Aqua Wave overview

Aqua Wave provides a SaaS-based, cloud security posture management (CSPM) solution for AWS Control Tower. Aqua CSPM continually audits your cloud accounts for security risks and misconfigurations.

This is performed across hundreds of configuration settings and compliance best practices, enabling consistent, unified multi-account security. It also provides self-securing capabilities to help ensure your cloud accounts do not drift out of compliance by leveraging a policy-driven approach.

Product features

Continuous cloud compliance
Audit hundreds of settings for risks and misconfigurations:

- CIS Benchmark, PCI-DSS, HIPAA, GDPR, SOC2 Type 2, Well-Architected Framework, custom requirements, and more.
- Scan AWS CloudFormation templates (Infrastructure-as-code) for weaknesses.

Auto remediation
Automatically fixes issues if configurations drift out of policy.

- Active monitoring provides detailed information and actionable advice
- Leverage automation remediation for self-healing infrastructure with least-privilege access to your customer’s environment

Enterprise scale and extensible
Multiple users and teams provide support for hundreds of cloud accounts using SSO with SAML 2.0. Integrations include:

- AWS Control Tower supporting hundreds of AWS accounts
- SIEM and many other collaboration tools
- RESTful APIs to add integrations and automation workflows

Highlights

- Visibility through a single-pane-of-glass into deployment risks
- Continuous Auditing for infrastructure security risks and misconfigurations
- Extensive compliance reporting, including CIS Foundation Benchmarks and many more
- Scans and reports for PCI-DSS, HIPAA, Well-architected Framework, GDPR, and custom needs
- Consistent policies and unified security to reduce risks in production
- Auto-remediation and self-securing infrastructure
- Detailed, actionable advice and alerts
- Real-time events monitoring with visibility into API calls via AWS CloudTrail
- Enterprise-ready scale integrations with AWS Control Tower and leading productivity tools
- Extensible open-source architecture
**How it works**

The Aqua CSPM integration enables automated onboarding of AWS accounts created via AWS Control Tower, by leveraging the inherent account provisioning workflow. This will ensure that any newly created account will automatically be audited and monitored according to best practices and compliance standards for AWS. Through this integration, you will gain a multi-account security framework that will ensure that all your AWS accounts are always in conformance with cloud infrastructure best practices.

Aqua CSPM makes sure enterprises are using the cloud securely, continuously monitoring and alerting on any identified risks – either accounts out of compliance or exposed to vulnerabilities. It examines a vast array of misconfigurations across user roles and privileges, certificates, and multi-factor authentication (MFA), specific service configurations, data encryption, networking, auditing features, usage trends and conducts anomaly detection. Additionally, it also provides extensive reporting for Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), AWS Well-Architected Framework, General Data Protection Regulation (GDPR), and supports custom compliance requirements.

With a cross-account security auditor Identity and Access Management (IAM) role, Aqua CSPM can only see the infrastructure configurations and provides useful insights into the security posture of your cloud services. The Aqua CSPM integration automates the creation of this IAM role when a new account is enrolled, ensuring that your AWS accounts are always in audited for conformance right out the gate.

The integration comes in the form of a CloudFormation template that is extremely easy to deploy in your AWS Control Tower management account in the home region. The home region is the AWS Region where the Landing zone is set up. The solution involves a one-time deployment of the CloudFormation StackSet, which gets automatically triggered as a part of the account provisioning workflow.

Solution available in [AWS Marketplace](https://aws.amazon.com/marketplace)