Proactively embed cloud security into your CI/CD process

Most enterprises must manage complex, multi-cloud environments. A single consistent interface can offer a significant advantage when it comes to monitoring and managing distributed, dynamic multi-cloud environments.

FireEye Cloudvisory is a control center for cloud security management that delivers visibility, compliance and governance to any cloud environment. Cloudvisory runs cloud-native microservices for asset discovery and compliance scanning to enable end-to-end automation of detection and response for complex multi-cloud environments. With Cloudvisory, you can take control of your cloud security.

**Figure 1.** Drill down to granular level on a per asset basis with Asset Inventory Inspector.

**HIGHLIGHTS**

- **Infrastructure as code**
  Cloudvisory scans infrastructure-as-code with Terraform APIs to improve your continuous improvement and continuous deployment (CI/CD) pipeline processes. It helps identify and address vulnerabilities early in the process before vulnerabilities and misconfigurations impact your production infrastructure.

- **CI/CD pipeline**
  When you look at a Test>Build>Run CI/CD pipeline process, Cloudvisory enables security at every step, from invocation to building, based on security best practices and even as cloud resources are moved into production. Cloudvisory can run continual assessments to ensure that processes are secure and do not drift from the original configurations.

- **IAM policy inspection**
  Cloudvisory offers a Policy Inspector for Identity and Access Management to identify who has access to what resources. The roles and permissions enabled for a given user or resource are critical when dealing with a forensic investigation or by enabling your team to be proactive with IAM policies.

- **Zero Trust**
  Zero Trust initiatives require consideration of the roles and permissiveness of both IAM and network policies. They also take a holistic view of your overall cloud security exposure and the impact of a potential breach, whether it is a user and password breach or a network security breach or data exposure.
The Cloudvisory Difference

**Machine Learning**
A complete set of (artificially) intelligent tools that work together to empower cloud security posture improvement.

**Intelligent Network Microsegmentation**
Cloud-native governance of network microsegmentation policies via cloud-native firewalls and security controls.

**Orchestrated Remediation**
Orchestrated remediation of compliance failures & governance of desired-state security policies.

Multi-cloud Native Support
In addition to public cloud providers such as AWS and Azure, Cloudvisory supports cloud-native visibility, compliance & governance for OpenStack and Kubernetes.

Agentless Monitoring & Execution
Agentless monitoring of all network flows across multiple cloud providers and accounts.

Figure 2.
Cloudvisory delivers always-on visibility, compliance, and governance over your cloud environments.

FireEye Cloudvisory is part of FireEye XDR
Learn more at [www.FireEye.com/XDR](http://www.FireEye.com/XDR)

©2021 FireEye, Inc. All rights reserved.
FireEye and Mandiant are registered trademarks of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners.
CS-EXT-DS-UG-EN-000299-03