

Security for Hosted Services and Technology

A comprehensive program to protect your most sensitive data

apexanalytix firststrike[®] software saves companies billions, every year, by identifying duplicate payments, overpayments, missed credits and fraud. Our apexportal[®] software is used for supplier onboarding and vetting, for ensuring global regulatory compliance and for continuously monitoring and improving your vendor master data. If you purchase our SaaS software, you can trust that we use the most rigorous of controls to protect your data from both unauthorized access and unexpected outages. Our SSAE 18-compliant data center features a highly reliable, redundant architecture with instant failover capability and one of the most comprehensive security programs in the industry.



PHYSICAL SECURITY

The protection we offer at our state-of-the-art data center begins with a strong set of physical controls. There is a single, highly protected point of entry that requires both a card key and authentication by two biometric factors (fingerprint and an iris scan). Security guards actively patrol the facility and surrounding property around the clock. In addition, there are more than 100 closed-circuit video cameras covering the interior and exterior.



DATA SECURITY AND BACKUPS

Your data is stored by Apexanalytix on SQL servers utilizing encrypted storage. Server access is strictly limited. Access to our hosted applications is controlled by user ID, password authentication and role-based authorizations. In the event of a major disaster, apexanalytix maintains a full disaster recovery infrastructure in a secondary data center 300 miles away. Daily data changes replicate automatically to the secondary data center and remain encrypted. All data is encrypted at rest. Incremental backups are performed daily, with full database backups each week to encrypted disk-based storage. They are then transferred into the apexanalytix Disaster Recovery data center. Long-term archives are encrypted and retained by our off-site technology partner. The complete backup of each month is stored off-site for one year and held in locked containers that can be opened only by authorized personnel.



SERVICE ORGANIZATION CONTROLS

We have completed a Service Organization Controls (SOC) 1, Type II Report for the apexportal and a SOC 2, Type II Report for the apexportal and firststrike.



DATA TRANSFER SECURITY

Data is transferred securely through the apexanalytix Managed File Transfer (MFT) System. You can choose from multiple secure transfer protocols, such as AS2, AS3, HTTPS/TLS and SFTP. Access to the MFT server and to client-specific folders requires an account and password. Data is never stored on the MFT system itself.



NETWORK SECURITY

Our network infrastructure is based on enterprise-grade switches, routers and firewalls. All communications—including login, file transfer and application access—are encrypted using 2048-bit SSL certificates. Access is controlled by Active Directory with passwords that meet rigorous requirements for complexity. Both network and server security logs are monitored for potential vulnerabilities.