**Security Management / Cybersecurity Suite**

* **Fort Knox System**: This system includes role-based access control, ensuring that each user only accesses the areas necessary for their job, along with auditing features that log every interaction with the system, making it tamper-resistant and easy to review for compliance and security.
* **Cloud Server Logs**: These logs record every action taken within the AngelTrack system, including user access and data modifications. The logs are securely stored in the cloud, providing a reliable audit trail that helps detect unauthorized activities and ensures accountability.
* **HIPAA Journal**: The HIPAA Journal tracks and records every interaction with patient records, ensuring full compliance with HIPAA requirements. It keeps a detailed history of who accessed or modified patient data, making it easy to review for privacy concerns and regulatory compliance.
* **AngelTrack’s Mark**: This feature is a security mechanism that assigns a digital fingerprint to all significant actions within the system. It creates an audit trail that helps track and review system usage, ensuring that all activities can be traced back to the responsible user.
* **TimeClock Security Feature**:
	+ **IP Tracking**: This feature ensures that clock-ins and clock-outs occur only from authorized IP addresses, adding a layer of security by confirming that employees are accessing the system from recognized locations.
	+ **Terminal System**: The Terminal System restricts time clock access to specific devices, preventing unauthorized clock-ins and ensuring that timekeeping records are secure and accurate.
* **2FA (Two-Factor Authentication)**: Two-Factor Authentication enhances login security by requiring users to verify their identity through an additional method, such as a code sent to their phone, reducing the risk of unauthorized access.
* **Biometric System**: AngelTrack integrates with biometric systems to use fingerprint or facial recognition for securing access. This system ensures that only authorized personnel can access sensitive data and perform critical functions within the platform.
* **Role-Based Access Control**: This system is designed to limit access to specific features and data based on a user’s role within the organization, ensuring that employees can only access information necessary for their job responsibilities.
* **Exfiltration Tripwire**: The Exfiltration Tripwire monitors for abnormal data access patterns, such as large-scale data exports, and alerts administrators to potential security threats. This feature helps prevent data breaches by detecting unauthorized attempts to remove data from the system.

These features collectively ensure that AngelTrack offers a secure, compliant, and robust platform for managing EMS and Fire operations, protecting both sensitive data and system integrity.