Fintel Technologies, Inc.

Security White Paper

August 2018

Executive Overview

The Fintel Platform is a Software-as-a-Service (SaaS) product designed to assist financial institutions in optimizing and managing their existing fraud and anti-money laundering compliance programs by allowing them to communicate and share information with counterparties. Fintel realizes that protecting customer data, ensuring proper security procedures, and mitigating any potential risk is essential to providing a trusted service that can be relied upon by financial institutions. Fintel takes a risk-based approach to security, and this paper outlines the measures that have been adopted to protect the data that is sent over the Fintel Platform.

Multi-Layer Security

Fintel recognizes that an effective security program cannot exist solely at a single layer of operation. As such, we take a security-first approach at all levels of the organization, from a Policy and Process perspective, through the Physical and Infrastructure layers, and into the Application and Product development spheres, where user and transactional data is processed.

Policy and Process

The first layer of defense in any security apparatus consists of having a comprehensive set of security processes and policies in place to ensure the protection of customer data, and that staff and contractors who have access to that data receive adequate training in the operation of those policies. Fintel's policies are designed to be in-line with many of the best practices and standards that have been published regarding data security, including the Cloud Security Alliance's STAR Framework and the ISO-27001 requirements.

Training

All Fintel Technologies employees undergo periodic training to ensure a security-first approach to their handling of customer data. Additionally, all contractors who could potentially access live customer data, are required to sign non-disclosure agreements and certify that they enforce security policies and procedures at least as stringent as those implemented by Fintel.

Authorized Access

Access to customer and transactional data is enforced on a least-privilege basis. Only the minimum number of accounts necessary to ensure the effective operation of the Fintel services are provided access to secured data. All employee and contractor accounts which have access to secured data are regularly reviewed both on a periodic basis and whenever an employee or contractors role within the company changes.

Change Control

Formal change control processes minimize the risk associated with system changes. All changes to the system, at both the infrastructure and application layers, are tracked and risk-analysis and quality assurance processes are executed before any change is applied.

Physical and Infrastructure

Fintel Technologies incorporates security conscious decision-making into the selection of all vendors, including those that provide physical office space and equipment as well as virtual computing services. Infrastructure policies require the use of firewalls at all ingress and egress locations, as well as the use of Unified Threat Management (UTM) systems. All customer access to the Fintel Platform is controlled through user interfaces (UIs), application-programming interfaces (APIs), or dedicated tools. Use of any of these methods of access requires a username and password with privileges appropriate for the requested access.

Networking

All network access to virtual hosts is protected by specific security groups dependent on the services provided by that host. Obtaining access to any host cannot be accomplished over an unencrypted/unsecured connection. Separate virtual private clouds (VPCs) are used to split production, staging, testing, and development environments as well as to segregate end-user and administrative traffic.

Security Patches

Fintel Technologies has a robust policy in place regarding security updates to all of its infrastructure components. Operating systems, databases, middleware, and application components are updated regularly using a risk-based approach considering vendor recommendations for criticality.

Application

The Fintel applications provide users with the ability to access data provided directly for their own use, or by another institution which has explicitly provided data in a sharing capacity. Fintel employs many security measures to ensure that the data provided to the application follows a secure flow from when loaded into the application through delivery to the end-user.

Encryption in Transit

All traffic into and out of the Fintel application is performed over HTTPS and is encrypted using a TLS protocol that leverages either the SHA-2 or AES algorithms.

Encryption at Rest

All data stored in the Fintel application is additionally encrypted at rest within the Fintel data services, including in any fault-tolerant system backups.

Integrations

All integrations with the Fintel systems are provided using an API which leverages HTTPS over the TLS protocol. The user security model is enforced at the API level and requires pre-registration with Fintel Technologies and the acquisition of an application specific key, allowing non-conforming integrations to be individually disabled without affecting the rest of the system.

Session Expiration

The Fintel Applications and API integrations all have session expiration timeouts, which require users to periodically re-authenticate.

Vulnerability and Penetration Scans

Fintel periodically performs OWASP compliant penetration testing and vulnerability scans of its infrastructure and software. Defects uncovered by these scans are flagged as highest-priority in the product development pipeline and remedied within the application or infrastructure on risk-sensitive timeline.

Additional Compliance Safeguards

In addition to the many layers of security measures described in this document, Fintel Technologies implements many additional security and compliance measures to support the needs of our customers.

Conclusion

At Fintel Technologies, we pride ourselves on the stance we take towards protecting our customers' data and we continually stress that a mature security apparatus requires coordination across all aspects of the organization, not just the technology arm. We want our customers to know that our approach protects their data, and that we will continue to evolve our policies and safeguards as newer technology becomes available.