers) across your hybrid environments

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

Broadest policy coverage across clouds, OS, containers, and Kubernetes: Cavirin offers the broadest set of out-of-box policies for AWS cloud services, for GCP cloud services and Azure. Cloud security & compliance is incomplete without coverage for compute instances (& operating systems) and containers; Cavirin offers comprehensive coverage of compliance & vulnerabilities for operating systems and containers. It also has policies for Kubernetes. With such broad coverage, you can be assured that you have your cloud infrastructure in safe hands.

Broad security standards and compliance coverage: Security policies across your infrastructure forms the basis for the compliance to industry standards benchmarks. Cavirin offers out-of-box support for a wide range of industry standards security and compliance benchmarks including NIST, HIPAA, PCI, SOC2, GDPR, ISO, and so on. Mapping of security policies to these benchmarks was done via human-assisted machine learning.

Configurable and Custom Policies: Configurable policies allows 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 be relevant for your organization or a specific asset group.

Actionable reports: Once you find gaps, it is even more important to have a plan to act on these findings. 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: In the dynamic cloud world, it is important to know where you stand and how you are improving or impairing on day-to-day basis. Cyberposture scoring provides you a score between 0 and 100, facilitates prioritized response plans so you can make informed decisions to protect against Cyberthreats. A score is computed for each resource based on weights & severity of the failed policies. Cavirin has used industry-standard NIST definition for score calculator 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.

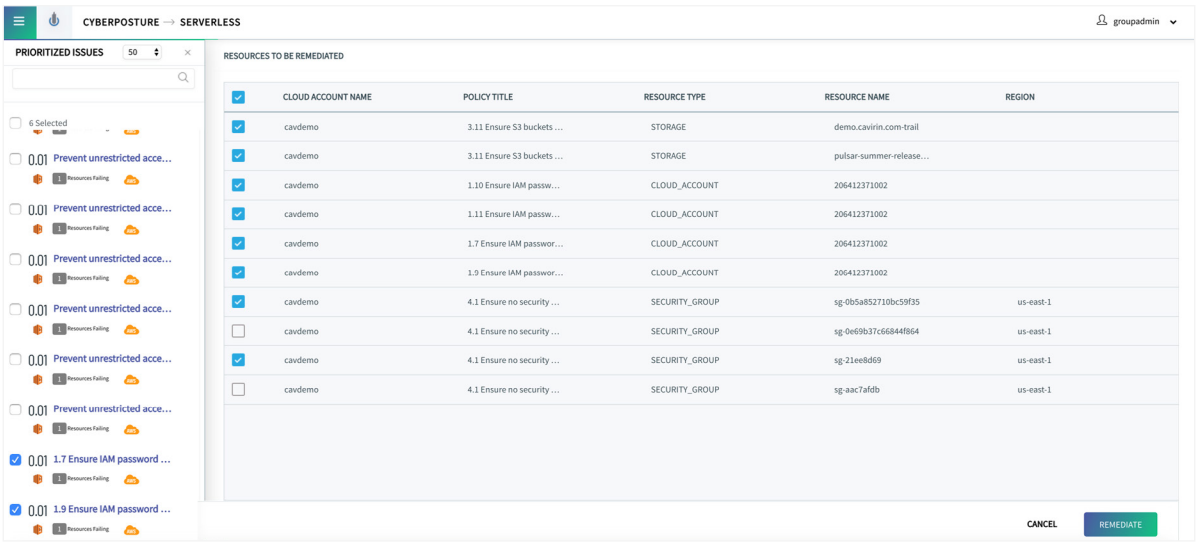
Proactive monitoring: Cavirin proactively monitors AWS CloudTrail, Google StackDriver, and Azure Audit logs to detect policy failures as changes are happening in your environment. After reaching a defined threshold for cloud resources, a full assessment is triggered automatically to ensure that you remain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

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

DevOps friendly API first architecture: Cavirin offers DevOps friendly API first architecture. This allows for easy integrations into the DevOps pipeline or to integrate with third-party reporting / dashboard platforms. Our Jenkins integration allows you to assess containers before deployment into your CI/CD pipeline.

Enterprise Integrations: Cavirin has integrated with ServiceNow and JIRA to open tickets and with Slack and PagerDuty to send notifications. It also has integration with Spluck SIEM and Google Security Command enter (GSCC) so that you can see Cavirin findings in the Splunk Dashboard and GSCC. It also integrates with RSA Archer for reports.

Fast & Easy deployment: Cavirin provides fast & easy deployment from cloud marketplaces (AWS, Azure, and GCP), and offers OVA for on-premise deployments. Cavirin assesses cloud services using cloud provider APIs. Cavirin offers agentless discovery and OS assessments. This allows Cavirin to deliver value to customers really fast. Our typical POC that assess clouds and OSes runs in less than an hour.



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 pack to align with organization's a) identify, access, and authorization policies, b) networking boundaries, c) security baseline, and d) data protection.
- 1300+ AWS policies covering 30+ top AWS cloud services including IAM, Elastic Compute Cloud (EC2), Simple Storage Service (S3), Elastic Block Store (EBS), Relational Database Service (RDS), Elastic File Store (EFS), DynamoDB, Simple Notification Service (SNS), Simple Queue Service (SQS), Elastic Search, RedShift, CloudTrail, Lambda, Elastic Container Registry (ECR), Kinesis, Snapshots, IAM Certificates, Key Management Service (KMS), ACM Certificates, CloudWatch, AWS Config, Virtual Private Cloud (VPC), Security Groups, Network ACL, Route 53, Auto-Scaling, Subnet, NAT Gateway, CloudFront, Elastic Load Balancing (ELB), and more.
- 550+ Azure policies covering top 7 services including Security Center, Storage Accounts, Logging and Monitoring, Networking, Virtual Machines, Service Bus, Azure Functions, and Security Baslines.
- 550+ Google Cloud policies covering top 7 services including Identity and Access Management, Logging and Monitoring, Networking, Virtual Machines, Storage buckets, Cloud SQL Database Services, and Kubernetes.
- AWS, Azure, and Google Network Policy Packs: 520 common ports

For Containers

- Cavirin Docker Image Hardening Policy Pack
- CIS Docker Community Edition Policy Pack (Cavirin-led)
- Cavirin Docker Image Patches and Vulnerabilities Policy Pack
- CIS Kubernetes Policy Pack (Cavirin-led)
- Container Linux (CoreOS) Hardening Policy Pack

For 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
- CIS Google Chrome Policy Pack

For Compliance

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

Continuous Monitoring

AWS Monitoring

S3, RDS, EBS, Instance Images, Security Groups, Classic Load Balancer, Amazon Application Load Balancer, VPC, Instance, KMS, CDN, IAM, CloudTrail, SNS, Amazon Auto-Scaling Groups, CloudWatch, SSL Certificates, IAM Certificates

AWS Auto-Remediation

Security Group, IAM, S3, Cloud Cloud Trail, 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

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.

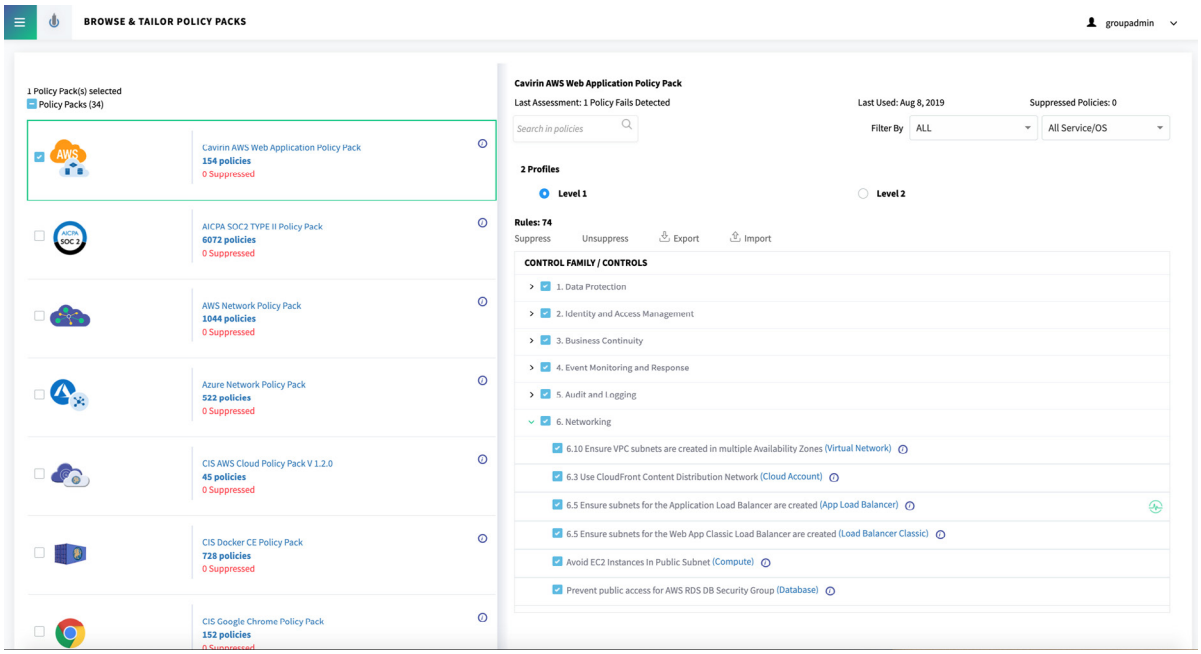
Operating System Based Policy Packs

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

Deployment Options and Details

- For deployments in VMware and KVM, use Cavirin's OVA format
- Launch Cavirin from Azure, AWS, and Google Cloud Marketplaces
- Create custom deployments in Azure, AWS, or GCP using AMI/VHD formats or use the Cavirin installer
- Integrates with Google Cloud Security Command Center
- 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.



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