FIREEYE™

A HOLISTIC CLOUD SECURITY APPROACH FOR GOVERNMENT

How local, state, and federal agencies can secure their cloud environments with Amazon Web Services and FireEye

amazon web services | Partner Network

ADVANCED TECHNOLOGY PARTNER

Introduction

Organizations across all industries and sizes are migrating to the cloud to gain speed, scalability, cost efficiencies and many other benefits.

The mindset of cloud adopters is also shifting from "cloud first"—putting all workloads into public cloud models—to "cloud smart," that prioritizes specific functions or requirements in cloud environments. For example, U.S. federal government institutions are adopting the 2019 Federal Cloud Computing Strategy to emphasize security and privacy considerations in all procurement decisions.

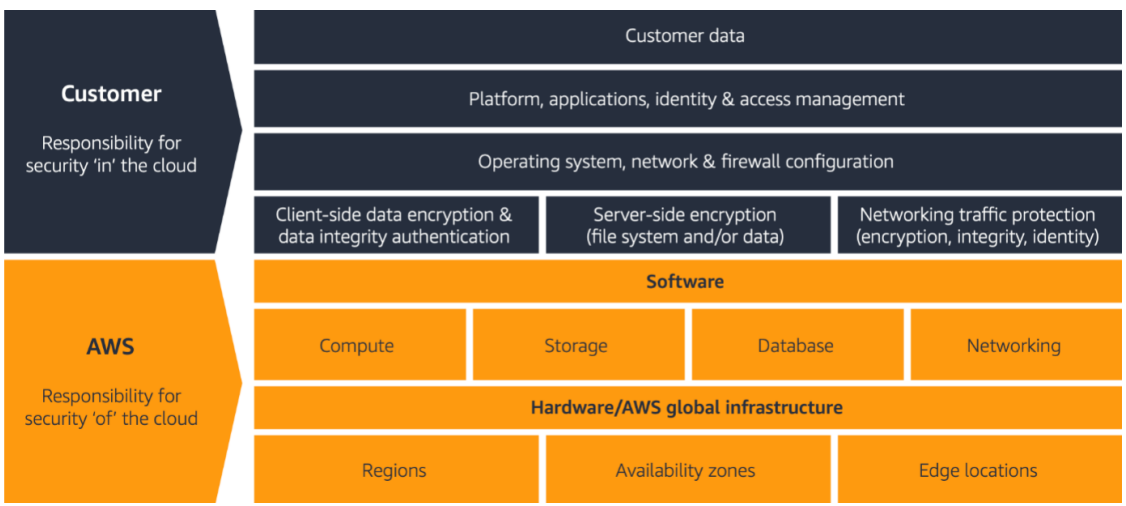
All institutions across the public sector are rightly concerned about securing data as it's stored, transferred and accessed via cloud environments. A single security breach resulting from ransomware or undetected misconfigurations can cause significant financial, privacy and reputational damage. In fact, analyst firm Gartner has reported that through 2025, 99% of cloud security failures will be the customer's fault.[1]

Evidence-based confidence is critical for cloud security. For that confidence, federal agencies and public-sector institutions must achieve visibility across cloud environments, while meeting compliance requirements and ensuring controlled user access.

It's a tall order because most organizations face staff shortages in cloud security skills and expertise. Regardless, those organizations are still responsible for protecting cloud data, applications, configurations and more (Fig. 1).

Figure 1. The Amazon Web Services Shared Responsibility Model for Cloud Security.

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



The Amazon Web Services and FireEye partnership can help to empower public-sector institutions and agencies to comprehensively secure their cloud environments.

The partnership helps fill gaps and meet objectives—no matter where your organization is in its cloud journey.

Partnership solutions offer a holistic approach to pursuing four distinct goals:

- Gain greater visibility
- Improve compliance efforts
- Achieve intelligent threat detection
- Build a measurable security strategy

1 Gartner (October 10, 2019). Is the Cloud Secure?

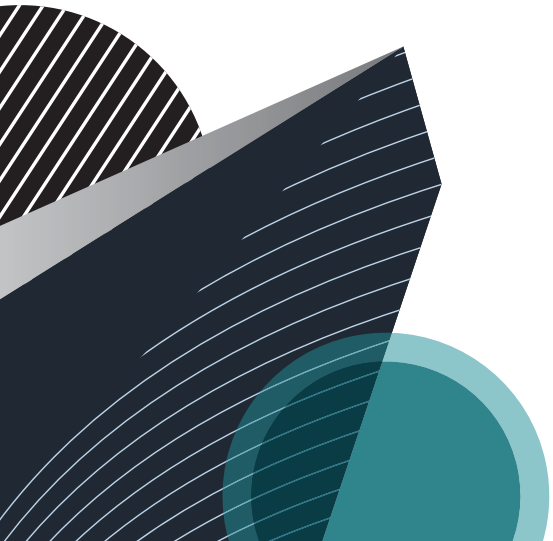
Gain Greater Visibility

Most organizations are wrestling with complex IT environments. The push to adopt cloud is burdensome for resource-thin security teams, who are already fatigued with an overwhelming volume of alerts.

Organizations can reduce false positives and gain contextual analysis of threats with FireEye Cloudvisory. It's a complete cloud security solution with a full suite of intelligent, cloud-native tools that work together to reduce integration complexity.

BENEFITS

- Gain uniform visibility across cloud infrastructure—including multi-cloud environments—through a single console
- Reduce risk of cloud security misconfigurations
- Automate policy management and intelligent detection to ensure governance with frameworks and practices such as NIST and FedRAMP
- Protect data and applications by continuously discovering and mapping of assets



Improve Compliance Efforts

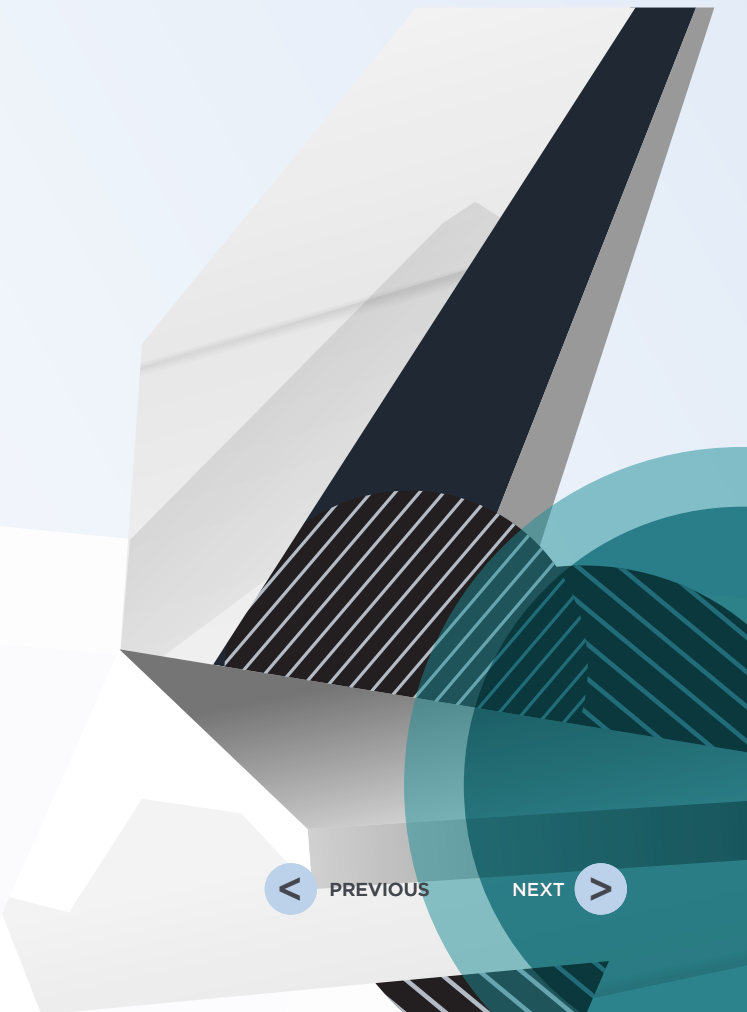
Government security teams—and those from enterprises—are often struggling to identify and collect data across their organization. Their skills shortages can result in a lack of ongoing compliance monitoring and enforcement of policy controls.

FireEye offers several solutions to help public-sector agencies gain control and improve compliance.

FireEye Cloudvisory can assess configurations against compliance standards and best practices from a single console. It continuously monitors environments and reports on actions that are out of compliance. Cloudvisory also provides visibility into which user activities and compliance issues may increase risks. Automated compliance reporting helps keep security staff focused on advanced tasks such as threat hunting instead of audit preparation.

For a full list of supported compliance standards, see **Continuous Compliance Assurance for Cloud Security**.

FireEye Helix is a security operations platform that empowers security teams with greater control across all cloud and non-cloud environments. It identifies and traces unusual behaviors to not only improve incident detection, but also centralize audit logging for compliance purposes. Helix also makes compliance reporting more efficient with customized dashboards.



Achieve Intelligent Threat Detection

It is imperative that federal, state and local governments secure sensitive data. They must be able to quickly discover and remediate threats. The sophisticated, ever-evolving cyber threat landscape can make it very challenging to know that they have the latest threat information.

FireEye solutions include intelligent detection capabilities to help organizations protect citizen data and mission-critical applications.

FireEye Cloudvisory is a control center for cloud security management that delivers visibility, compliance and governance to any security 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.

FireEye Email Security—Cloud Edition is a secure email gateway (SEG) that stops advanced threats with firsthand knowledge of cyber attacks. The solution blocks malware, phishing URLs and impersonation techniques, leaving attackers no chance to take advantage of users.

FireEye Endpoint Security combines the best of legacy security products, enhanced with FireEye technology, expertise and intelligence to defend against today's cyber attacks. Based on a defense-in-depth model, the solution uses a modular architecture with default engines and downloadable modules to protect, detect, respond to and manage agents.

FireEye Network Security is a suite of products that provides advanced threat protection and investigative capabilities, wherever an organization's data resides. The solution offers visibility into the world's most sophisticated attacks and protects networks, assets and users from known and unknown threats. FireEye Network Security and Forensics are available as Amazon Machine Images (AMIs), giving customers the ability to run these products natively in their AWS environments.

FireEye Detection On Demand is a threat detection service that identifies file-borne threats in cloud or web applications. It rapidly inspects and detects known and unknown threats and validates the security of files and content with the latest threat intelligence.

FireEye Helix integrates disparate security tools and augments them with SIEM, orchestration and threat intelligence capabilities. It detects and remediates advanced threats with security analytics that use machine learning and artificial intelligence. Helix also simplifies cyber security operations by automating incident response.

Build a Measurable Security Strategy

Sometimes public-sector institutions must step back and get an objective, comprehensive assessment of their existing cloud security architecture. This can help identify infrastructure and staffing resource gaps, as well as other risks, while defining a strategic roadmap for improvements.

Mandiant assessments evaluate current security environments and offer detailed, practical recommendations toward outcomes such as making sure that personnel with relevant skills have access to appropriate technology.

Mandiant Cloud Architecture and Security Assessments help organizations gain risk visibility related to existing cloud configurations. They also review functional capabilities to see where proactive threat monitoring and detection can improve. Mandiant experts also recommend security control prioritizations and offer tactical coaching for effective risk management.

Mandiant Security Validation includes a cyber security management platform that enables public sector institutions to continuously validate the effectiveness of their security posture. It provides evidence of configuration issues and gaps across people, processes and technologies. By identifying gaps and redundancies, organizations can optimize both security posture and spend.

Take the Next Step

FireEye can support your cloud mission—whether your organization is just starting to migrate workloads to Amazon Web Services or is actively shifting to a multi-cloud architecture.

To learn more about cloud security, visit: **www.FireEye.com/cloud**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™