Achieve cloud compliance and control with FireEye Cloudvisory

Cloud-native security controls are more secure than traditional datacenter approaches, but are not being properly leveraged. This leaves enterprises with massive security holes that can be exploited by hackers and greatly impacts application uptime and business agility. Core cloud security challenges include:

1. Real-time visibility into cloud infrastructure security is non-existent, delaying detection of critical threats.
2. Cloud security controls are not being used to “least privilege” allowing risky access and increasing threat of breach.
3. DevOps teams lack a method for organizing, testing, auditing, monitoring and enforcing provisioned controls, leading to misconfiguration of policies.
4. Misconfiguration of cloud security controls is the leading cause of risk and breach.
5. Lack of continuous compliance validation and enforcement of policy controls leaves enterprises exposed to great risk.

Cloudvisory delivers cloud visibility, security, and policy management. It provides customers visibility framework for understanding the infrastructure intricacies, finds areas of concern, and incorporates a push-button remediation solution that aligns with enterprise change management procedures.

Cloudvisory is is enterprise-class, highly scalable, and trusted by Fortune 500 customers for centralized security management across cloud, hybrid-cloud, and multi-cloud environments. Cloudvisory delivers a complete cloud security platform through cloud-native integrations and controls for continuous Visibility, Compliance & Governance – with a full suite of tools that enable any organization to quickly mature their cloud security posture through a phased implementation approach.

The Cloudvisory Difference

Machine Learning
Intelligent Microsegmentation
Orchestrated Remediation
Multi-Cloud Native Support
Agentless Monitoring & Execution

The Shared Responsibility Model maps your end-to-end security

The Shared Responsibility Model (SRM) makes it easy to understand your role in protecting your unique AWS environment. Choose from the many cloud-ready software solutions to meet the highest standards of data security in the cloud.

---

### Customer Responsibility for security ‘in’ the cloud
- Platform, applications, identity & access management
- Operating system, network & firewall configuration
- Client-side data encryption & data integrity authentication
- Server-side encryption (file system and/or data)
- Networking traffic protection (encryption, integrity, identity)

### AWS Responsibility for security ‘of’ the cloud
- Compute
- Storage
- Database
- Networking
- Regions
- Availability zones
- Edge locations

---

**FireEye: Intelligence-Led Security**

FireEye is the intelligence-led security company, bringing together innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant consulting.

Cloudvisory empowers customers with a single plane of glass to manage multi-cloud environments. The expanded offering will assess configurations against compliance standards and best practices, deliver ongoing monitoring of environments, and report on actions that are out of compliance, providing visibility into which user activities and compliance issues can increase an organization's risk profile.

---

**AWS Resources**

https://www.cloudvisory.com/

https://www.fireeye.com/solutions/cloud-security.html

---

**Additional information**

https://aws.amazon.com/compliance/shared-responsibility-model/