Customer Case Study:
Health Care Organization Secures Multi-Cloud Environments with CNAPP Cloud Security Tool

Industry: Health Care

Engagement Type: Cloud Security Tool Deployment

Delivery Format: Remote

Engagement Duration: 5 Days

Client Overview

Health Care Organization is a technology-forward health care provider operating across North America. With business-critical applications and services distributed across more than 35 AWS accounts and multiple Azure tenants, Health Care Organization sought to improve cloud governance, strengthen its security posture, and prepare for audit readiness across their rapidly growing cloud estate.

To achieve these goals, the customer engaged our team to perform a Deployment of a Cloud Security Tool, laying the foundation for identity-aware security operations, multi-cloud visibility, and continuous compliance across AWS, Azure, and Kubernetes environments.

Engagement Objectives

- Deploy and configure Cloud Security CNAPP Toll with account hierarchies, user roles, and SSO foundations
- Onboard and monitor AWS and Azure environments, including over 35 AWS accounts and 11 Azure subscriptions
- Surface identity and permissions risks using CIEM (Cloud Infrastructure Entitlement Management) capabilities
- Review compliance posture against CIS, NIST, PCI, NYDFS, and other standards
- Train and enable Health Care Organization's internal team to operationalize the platform and plan for future expansion

Strategic Priorities

- **Unify Visibility Across Cloud Providers:** Health Care Organization required centralized insight into its cloud estate to reduce silos between cloud accounts, subscriptions, and Kubernetes

clusters—ensuring that both identity risks and misconfigurations could be tracked from a single pane of glass.

- **Identity and Access Governance at Scale:** The security team aimed to map federated user access, privilege inheritance, and excessive permissions to reduce potential exposure from over-entitled roles and unused credentials.
- **Streamline Audit and Compliance Monitoring:** Compliance with frameworks like CIS, NIST, and PCI was a high priority. The organization sought to automate posture checks and begin reporting findings proactively to internal audit teams.
- **Operational Enablement and Workflow Integration:** The goal was not only to configure the platform, but also to equip the security team to interpret, prioritize, and respond to findings—while laying the groundwork for integrating with systems like Splunk, Jira, and ServiceNow.

Approach

We followed a phased, hands-on delivery model tailored to the organization's cloud maturity and future roadmap. Sessions were conducted remotely and designed to ensure platform configuration, knowledge transfer, and strategic alignment.

1. Identity Setup and Architecture Configuration

- Created four local users: Admin, Admin/Owner, and two Read-Only roles
- Enabled authentication integration via **Entra ID** (formerly Azure AD), preparing for SSO onboarding into CNAPP Tool
- Established a default account hierarchy with clear paths for future folder segmentation based on business units or compliance zones

2. Cloud Provider Onboarding

- **AWS:** Connected to one AWS Organization with **35+ accounts**, using a read-only role (CSPM Role) for posture assessment
- **Azure:** Onboarded two Azure tenants with a total of **11 active subscriptions**
- Validated telemetry flow, account metadata, and resource visibility across all regions and services

3. Kubernetes Inventory and Visibility

- Detected one **Azure Kubernetes Service (AKS)** cluster via cloud provider monitoring
- While Helm-based onboarding was not completed during the engagement, compliance scans were proposed to extend visibility into Kubernetes worker nodes in the near term.

4. Risk Analysis and Console Enablement

Asset Inventory & Findings Review:

- Explored inventory views by provider, region, service, and risk level.
- Conducted interactive sessions on:
    - Filtering assets by misconfiguration severity, compliance status, or resource type
    - Investigating misconfigurations (e.g., overly permissive IAM roles, unencrypted storage, public access)
    - Using snooze, ignore, and remediation workflows for triage and task management

IAM Governance with CIEM:

- Delivered a walkthrough of **Cloud Infrastructure Entitlement Management (CIEM)** features
- Queried federated user permissions and mapped privilege paths across multiple accounts
- Identified:
    - Roles with excessive privileges (e.g., iam:PassRole, ec2:CreateSnapshot)
    - Inactive users with high-risk entitlements
    - Federated access risks and lateral movement paths

Policy Management & Alerting:

- Reviewed active and template-based policies for threat detection
- Explained alert forwarding workflows to Splunk and ticketing integrations with Jira and ServiceNow (integration not implemented yet, but planned)
- Introduced custom policy creation to define rules based on Health Care Organization's risk tolerance (e.g., tag compliance, public-facing assets, privileged users)

Compliance Frameworks:

- Mapped assets and findings against built-in benchmarks:
    - CIS AWS / Azure Foundations
    - NIST 800-53
    - PCI-DSS v3.2
    - HIPAA
- Explained how to modify, extend, or bundle policies into custom frameworks to align with internal controls

Reporting & Output:

- Reviewed PDF and CSV export options, filtered reports, and dashboard snapshots
- Scheduled daily and weekly reports for executive summaries and team-specific overviews

Additional Insights & Future Roadmap

- **IaC and CI/CD Integration:** While not deployed during the deployment, discussions covered scanning for GitHub, GitLab, Jenkins, and Terraform Cloud pipelines to “shift security left” in future phases
- **Workload Protection:** Cloud VMs are now being scanned to address runtime risk. Deeper container scanning will be addressed as workload protection modules are evaluated for in-account deployment
- **Planned Enhancements:**
    - Create custom folders in the Cloud Security Tool hierarchy to reflect business structure
    - Enable SSO through Cloud Security Tool once Entra ID federation is finalized
    - Activate Jira and Splunk integrations for real-time remediation workflows
    - Roll out policies targeting encryption, tagging compliance, and shadow IT detection

Results & Impact

- **Complete Cloud Posture Visibility Achieved:** Health Care Organization now has unified access to all cloud accounts and subscriptions, enabling fast detection of misconfigurations and compliance gaps
- **Identity Risk Reduced:** Teams can now investigate privilege inheritance, analyze access paths, and identify excessive or unused entitlements—especially for federated identities
- **Audit Readiness Accelerated:** Mapped compliance controls across multiple standards allow internal audit and GRC teams to monitor posture continuously
- **Operational Team Empowered:** Analysts and engineers can now take action within the platform—from assigning remediation to exporting filtered findings and preparing strategic reports
- **Scalable Foundation Established:** With strategic guidance and clear documentation, the customer is prepared to expand platform adoption into CI/CD, third-party alerting, and deeper workload protection

Customer Feedback

“The deployment provided both technical depth and operational clarity. It helped us move from static configuration to active cloud risk management in just five days. We’re now positioned to scale cloud security across our organization with real visibility and confidence.”
— **Cloud Security Lead**, Health Care Organization.

Address:
1000 Brickell Av, Suite 1015
Miami, FL 33131

Phone:
+1 (786) 397-0480

Maill:
info@mpivpartners.com