nClouds | AWS Case Studies

UpEquity

How nClouds helped fintech UpEquity build out a well-architected multi-account strategy on AWS that is PCI-compliant.

UpEquity

Industry

Financial Services, Fintech, Real Estate, Mortgage

Location

Austin, TX

Challenge

Build out a well-architected multi-account strategy on AWS that is PCI-compliant.

Featured Services

AWS Well-Architected Framework, DevOps Services, Security, Consolidated Billing, AWS Control Tower

About UpEquity

UpEquity's mission is to transform the home-buying experience by giving every person the opportunity to make a competitive, winning offer on their dream home. Its Buy with Cash program helps homebuyers make an all-cash offer that's 4X more likely to be accepted than traditional mortgages. UpEquity's differentiated mortgage technology works at superhuman speed to provide a painless, fast mortgage experience for its customers. The Austin-based firm has experienced 9X growth in the last year and carries a Net Promoter Score 3X the industry average, further highlighting the company's truly unique approach in an otherwise saturated market. For more information about UpEquity, go to: upequity.com

Benefits Summary

Automation for accelerated innovation

Cost optimization

Enhanced compliance, security, and governance

CHALLENGE

Build out a well-architected multi-account strategy on AWS that is PCI-compliant.

UpEquity needed an uncomplicated way to govern multiple AWS accounts, easily provision/decommission AWS accounts, and maintain Payment Card Industry (PCI) compliance.

Why AWS and nClouds

UpEquity wanted to launch its mortgage platform quickly and needed a dependable partner to get its AWS environment off the ground. The VP of Engineering had engaged nClouds engineering experts at his previous company. He was impressed by the sales team's professionalism, efficiency in delivering the SoW, honesty, and knowledge of AWS. He admired the quality of nClouds' work and invited them to be UpEquity's Managed Service Provider (MSP) for ongoing DevOps services.

UpEquity leveraged several Amazon Web Services:

- **Amazon GuardDuty** - A managed threat detection service that provides UpEquity with an accurate and easy way to continuously monitor and protect its AWS accounts and workloads.
- **AWS CloudTrail (CloudTrail)** - For governance, compliance, operational auditing, and risk auditing of the AWS account.
- **AWS Config** - A service that enables UpEquity to assess, audit, and evaluate the configurations of AWS resources.
- **AWS Control Tower** - Automates the set-up of a baseline environment, or landing zone, that is a secure, well-architected multi-account AWS environment.
- **AWS Organizations** - Provides policy-based management for multiple AWS accounts.
- **AWS Single Sign-On (SSO)** - Makes it easy to centrally manage SSO access to multiple AWS accounts and business applications.

> "nClouds built a solid architectural foundation for the launch of UpEquity. They applied their deep AWS experience and DevOps skills to support our rapid growth and innovation."
>
> **Jeff Boone,**
> Director Of Engineering, UpEquity

UpEquity's solution stack also included additional, essential third-party tools:

- **Google Workspace (formerly known as G Suite)** - A suite of web applications created by Google for businesses.
- **HashiCorp Terraform** - An infrastructure-as-code (IaC) tool that allows UpEquity to create, update, and version its AWS infrastructure.

nClouds' Solution Architecture for UpEquity:

UpEquity's mortgage application was in a proof-of-concept stage when they approached nClouds to build the foundation of their AWS infrastructure to support that application. nClouds recommended a multi-account strategy to enable UpEquity to support innovation and agility, group workloads based on business purpose and ownership, apply distinct security controls by environment, constrain access to sensitive data, and limit the scope of impact from adverse events. nClouds applied best practices of a well-architected multi-account AWS environment by implementing AWS Organizations.

AWS Organizations comprises organizational units (OUs), logical groupings of accounts organized into a hierarchy that enable UpEquity to apply management controls. In this solution, there is one OU for each environment and one core OU that groups accounts together to administer as a single unit.

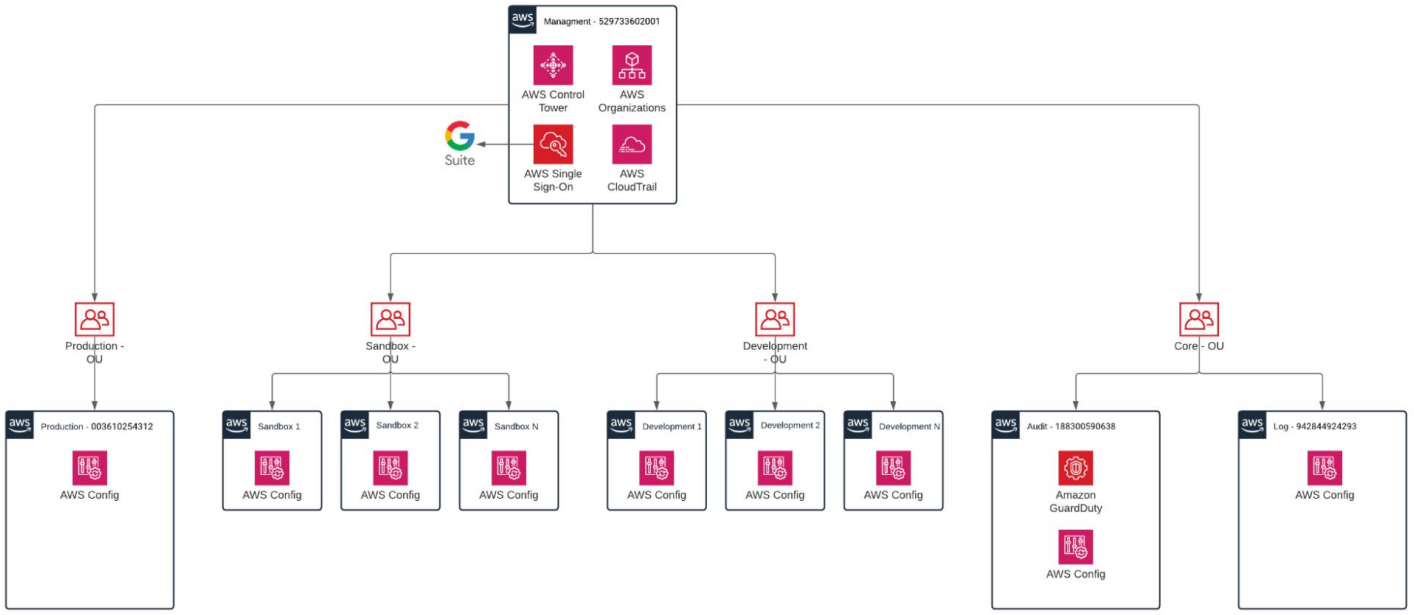
- The **core OU** includes an audit account and a log account. The audit account manages policies and permissions, and the log account handles all the application and infrastructure logs generated by the other accounts.

- A **sandbox OU** holds AWS accounts that individual developers use to experiment with AWS services.
- The **development OU** contains accounts in the dev and test environments.
- The **production OU** contains accounts for the production environment.

The consolidated billing feature of AWS Organizations provides UpEquity with one bill for multiple accounts and easy tracking of charges across multiple accounts. It enables UpEquity to optimize costs by combining the usage across all accounts in the organization to share volume pricing discounts, Reserved Instance discounts, and Savings Plans.

A management account has control over security, infrastructure, and finance policies. In this solution, the management account includes AWS Organizations, AWS Control Tower, AWS SSO, and CloudTrail. AWS Control Tower automates the setup of an overall multi-account environment called a landing zone, and it easily integrates with AWS Organizations. AWS SSO handles the user's access using Google Workspace as the identity provider. Account Factory, a product in AWS Service Catalog, provisions new accounts and enrolls existing accounts in the landing zone. Terraform templates spin up all the resources and services.

High-level architecture diagram:



The Benefits

Teaming with nClouds, UpEquity now has a best-practices well-architected multi-account environment. The project has yielded numerous benefits:

Automation for accelerated innovation

AWS Control Tower's automation and governance model saves UpEquity time and effort, so their engineers can focus on innovation. It automatically provides ongoing policy management. Its prebuilt multi-account framework with a predefined OU structure creates new accounts and provisions resources quickly. While AWS Control Tower enables automated setup of AWS environments, it also enables UpEquity to customize its functionality based on business needs and an ever-changing economic environment. Account Factory automatically applies resources and roles to newly created accounts and enrolls existing accounts in the landing zone. Terraform's IaC automates infrastructure deployments and configurations.

Cost optimization

Besides the obvious advantage of receiving a single bill and having easy tracking for multiple accounts, AWS consolidated billing enables UpEquity to optimize costs. It combines the usage across all accounts in the organization to share volume pricing discounts, Reserved Instance discounts, and Savings Plans.

Enhanced compliance, security, and governance

Financial institutions such as UpEquity must put in place comprehensive internal controls and supporting documentation to achieve PCI compliance. UpEquity's multi-account environment enables them to create grouping mechanisms to ensure that accounts meet PCI compliance requirements.

In a multi-account environment, accounts act as containers with resources used for a common purpose. So in the event of a security issue or misconfigured resource, the blast radius is reduced to a single account. In each of the accounts, AWS Config detects and provides mitigation recommendations for incorrectly configured resources.

In the management account, AWS SSO provides access boundaries across accounts by setting up custom permissions to accounts in UpEquity's organization using Google Workspace as the identity store. CloudTrail monitors events for each account and delivers those events as log files.

In the core OU, the audit account performs cross-account auditing and centralized security operations. The log account handles the application/infrastructure logs generated by the other accounts. Amazon GuardDuty detects unexpected and potentially unauthorized and malicious activity in the AWS environment.

AWS Control Tower sets up guardrails, high-level rules for ongoing governance that limit actions based on UpEquity's policies and detect non compliant resources. Guardrails are implemented in AWS Organizations' service control policies (SCPs). SCPs are highly customizable programmatic boundaries for service actions in individual accounts and OUs. AWS Control Tower's integrated dashboard provides alerts on noncompliant resources that need to be remediated.