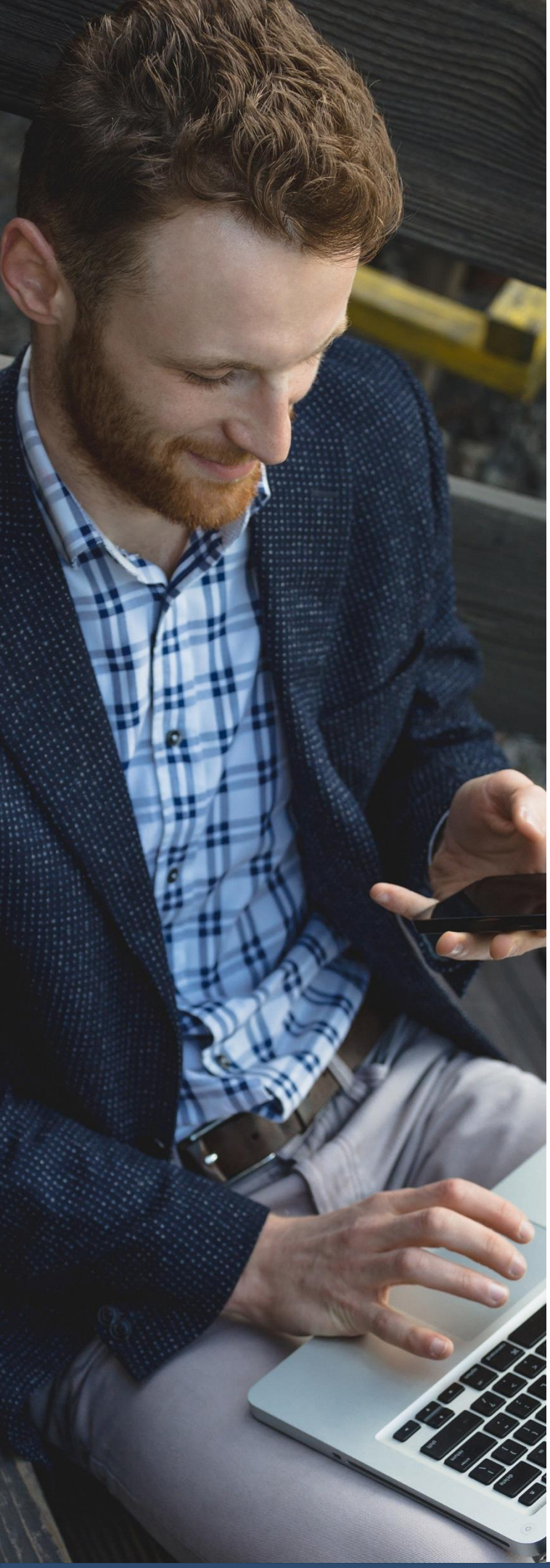
Finagraph

Security Overview

Finagraph's security program is designed to keep customer information safe and secure

October 2020



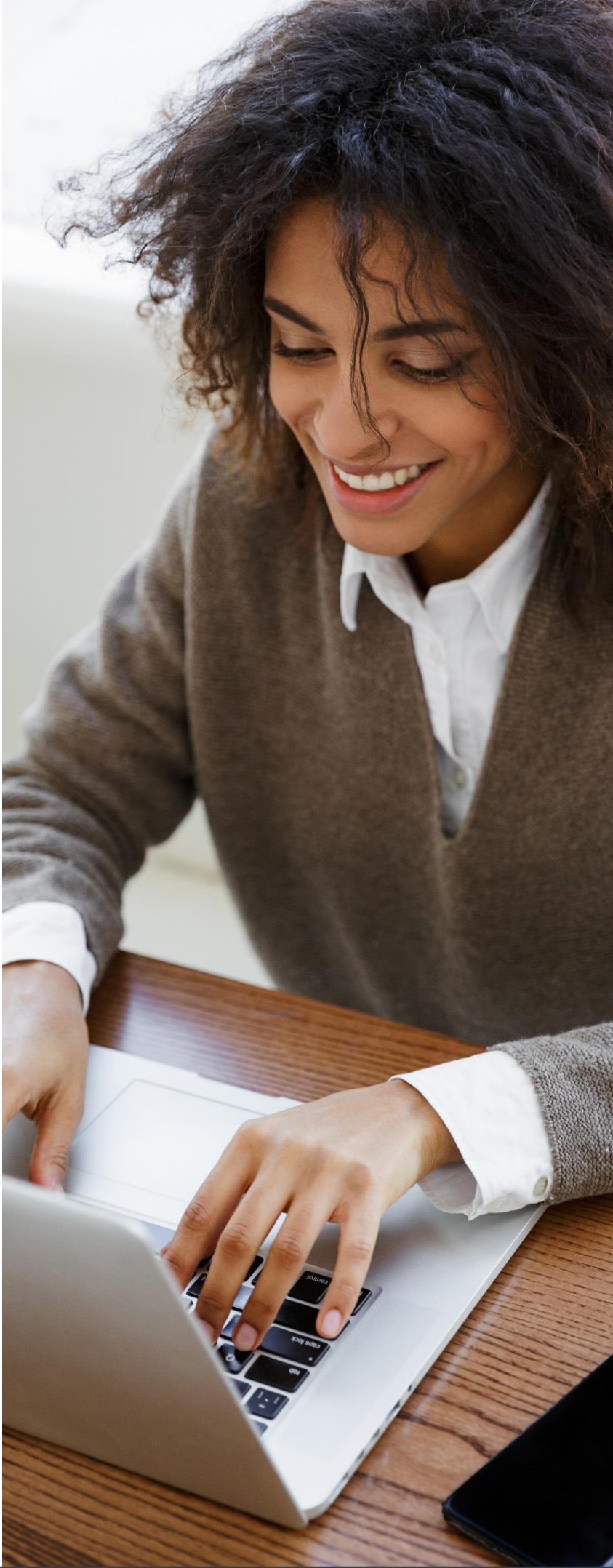
CONTENTS

Security First

Security is more important now than ever and at Finagraph, we have not only built all of our products and services with security technologies as the foundation, but also built our organizational culture with security in mind.

Our overarching goal is to help every business eliminate cash flow as a reason for failing and also radically streamline the banking and lending industry with breakthrough software and services.

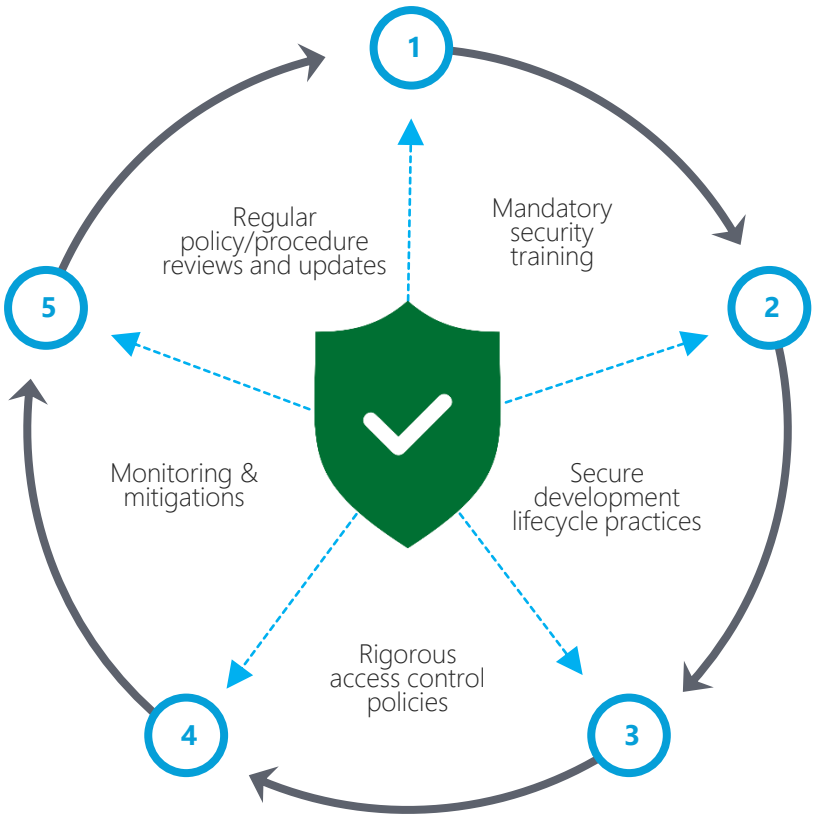
This document outlines how we engineer security practices and technology into our products so our customers can be confident they are safe and secure.



Finagraph: A Cohesive Security Culture

As an organization, Finagraph is focused on building a cohesive security culture that include processes and protocols to address:

- ✓ Data protection
- ✓ Incident management
- ✓ Business Continuity & Disaster recovery

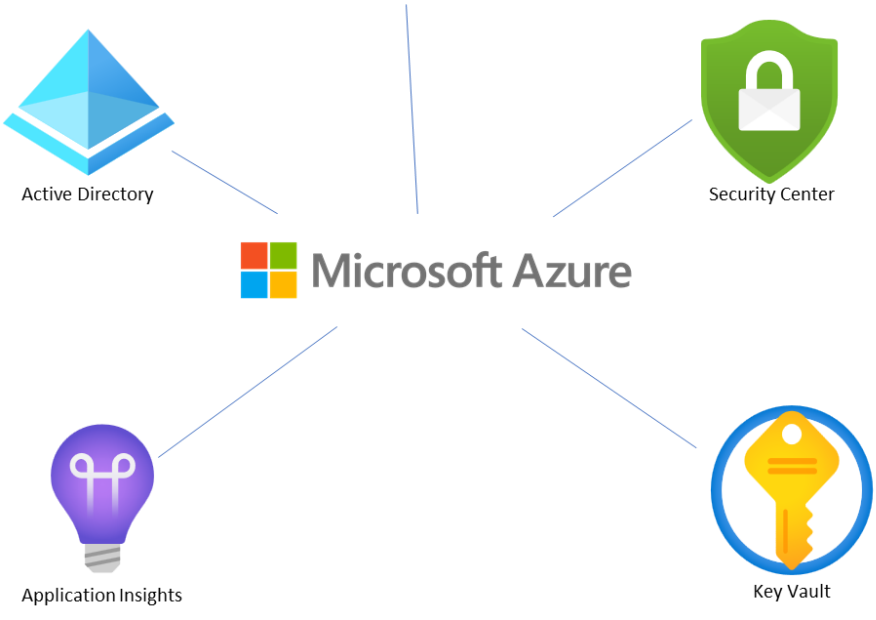


Secure Cloud Infrastructure

Finagraph products and services are built on Microsoft Azure as our premier secure cloud provider.

- ✓ Finagraph uses best-in-class secure cloud infrastructure provider, Microsoft Azure, to host the Strongbox platform
- ✓ Finagraph leverages years of security enhancements that Microsoft Azure offers with their Platform as a Service (PaaS) services to better protect against security incidents
- ✓ Finagraph uses automatic vulnerability assessments, advanced threat protections 24x7 allowing us to respond and resolve adverse events
- ✓ The Azure platform maintains regular, independent security audits including SOC I, SOC II, and SOC III

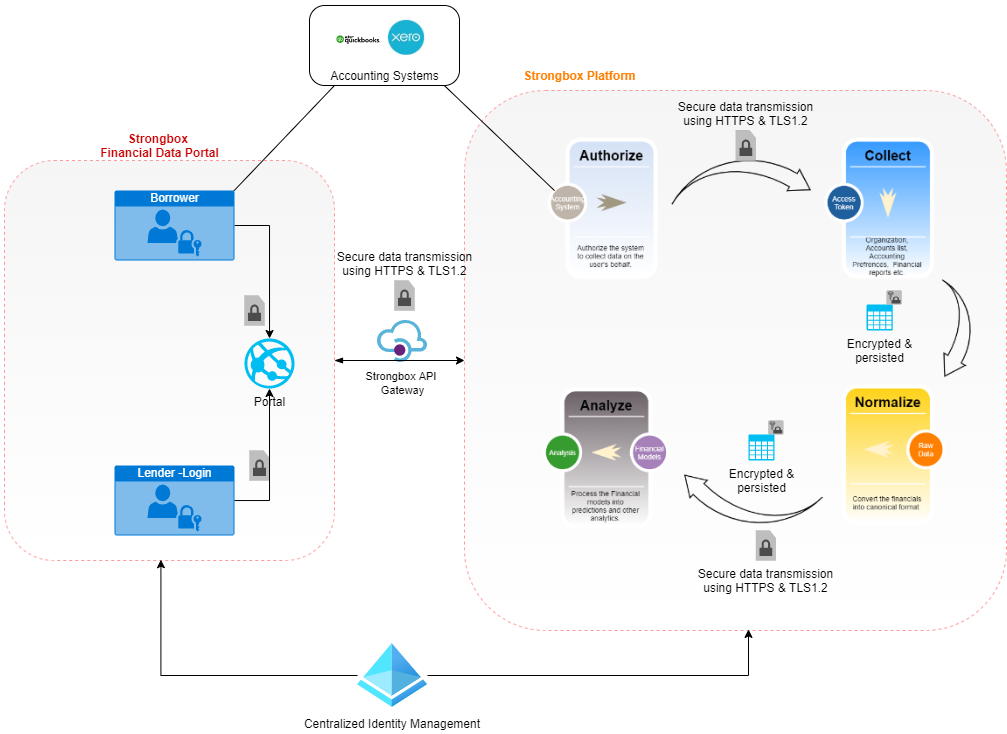
Microsoft Compliance offerings



Strongbox Secure Architecture

The Strongbox architecture implements industry best practices and secure patterns including, but not limited to the following:

- ✓ Data classification
- ✓ Centralized Identity management (for both users and applications)
- ✓ Data encryption during transit and at rest
- ✓ Data isolation



Finagraph STRONGBOX™

Data Classification

Data within the Strongbox platform is classified under the following:

- ✓ High Business Value
  (includes both restricted & confidential)
- ✓ Low Business Value
  (includes internal and public)

High Business Value Examples

- Data obtained from accounting system
- Any financial data derived from raw data
- Credentials, Access tokens, Refresh tokens, Certificates

Low Business Value Examples

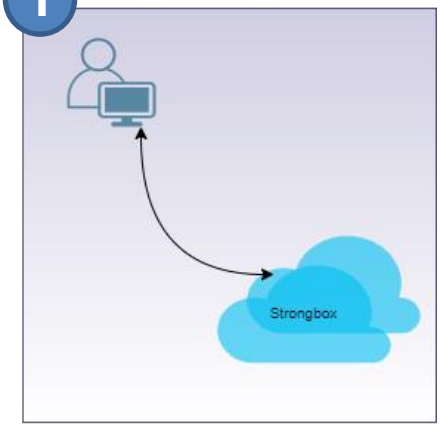
- Platform/product internal ids
- Any state management constructs

Finagraph STRONGBOX™

Data Encryption in all Finagraph Products & Services

The combination of the Advanced Encryption Standard (AES 256) and Transport Layer Security (TLS) help keep sensitive data safe in these scenarios:

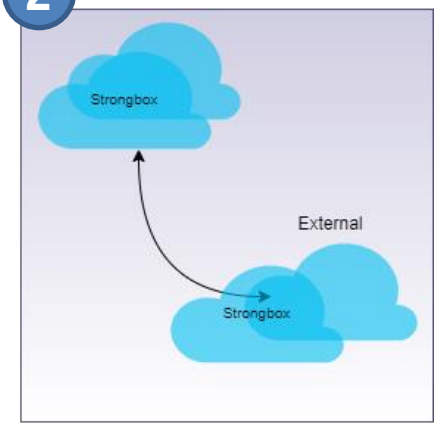
1



Data in transit between customer & Strongbox*

Any/all communication between customers and Finagraph services

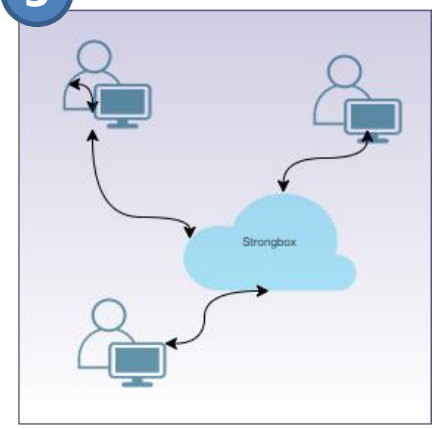
2



Data transfer between Strongbox components and any external services*

Any communication both internal –> internal and internal –> external uses HTTPS. And, high business value data is encrypted at rest and in-transit using AES 256 and Transport Layer Security (TLS1.2+)

3



Data isolation in multi-tenanted scenario*

As a multi-tenanted solution all customer data is isolated by customer (aka tenant) to add an extra layer of protection

* This applies to all Finagraph Products and Services

Strong Authentication

Secure Monitoring

Strong Authentication

- ✓ Finagraph uses industry-leading identity providers such as Auth0 for our identity and authentication management in our products.
- ✓ We adhere to the best-in-class compliance frameworks to ensure information security across the board.

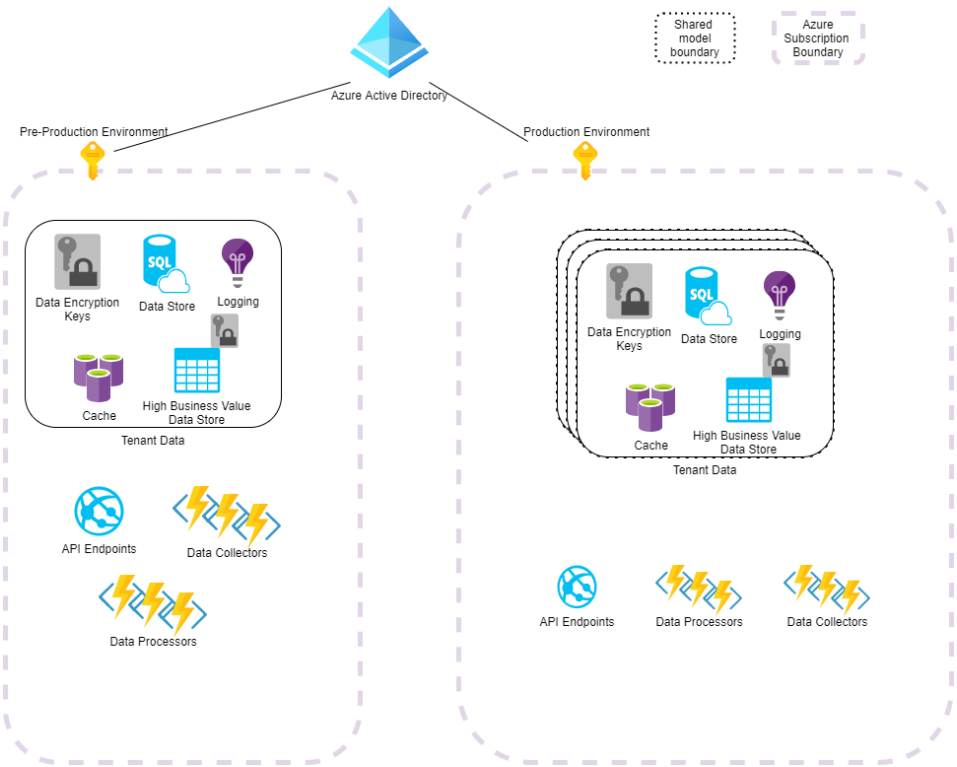
Secure Monitoring

Finagraph continuously monitors with our 24/7 on-call team to help rapidly respond and resolve critical issues. As an organization, Finagraph is focused on building a cohesive security culture that include processes and protocols to address:

- ✓ Data protection
- ✓ Incident management

Data Isolation

- ✓ Data isolation across pre-production and production environments is enabled by using Azure Active Directory & Role Based Access Control (RBAC) to ensure there is no cross-contamination of test data and customer data.
- ✓ In addition, to limit exposure between tenants, Strongbox also uses a ConsumerId (aka TenantId) discriminator to isolate tenant specific data.



Threat Detection & Mitigation Process

- ✓ We use Azure Security Center as our centralized solution for strengthening our security posture across our infrastructure
- ✓ With Azure Defender we leverage the continuous vulnerability assessments, threat protection capabilities to protect the resources & workloads

Business Continuity/ Disaster Recovery

Finagraph's business continuity planning covers a broad range of organizational and product process to ensure seamless customer experiences, secure data backup and safe workplace practices in the event of a disaster or emergency.

Some of the processes we have in place include:

- ✓ Automatic data backup with point-in-time restore for up to 35 days, and long-term retention
- ✓ Locally redundant storage through the Azure Storage platform.
- ✓ Infrastructure provisioning and management using declarative models to enable easier recovery in an alternate Azure Datacenter
- ✓ Comprehensive communication and information distribution

SOC II Audit

SOC II Audit

Finagraph completes a SOC II Annual Audit each year. Finagraph's comprehensive security policies are monitored for compliance and updated regularly to maintain up-to-date industry best practices to meet the current security needs of our clients.

Finagraph's policy library includes:

- ✓ Security Policy
- ✓ Privacy Policy
- ✓ Business Continuity Plan
- ✓ Secure Development Process
- ✓ Data Management Policy

Independent Security Testing

Independent Security Testing

Finagraph participates in regular penetration testing and vulnerability assessments completed by third-party security experts to help us maintain a resilient information security program. Each component of our product is tested to ensure:

- ✓ Confidentiality – protecting sensitive information from unauthorized users
- ✓ Integrity – protecting information from being tampered with
- ✓ Availability – providing access to information when needed

Microsoft Azure

Security links for more information

Azure Security Fundamentals

Access

docs.microsoft.com/en-us/azure/security/fundamentals

Azure Security Advantages of PaaS

Access

docs.microsoft.com/en-us/azure/security/fundamentals/paas-deployments

Azure Security Center

Access

azure.microsoft.com/en-us/services/security-center

Azure Defender

Access

azure.microsoft.com/en-us/services/azure-defender