DATA SHEET

cavirin

CONTINUOUS SECURITY ASSESSMENT AND REMEDIATION FOR HYBRID ENVIRONMENTS

Cavirin offers a true continuous security assessment and remediation platform, permitting CISOs and their SecOps teams to better manage security across their hybrid workloads. It enables them to do this automatically and apply best practices, versus existing approaches that are optimized for either on-premise or the cloud, are point-in-time instead of continuous, are time-intensive and prone to error, and that do not offer the breadth and depth of customized benchmarking.

Cavirin is a purpose-built, agentless and 'touchless' solution that deploys quickly within on-premise, cloud, and containerized infrastructures. It helps organizations reduce complexity, increase agility, and drive dramatic increases in efficiency with their security, risk and compliance programs through OS hardening and one-button remediation.

A true scale-out architecture guarantees linear analysis performance independent of deployment size, and content richness ensures 2-3x deeper coverage vs the competition. The solution reflects Cavirin's leadership in cloud-agnostic security with integrations for AWS, Microsoft Azure, and Google Cloud Platform. Private cloud support includes VMware and KVM, and Cavirin has taken a leadership role in protecting Docker containers and images.

- Reduce attack surface with AWS, Google Cloud Platform, and Microsoft Azure migrations
- OS hardening reduces vulnerabilities
- Immediately detect configuration drift from baseline security posture
- Simplify security configuration management
- Easy to deploy on-premise, SaaS, or cloud – agentless and API-driven architecture
- Monitors and alerts on security-impacting events

CAVIRIN FOR IT SECURITY

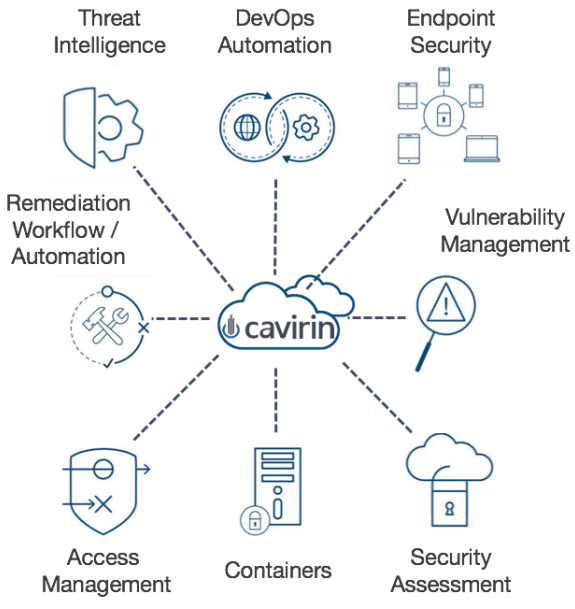
Cavirin Pulsar is a security assessment and remediation platform that enables organizations to implement a process of continuous security improvement, measured against all major best practice benchmarks. With continuous risk visibility, automated assessment and reporting, and prescriptive remediation guidance, IT staff can prioritize systems and remediation efforts, proactively reducing the cyberattack surface across on-premise, cloud, and complex hybrid IT infrastructures.

CAVIRIN FOR RISK AND COMPLIANCE

As a compliance platform, Pulsar enables Chief Risk & Security, as well as IT and DevOps leadership to implement continuous compliance practices providing audit ready evidence and up-to-the-minute compliance assessments, measured by every major regulatory and security best practice framework.

ELASTIC SCALE FOR THE CLOUD

Security must scale with the cloud to eliminate any blindspots, with the platform capable of supporting a million workloads or more across complex IT infrastructures. As these virtual and now containerized workloads expand and contract in real-time, IT must ensure that they adhere to the proper standards and benchmarks for their respective applications and data.



Extensible, API-Driven, and DevOps-Ready

KEY FEATURES:

Interoperability and DevOps-Friendly
Envisioned from day-one as a DevOps-friendly platform, Cavirin is a central point of integration across vulnerability assessment, configuration automation, threat intelligence, logging, access, and visibility vendors. Rich APIs deliver additional value to the CISO implementing the solution.

Next Generation UI
The UI focuses on simplicity and intuitive workflows, so that complex security scans and compliance assessments can be setup, run, and managed with a few simple mouse clicks. Its comprehensive dashboard then presents these scan results.

Agentless 'Touchless' Discovery and OS Hardening
Lightweight agentless discovery of data center and cloud resources across physical, logical, and virtual workloads provides a unified, near real-time view of assets and their configuration state. This greatly simplifies OS hardening.

Continuous Visibility
Cavirin continuously discovers, monitors, and tracks the state of IT assets, providing a superior alternative to periodic, snapshot-in-time audits that may not expose policy violations until it's too late. This real-time visibility is critical in the fast-moving world of virtualization and containers.

Automation and One-Button Remediation
Cavirin automates compliance reporting and on-demand risk assessments of operational, regulatory and security policies against frameworks and best-practice benchmarks. The platform then takes this to the next step with one-button remediation based on identified vulnerabilities.

Broad Policy Support
Policies are available for all major compliance and best practice frameworks, including NIST 800-53 R4, PCI DSS 3.2, HIPAA HITECH, ISO 27002, NIST Cyber Security Framework, CIS CSC 6.1, SOC 2 2016, CIS Benchmarks including AWS, and DISA STIGs. Cavirin can adapt any security standard or framework to align with evidence gathered through the Security Content Automation (SCAP) or Scripted Policy Framework process.

Monitoring and Alerts
A Risk Signaling Engine that is capable of monitoring security impacting events from various sources, run instant event-triggered assessments, raise alerts and provide options for mitigation workflows, enhances the real-time handling of security compliance posture.

ABOUT CAVIRIN
Cavirin reduces the chance of breach for organizations by providing continuous security assessment and remediation across physical, public, and hybrid clouds, supporting AWS, Microsoft Azure, Google Cloud Platform, VMware, KVM, and Docker. The company's cloud-agnostic solution offers continuous visibility, is agentless and multi-tenant, and scales to the largest physical and virtual infrastructures. For regulated industries, Cavirin offers up-to-the-minute compliance assessments, supplying audit-ready evidence as measured by every major regulatory and security best practice framework including CIS, DISA, PCI and HIPAA, as well as supporting internal corporate policies.

SOLUTION BENEFITS:

Continuous Risk Visibility and Management
Automated assessment enables a continuous consolidated view of security risk and policy compliance compared to manual snapshot assessments that are quickly out of date.

Improved Security Posture and Resilience
Continuous risk visibility, automated assessment, and prescriptive remediation guidance enable teams to remediate risk faster, reducing the cyberattack surface, improving security posture, and lowering the risk of a breach.

Continuous Compliance for Regulated Verticals
Painful annual and quarterly audit sprints become a thing of the past as continuous monitoring, automated assessments, and on-demand, audit-ready reports enable compliance to become a continuous process.

Lower Cost to Implement Best Practices
Pulsar dramatically reduces the cost of IT security management programs through automation of manual processes, freeing up resources for more strategic projects and more dangerous threats.

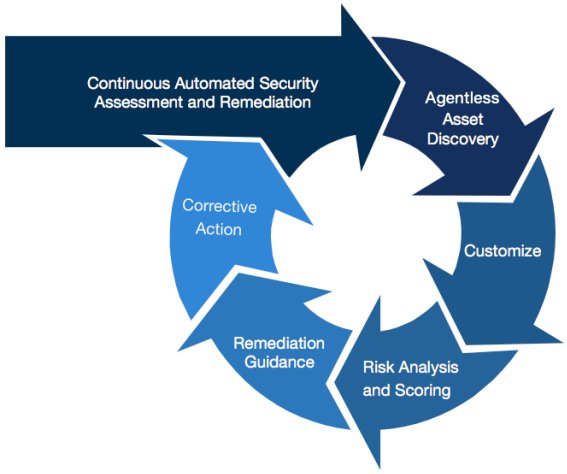
Sales Enablement
Allows IT and security teams to better support sales teams with fast turnaround of IT risk assessments and proof of compliance, critical to closing deals in today's hyper competitive sales environment.

80%

Decrease in Chance of Breach

90%

Decrease in Cost to Baseline Security Posture



Cavirin: From Risk to Remediation