How secure is my data?

An overview of Finscape information security controls and policies

Background

Finscape is a Business Intelligence system which contains sensitive sales data gathered from leading investment providers and distributors. Naturally, those organisations want to be confident that the data they contribute remains secure and confidential. This datasheet provides an overview of the systems and controls which Finscape has implemented to protect our clients' data and to ensure it remains secure at all times.

The document is not intended as a substitute for technical due diligence and Finscape is happy to cooperate with your infosec team to provide detailed answers to their questions. It is also worth noting that the Finscape data agreement contains robust contractual safeguards around confidentiality and privacy.

Engineering quality

Finscape system development has been undertaken by Altus, an ISO27001 certified software developer with a 15-year record of delivering secure, operational systems for the investment industry. Altus was a spin-off from Bath-based IPL Systems who specialised in safety-critical, real-time software for the military and telecommunications sectors; Altus was founded with the explicit aim of bringing the same engineering quality to financial services.

Altus systems are used by over 200 of the UK's largest investment providers and distributors to trade and transfer assets worth billions of pounds. Those systems are characterised by high availability, straight-through processing and very low error rates – all qualities which have been core to the design of Finscape.

System Design

Security and confidentiality has been designed into Finscape from the outset. Clients can see their own data in fine, granular detail but will only ever be presented with an aggregate view of the rest of their relevant market. The ability for clients to define their own more focused market cohorts is on our development roadmap but this will be closely managed and monitored to ensure it is never possible to identify data specific to one competitor.

Finscape has been explicitly designed to comply with GDPR regulation. The system takes a weekly feed of the FCA base register and supplements this with additional data via API calls to the relevant FCA service. The FCA information on distributors is further enriched via our own proprietary research which captures publicly available data such as organisational hierarchies and individual contact details via firms' own websites.

Hosted Environment

The system runs via Amazon Web Services (AWS) in a virtual private cloud where AWS operates, manages and controls the components of the virtualization layer down to the physical security of the facilities in which the service operates. AWS provide 24/7/365 support for the hosting infrastructure and work closely with the Altus Support team to manage any service issues.

The Hosted Environment infrastructure is located in AWS secure data centres with no public access, 24 hour video surveillance and 24 hour on site security personnel.

Network access to the service is restricted by:

- Firewall IP whitelisting allowing access only from Altus and client IP addresses via the appropriate port
- GlobalSign issued certificate to authenticate over https
- Unique digital certificates provided to each client and validated by Apache
- Client Id, user name and password validated by the application

All client data is encrypted in transit to and from the Hosted Environment and on database servers in a separate firewalled network segment. All Internet communication is encrypted using SSL and all service requests are handled by Apache and proxied through to Microsoft IIS.

Administration access is supported by VPN service. Only personnel directly involved in support of the Hosted Service are permitted access. Any personnel accessing the servers use individual multi-factor login credentials governed by password complexity and rotation policies. No access to customer data is available to AWS support staff.

Monitoring and Audit

Netwrix Auditor is installed to ensure that members of staff with access to the Hosted Environment cannot interrupt its operation or delete any stored entries. When an approved administrator accesses the Hosted Environment, they are presented with a warning reminding them that their activity is being recorded and that they need to specify their ticket reference when prompted to do so.

All administrative interaction with the Hosted Environment is retained in a searchable video archive allowing precise examination of all actions performed for both compliance and forensic purposes. These logs are retained for two years.

Netwrix Auditor supports the configuration of automated alerts triggered to help identify suspicious activity such as failed SQL logins, change of file share permissions, account creation etc. Such actions result in e-mail alerts being sent to a distribution list including the Risk and Compliance Manager.

Regular penetration tests are carried out by an independent third-party specialist including specific objective tests to verify the segregation of data within our services.

A monthly compliance check is performed to ensure that access is compliant with our policies and procedures. Should any anomaly or non-conformity be discovered, an Incident Report is raised. Depending on the incident root cause, action will be taken, up to and including disciplinary procedures.

Resilience

AWS data centres are powered from commercial utility underground conduits with UPS and diesel generator backup. Each data centre has multiple Tier 1 Internet links plus dual redundant network infrastructure. All equipment is monitored 24 hours a day by AWS Cloudwatch software.

All hardware is replicated across AWS availability zones which are independently powered and cooled, and have their own network and security architectures. In the event of a complete failure of primary availability zone, which in itself comprises multiple facilities, we will manually switch over to infrastructure in the secondary availability zone. Server failover is regularly tested by Altus.

Data recovery measures include:

- Daily differential and weekly full operating system and database backups managed by AWS, encrypted and stored in secure offsite backup facility.

- Database log shipping every minute to DR infrastructure to enable rapid point in time recovery.

People

Finscape operates rigorous staff vetting procedures with checks carried out both before and during employment. Staff undergo continuous Data Protection and Information Security training and assessment. Access to the Hosted Environment is strictly limited based on valid business requirements.

The operation of Altus hosted services and the activities of staff are governed by a set of Information Security policies. These policies ensure all staff understand their responsibilities in protecting clients’ data and maintaining our very high standard of Information Security. Policies are reviewed at least annually and are readily available on request.