FEDERAL GOVERNMENT: MULTI-CLOUD SECURITY, GOVERNANCE, AND COMPLIANCE

SPOTLIGHTS

Industry
Federal Government

Use Case
Multi-cloud governance, compliance, and cybersecurity performance monitoring

Mission Benefits
- Provides department/agency-wide cybersecurity and privacy performance.
- Verifies regulatory compliance prior to deploying workloads to production environments.
- Reduces the cost and required resources to process independent system-level Authorization to Operate (ATO) by leveraging an enterprise strategy for automating the ATO for each cloud service provider (CSP).
- Implements a security management approach that protects any authorized cloud environment, independent of data, enabling broad governance.

Operational Benefits
- Supports AWS GovCloud (East) and Azure Government Cloud.
- Centrally discovers all cloud native services used in GCP, AWS, and Azure.
- Simplifies adherence to established security best practices (e.g., PCI DSS, GDPR, ISO 27001:2013, and NIST).

Security Benefits
- Automates FISMA and NIST Compliance (e.g., NIST SP 800-53 and NIST SP 800-171).
- Aligns CSP infrastructure security policy with government security standards and guidelines (e.g., NIST SP 800-53).
- Supports the Cloud Security Alliance Cloud Controls Matrix (CCM).

Mission Drivers

Federal governments will use the cloud as a new foundation upon which to build more effective security capabilities across domains, including cyberspace. An explosion of government adoption of public, private, and hybrid cloud services has introduced new ways to scale and deliver efficient operations across multiple cloud platforms. Many federal governments have committed to modernizing their IT infrastructure to better utilize the latest technologies for improved productivity and operations. As part of this modernization effort, federal agencies are migrating legacy systems to the cloud, opening the way for increased agility. As an example, the US 2019 Federal Cloud Computing Strategy outlines a long-term, high-level strategy to drive cloud adoption and prioritize commercial clouds. It recognizes that "hybrid and multi-cloud environments can be effective and efficient at managing workloads." As opportunities to move to the cloud increase, however, so do the risks.

Furthermore, the US Data Center Optimization Initiative requires US federal agencies to consolidate and modernize IT infrastructure. As part of this initiative, the Cloud Smart strategy accelerated agency data center consolidations and closures, resulting in cloud adoption.

The key objectives for government cloud policy are:

- Reduce costs through consolidation, optimization, and innovation
- Enable elastic growth and scale to meet evolving operational needs
- Streamline processes to reduce redundancy and increase efficiency

Business Problems

As federal agencies continue to transition and expand their footprint into the cloud, it is critical to ensure these systems are secure and vulnerabilities are addressed immediately. Today's adversaries are more skilled and persistent, able to exploit vulnerabilities at a faster pace than before. As more systems transition to or are created in the cloud, these environments come with inherited risks across the Federal Enterprise Architecture (FEA) that can grow exponentially.

The cloud creates a number of challenges for governments, especially when expanded across multi-cloud environments. The US Department of Defense has inventoried more than 500 cloud deployments with different service providers across all its agencies, leaving open questions around data protection, risk management, and governance.

As agencies transition from cloud acquisition to cloud maturity, the top concerns include:

- Disparate cloud environments making cloud/multi-cloud governance complex

- Decentralized administration and lack of visibility resulting in inadequate security and compliance
- Multi-cloud management causing undue operational burden, hindering ability to rapidly detect and respond to threats

Traditional Approaches

The traditional ways of meeting each agency's cybersecurity governance and compliance requirements are typically process-oriented and manual. The Risk Management Framework (RMF) provides guidance on managing risks across the enterprise. Each agency's applications, systems, and networks must undergo this process to achieve ATO. Each department or agency must then provide metrics based on government-wide policies and objectives.

These three key metrics provide a comprehensive view of an agency's cybersecurity and privacy performance:

- Chief Information Officer (CIO) FISMA metrics
- Inspectors General (IG) FISMA metrics
- Senior Agency Official for Privacy (SAOP) metrics

The principal drawbacks to this approach are:

- Metrics are time-consuming to generate
- Manual processes are susceptible to errors
- Metrics are not in real time or dynamically updated

Palo Alto Networks Approach

The expansion of government reporting and metrics provides opportunities to enforce standardized policies that comply with regulations and govern agency security requirements across the federal cloud environment. Meanwhile, the methods for securing virtualized environments and cloud native workloads have evolved alongside the infrastructure in which they reside. Palo Alto Networks offers Prisma™ Cloud, a cloud native security platform that provides comprehensive visibility, threat prevention, compliance assurance, and data protection in a consistent manner across multi-cloud environments. This allows agencies to define policies based on agency requirements, security best practices, and automated monitoring of violations.

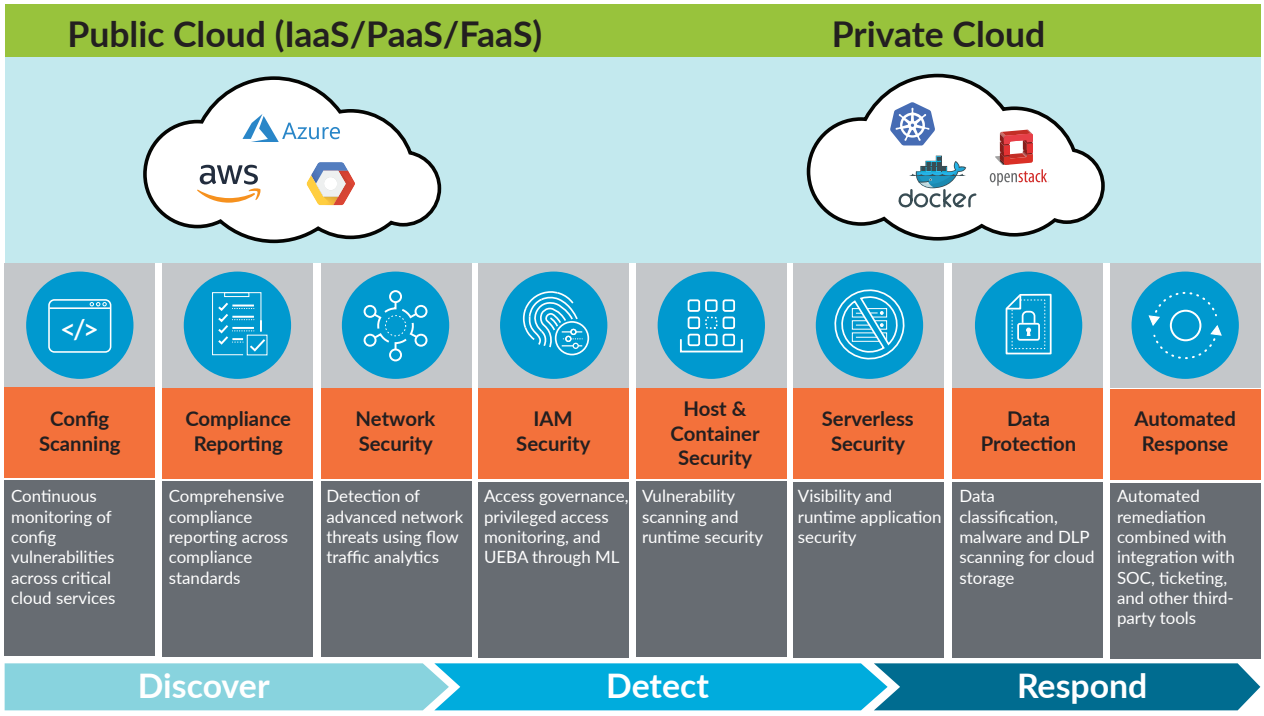

Figure 1: Multi-cloud governance with Prisma Cloud

Ensuring governance and compliance across multi-cloud environments requires:

- **Real-time discovery and classification** to identify resources and data across cloud platform- and infrastructure-as-a-service (PaaS and IaaS) environments.
- **Configuration governance** to ensure application and resource configurations match security best practices as soon as they are deployed, in addition to preventing configuration drift.
- **Compliance auditing**, leveraging automation and built-in compliance frameworks, to ensure compliance at any time and generate audit-ready reports on demand.

Prisma Cloud helps agencies ensure any deployed resources are correctly configured and adhere to agency security standards from the moment of deployment. Additionally, ensuring continuous compliance and generating audit-ready reports, once multi-month tasks, can be automatically processed in real time. Prisma Cloud continuously monitors, discovers, and assesses the configuration of newly deployed resources in real time, generating reports against a library of policies and compliance frameworks that includes NIST, CIS, PCI DSS, HIPAA, GDPR, ISO, and SOC 2.

Deployment Considerations and Best Practices

To prevent successful attacks, it's essential to ensure cloud applications are correctly configured and adhere to agency security standards from day one. Additionally, to keep public confidence and trust alive, it's critical to make sure these applications—and the data they collect and store—are properly protected and compliant. Meeting security standards and maintaining compliant environments at scale is the new expectation for security operations. As an agency transitions data processing from on-premises to the cloud, there are a few key considerations and best practices to keep in mind:

- **Bifurcation:** Help manage and measure risk across the agency's multi-cloud ecosystem by defining organizational roles and responsibility to inform department-wide dashboards.
- **Regulatory compliance:** Establish and enforce a "comply before connecting" strategy over how applications progress from code to production, providing oversight across hosts, containers, and serverless infrastructure in a single platform.
- **Security:** Replace manual auditing and investigations with automated reporting, prioritization, and remediation.
- **Multi-cloud environments:** Simplify cloud security management and achieve consistent protection. Provide comprehensive visibility, threat detection, and rapid response across your entire cloud ecosystem, including Google Cloud Platform (GCP™), Amazon Web Services (AWS®), and Microsoft Azure®.

Customer Implementation

Agencies themselves are responsible for securely configuring the instances, operating systems, and any necessary applications as well as maintaining the integrity of the data processed and stored by each virtual machine. The cloud service provider (CSP) is responsible for securing the underlying infrastructure. This shared responsibility model is often a point of confusion for consumers of cloud services. It must be noted that cloud services have default configurations that may be secure upon implementation, but it is up to the customer to make the assessment and lock those service configurations down to ensure the integrity of the data itself. Security and compliance risks in cloud computing threaten an agency's ability to drive mission performance and improve operational management. The dynamic nature of the cloud, coupled with the potential complexity of having multiple CSPs in the environment and the massive volume of cloud workloads, can make security and compliance cumbersome.

Public cloud environments use a decentralized administration framework that often suffers from a corresponding lack of centralized visibility. Additionally, compliance for these environments is complex to manage. Incident response requires the ability to rapidly detect and respond to threats—areas in which public cloud capabilities are limited.

Seeing the adoption of public cloud services by multiple agencies, a defense agency built a cloud governance environment as a department-wide service. Other federal departments and agencies will be able to use this centralized service to connect their disparate cloud environments as well as monitor risk and performance of those environments through a centralized service. This will also allow for streamlined reporting through simplified dashboards specifically designed to monitor each agency's security requirements.

Implementation Overview

Figure 2 depicts how this agency leveraged Prisma Cloud to measure risk, performance, and automated remediation of noncompliant multi-cloud environments. The dashboards show realtime monitoring of compliance and risk performance metrics set forth by agency security requirements. Bifurcation is achieved and proper oversight is established with automated and dynamic realtime reporting.

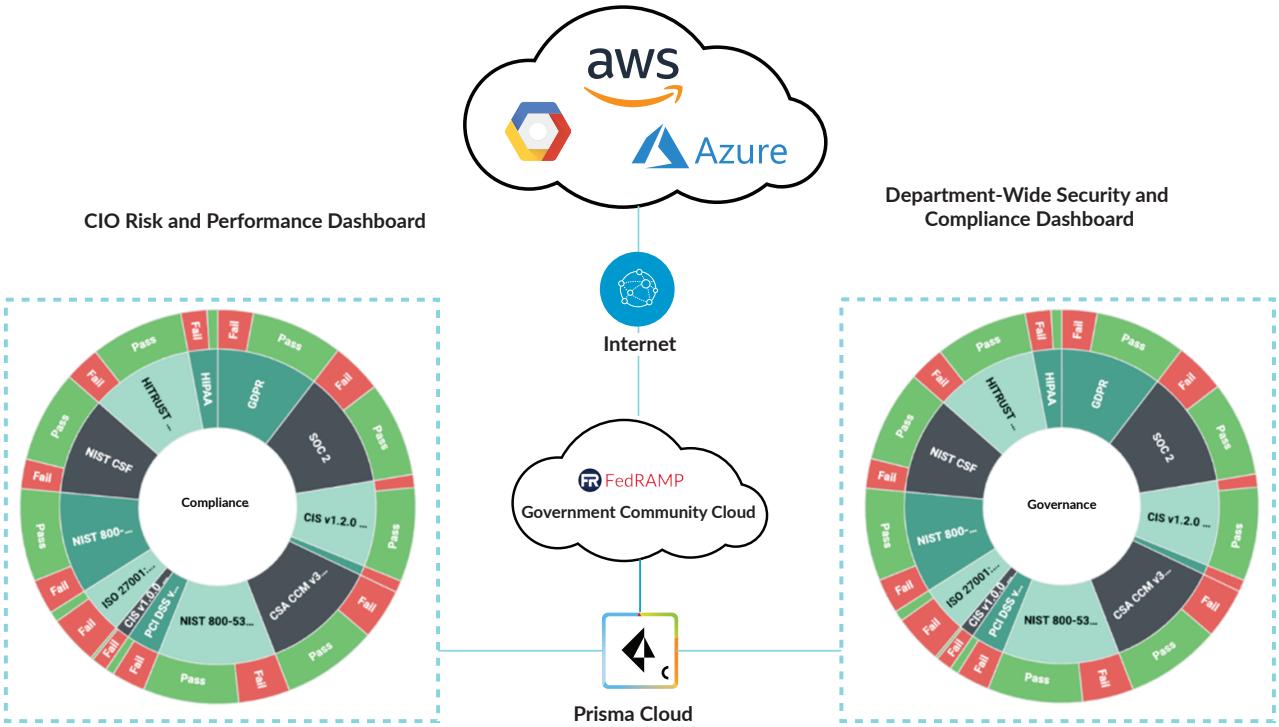

Figure 2: Agency monitoring of multi-cloud environment

Results

- Measures security policy performance against established metrics
- Improves visibility of assets and applications
- Automates security and compliance posture reporting
- Monitors threats in real time to identify noncompliant configurations, network intrusions, and host vulnerabilities
- Detects anomalies to identify account compromise and insider threats
- Conducts forensic investigation of current threats and past incidents to quickly determine root cause
- Prioritizes issues and responds with contextual alerts

Benefits of Cloud Native Security with Palo Alto Networks

Through proactive security assessment and configuration management using industry best practices, Prisma Cloud makes cloud computing environments more resilient. Prisma Cloud enables agencies to implement continuous monitoring of their multi-cloud infrastructure, automatically providing up-to-date security posture status to help agencies make cost-effective, risk-based decisions about service configuration and vulnerabilities inherent in cloud deployments. Organizations can also use Prisma Cloud to prevent the cloud infrastructure from falling out of compliance as well as provide visibility into the security posture of the cloud to avoid failed audits and subsequent fines associated with data breaches and noncompliance. Palo Alto Networks continues to support federal government missions and objectives to secure information systems and data across the FEA, aligned with industry best practices and all applicable laws, regulations, and guidance.

By leveraging Prisma Cloud to standardize several security functions, federal agencies may realize the following benefits:

Mission Benefits

- Department/Agency-wide cybersecurity and privacy performance.
- Verification of regulatory compliance prior to deploying workloads to production environments.
- Reduced cost and resources required to process independent system-level ATO by leveraging an enterprise strategy for automating the ATO for each CSP.
- A security management approach that protects any authorized cloud environment, independent of data, enabling broad governance.

Operational Benefits

- AWS GovCloud (East) and Azure Government Cloud support.
- Centralized discovery of all cloud native services, assets, and accounts used in GCP, AWS, and Azure.
- Simplified adherence to established security best practices (e.g., PCI DSS, GDPR, ISO 27001:2013, and NIST).

Security Benefits

- Automated FISMA and NIST compliance (e.g., NIST SP 800-53 and NIST SP 800-171).
- Alignment of CSP infrastructure security policy with government security standards and guidelines (e.g., NIST SP 800-53).
- Support for Cloud Security Alliance: Cloud Controls Matrix (CCM).

Additional Resources

For more information on how Palo Alto Networks can secure cloud environments, please visit our Prisma Cloud page. Visit our Federal Government page to learn how to modernize agency operations while managing risks.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

multi-cloud-security-governance-and-compliance-uc-011620