Cavirin Secure on AWS

aws partner network | cavirin

Challenges
Cloud computing brings new security challenges

We have on our hands an explosion in IT complexity due to on-demand, agile consumption - of hundreds of services, with thousands of configurations, across multi-clouds/regions. This cloud computing paradigm shift demands a fresh, cloud-native IT security perspective. FSI organizations need to ensure proper access controls, data protection mechanisms, and robust audits of their heterogenous environments. Teams within FSI organizations need to operationalize cloud security with current teams, processes, and skillsets. DevOps pipelines incorporate need to include security baselines with precise, prescriptive security standards for cloud computing. Additionally, we need to setup organizations to evolve into real-time, continuous security organizations.

The Cavirin Secure Solution
Build your "First line of defense", continue with real-time security

Cavirin Secure starts by building a "First line of defense", ensuring "robust configurations" of key infrastructure and platform services which are the new "perimeter" security of cloud environments. Our one-click policies make it easy to ensure baseline access controls, data protection measures (encryption, privileged access), boundary controls, audits, monitoring, and compliance. Security operations teams use resulting prioritized remediation reports to create tickets to easily fix misconfigurations. Organizations can continue with Cavirin's full Cyberposture Intelligence platform, enabling devOps integration, and continuous IT health checks through real-time monitoring, threat detection, and auto-remediation.

Benefits

Use Cavirin's platform to build the "First Line of Defense" and continue with devOps integration, organization-specific policies, and real-time security.

Easily build a "First Line Of Defense"
Broadest set of policy checks across key IaaS, PaaS, OSs, container ecosystems - mapped to CIS, NIST, PCI, HIPAA, GDPR, etc.

Build custom policies easily
Customize policies per organization specific policies and asset groups, via our configurable and custom policy packs.

Operationalize cloud security
Prioritized list of fixes, with specific steps to fix misconfigurations, and operationalize via tickets, notifications, and one-click remediation.

Attain continuous security
Extend baseline and custom checks to devOps pipelines, monitor events in real-time, and integrate threat detection into cyberposture.

Cavirin on AWS

In the "shared responsibility" model customers are responsible for securing their AWS service instances. "Shared responsibility" is required as AWS must provide flexibility or choice – so customers can consume cloud for varied use cases. Cavirin has built a cloud-native, API driven, agentless solution to empower customers to perform one-click baseline configuration checks per environment. We discover AWS service instances, optimally retrieve bulk configuration information, and utilize Amazon Simple Queue Service, Amazon Simple Notification Service, and AWS Lambda functions to allow one-click remediation of misconfigurations. The core "First Line of Defense" solution is extended to incorporate AWS CloudTrail and Amazon CloudWatch for real-time monitoring, and Amazon GuardDuty for threat management. Cavirin is an APN Advanced Technology Partner and has achieved the AWS Security Competency.

Features

"First Line of Defense" (30+ AWS Services)

Broad set of policies for key IaaS, PaaS, OSs, and containers. Cavirin has built important policy checks for over thirty AWS services - Amazon Elastic Compute Cloud, Amazon Simple Storage Service, Amazon Virtual Private Cloud, Security Group, AWS Identity and Access Management, AWS Cloud Trail, AWS Key Management Service , AWS Kubernetes, databases, and more. Prioritized, specific remediation reports are provided to fix and integrate into devOps pipelines. Organization-specific policy checks are supported via configurable & custom policies, and tag-based asset groups.

Continuous security via cyber posture intelligence platform

Extend "First Line of Defense" for continuous IT health checks. We have integrated our platform with AWS CloudTrail and Amazon CloudWatch (matching our policies) to alert users of specific changes to the environment in real-time. Furthering our core cyberposture score, we have integrated all Amazon GuardDuty signals into our policy checks.

Case Study: FSI (non-traditional capital markets)

Challenges

The customer is a working capital marketplace, that seamlessly matches Account Receivables with Account Payables to turn receivables into cash flow and payables into income. Their customers, due to sensitive financial data, demand rigorous compliance and cloud security posture management. The solution spans hybrid environments consuming varied IaaS, PaaS, OSs, and containers resources.

Solution

Deployed on AWS, Cavirin's "First Line of Defense" with one-click policies (SOC2, NIST, GDPR, etc.) are used to scan and fix misconfigurations across IaaS, PaaS, and container services. Cavirin's platform will be used for OS config checks next.

Results

The client was able to simplify security and compliance using Cavirin as a single-pane of glass to discover resources, scan against benchmarks, and fix misconfigurations. The company has been able to provide valuable technical evidence to audit.

Get started with Cavirin solutions on AWS

Contact Cavirin for further information.