Overview
Cavirin’s CyberPosture Intelligence offers a hybrid cloud security solution that easily integrates with your existing IT software to provide overall visibility and secure both workloads and cloud services, across any environment. This continuous protection, monitoring, and remediation, automates compliance and secures your organization from possible cyberattacks so you can comfortably move workloads to the cloud. Further, our patent pending machine learning, powering Cavirin CyberPosture Intelligence, provides you the most accurate credit-like scoring view of your cybersecurity posture so you can make informative decisions to protect your organization.

The Cavirin solution offers quick deployment, a cost-optimized footprint, and closes the gap from monitoring to change management. Its agentless architecture offers continuous visibility, is API-driven, and scales to the largest physical and virtual infrastructures. Cavirin supports the industry’s broadest horizontal coverage to offer up-to-the-minute compliance and risk assessments to supply audit-ready evidence as measured by every major regulatory and security best practice framework. These include CIS, DISA, GDPR, SOC, PCI, and HIPAA, as well as customized internal corporate policies. At its core, Cavirin allows enterprises to maintain their “golden” cybersecurity posture through:

- Continuous risk and cybersecurity posture management via automated scoring
- Integration of security into DevOps via Cavirin’s APIs
- Continuous compliance with the most comprehensive suite of industry regulations, best practices, and frameworks
- Prioritized remediation guidance and auto-remediation for golden posture

Popular Client Use Cases

- **Automate Compliance** to increase an organization’s operational efficiency and save hundreds of man-hours previously dedicated to manual processes.

- **Secure Cloud Migration** to not only address the requirements in the shared responsibility model but to augment the security capabilities provided by AWS, Google Cloud, and Azure.

- **Hybrid Cloud Visibility** to provide the most accurate credit-like scoring view of an organization’s security posture so informative decisions can be made to protect the company from today’s cyber threats.
Key Features

Agentless Resource Discovery - Agentless discovery of on-premises and AWS, Azure, GCP and Docker resources enables a unified view of all assets at layers including the cloud account, operating systems, containers and container orchestration. Authentication modes for AWS include ARN, IAM roles and Access/Secret Keys, while GCP and Azure are authenticated via service accounts.

CyberPosture Dashboard - Armed with visibility, Cavirin continuously assesses the security posture of all managed cloud services and workloads to compute a CyberPosture score, a number between 0 and 100. A score of 100 represents the least risk. Representing risk in this manner facilitates prioritized response plans and in-depth security analytics including score drill downs from the company level to cloud services, asset groups, individual resources, policy pack/control families and operating systems. At any of these levels, Cavirin depicts trends of CyberPosture scores to help CISOs assess the impact of security posture improvements.

Enterprise Integrations - Cavirin can push change requests into JIRA and ServiceNow for failed policies/controls, helping DevOps users manage work assignments in those systems. Notifications related to completed assessments and real-time monitoring alerts can be pushed to PagerDuty, Slack, and exported to RSA Archer.

Intuitive Workflow - The CyberPosture Dashboard is integrated with a workflow that guides the operator through cloud account selection, target workload discovery, framework selection, monitoring configuration, and finally assessment and remediation. This wizard-based approach reduces training requirements and the potential for error.

Comprehensive CyberSecurity & Compliance - With Control Frameworks for AWS, GCP, Azure and Containers, Cavirin automates CyberPosture assessments using a suite of configuration and vulnerability management frameworks as follows. Some of these frameworks were authored by Cavirin as indicated on the next pages. In aggregate, these frameworks result in 80,000+ controls.

Deployment Flexibility - The Cavirin solution is deployable within AWS, Azure, Google Cloud, or within an on-premise VM. It is also available from the AWS, Azure, and Google Cloud Marketplaces. Initial setup to first remediation guidance is under thirty minutes but with the added security offered by deploying within the organization’s security boundaries.

Comprehensive Reports - Assessments of control frameworks can be run on-demand or on a daily, weekly or monthly schedule. In all cases, reports are generated at the following levels:

- Asset Group report (Excel, PDF) for a given collection of resources. This report depicts an asset group CyberPosture score, its trend and the ability to drill down by Policy Pack or resources.
- Device report for compute resources (Excel, PDF). This report depicts pass/fail for policies in the various OS hardening policy packs including CIS, HiPAA, PCI and so on, for each compute resource.
- Remediation report for failed policies (Excel, PDF). This report depicts the list of devices failing each policy for in the various OS hardening policy packs including CIS, HIPAA, PCI, etc.

Configurable Controls - Any policy or policy pack can be suppressed to help organizations customize pre-built control frameworks to align with their CyberPosture strategy. Suppressed policies do not impact CyberPosture scores and are audited in compliance reports. In addition, Cavirin’s CyberPosture Language can be used by SecOps teams to author organization-specific controls and enforce them*. In the Policy Editor mode, such controls can evaluate any OS-level configuration*. In the Policy Builder mode, less technical users can drag and drop and build rules that evaluate presence of packages or files*. Once these rules are approved for an organization, they can be added to a custom policy pack to augment CyberPosture assessment and scoring.

Inject Security into CI/CD Workflows - As an “API-first” platform, Cavirin can inject security into CI/CD workflows so that only containers that meet security golden posture are promoted to development, staging and production.

Machine Learning - Technical controls mapped to Compliance and Security Frameworks (e.g. HIPAA, NIST 800-171) now leverage a Machine Learning based Recommender System to ensure consistency and accuracy of mapping and the resulting weights and severity. This further improves the efficacy of CyberPosture scoring and resulting remediation guidance.

* Spring 2019 Release
Closed-Loop Security For Auto-Remediation based on Golden Posture

- Based on a target CyberPosture score, a Cavirin Lambda Function can auto-remediate services across AWS and Google Cloud. The same capabilities for Azure will be available as part of the Spring, 2019 release. For container and VM workloads, Ansible integration creates playbooks used to harden images and detect security posture drift. Alternatively, the system generates an optimized response plan consisting of the list of failed policies, which if addressed will help an organization achieve its target posture.

Continuous Monitoring & Alerts

- Complementing Cavirin’s control and compliance frameworks, the solution aggregates events from AWS CloudTrail and Google StackDriver to detect indicators of compromise of your infrastructure. The alert system is based on user-settable thresholds for specific events. For example, you can alert SecOps if more than a threshold of AWS instances are instantiated within an hour – a well-known pattern of abuse or breach of AWS infrastructure. Any alert can result in a notification via Slack, PagerDuty or email. Alerts can also trigger an AWS Lambda function or Google Function for auto-remediation. The system also integrates with RSA’s Archer.

Top Benefits to Enterprises

- CyberPosture scores in under 30 minutes given Cavirin’s agentless architecture and simple installation

- Protect both the cloud infrastructure as well as workloads through comprehensive cybersecurity controls

- Automate DevSecOps by securing containers and images prior to deployment

- Early warning of breaches or compromise of infrastructure using real-time monitoring of AWS CloudTrail and Google StackDriver events
Specifications (Winter, 2019 Release)

Control Frameworks

For Public Clouds
- AWS CIS Foundation Benchmark: 43 controls spanning 9 AWS services including IAM, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon Virtual Private Cloud (Amazon VPC), Security Groups, AWS Key Management Service (AWS KMS), Amazon CloudWatch, AWS CloudTrail, AWS Config
- Cavirin AWS Web Services Policy Pack: 84 controls derived from CIS Three-Tier, spanning 17 AWS services including EC2, S3, Amazon Elastic Block Store (Amazon EBS), Elastic Load Balancing (ELB), Amazon Relational Database Service (RDS), Auto-Scaling, IAM, Amazon VPC, Security Groups, Subnet, NAT Gateway, Amazon CloudFront, Amazon CloudWatch, Amazon Simple Notification Service (Amazon SNS), Route 53, and AWS Config
- CIS Microsoft Azure Policy Pack (Cavirin-led): 41 controls spanning 6 services including Security Center, Storage Accounts, Logging and Monitoring, Networking, Virtual Machines, and Other Security Considerations
- AWS, Azure, and Google Network Policy Packs: 520 common ports

For Containers
- Cavirin Docker Image Hardening Policy Pack
- CIS Docker Community Edition 17.06 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:
Amazon S3, Amazon RDS, Amazon EBS, Amazon SNS, Amazon CloudWatch, Amazon Simple Notification Service (Amazon SNS), Route 53, and AWS Config

Cavirin installer
Create custom deployments in Azure, AWS, and Google Cloud Marketplaces
Launch Cavirin from Azure, AWS, and Google Cloud
Cavirin’s OVA format
Launch Cavirin from Azure, AWS, and Google Cloud
For deployments in VMware and KVM, use Cavirin’s OVA format
For compliance and security use cases that do not involve real-time monitoring, a single virtual machine is adequate.
Certified configurations include:
- VMware: 4 core x 16 GB memory with 300 GB disk – benchmarked to assess 1,000 target devices for CIS Policy Pack in an hour
- VMware: 8 core x 64 GB memory with 300 GB disk – benchmarked to assess 12,000 target devices for CIS Policy Pack
- AWS EC2 m5. xlarge: 4 core x 16 GB memory with 300 GB disk – benchmarked to assess 1,000 target devices for CIS Policy Pack in an hour
- AWS EC2 m5.4xlarge: 8 core x 64 GB memory with 300 GB disk – benchmarked to assess 12,000 target devices for CIS Policy Pack

Minimum Resource Requirements

AWS Auto-Remediation:
AWS Lambda Functions

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:
Google Functions

Operating System Based Policy Packs

- Amazon Linux (2016, 2017, 2018 versions inc. AWS Linux 2)
- Ubuntu (12.04, 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