CANDA Solutions
THINGS DONE

10500 Little Patuxent Pkwy, S. 620
Columbia, MD 21044

855.55.CANDA (22632)
info@candasolutions.com

ENTERPRISE INVESTIGATIONS MANAGEMENT

Delivering Enterprise Investigation Management by bridging the gap between the HR, Security, Insider Threat, Cyber and Physical activity to continuously deliver trust while minimizing organizational risk exposure.

FRESH HAYSTACK

INVESTIGATIONS MANAGEMENT
INDUSTRIAL / PERSONNEL SECURITY
INSIDER THREAT DEFENSE
CONTINUOUS ADAPTIVE RISK EVALUATION

October 2020

WfMC Awards for Excellence in Case Management WINNER 2017

Inc. 5000 HONOREE

2018 GREATER WASHINGTON INNOVATION AWARDS™ FINALIST

Gartner

WHY INVESTIGATIONS MATTER?

SUMMARY

Many organizations today are struggling with Enterprise-wide Personnel Risk visibility. To facilitate, centralize, improve and simplify cross-departmental process that consolidates alerts and cases into a single platform for timely and higher-quality Investigations Management.

Enterprise Risk Management across different parts of any corporation for a regrettably, multiple factors, including human ones, can generate a high-risk profile whether intentional or not. Enterprise Investigations Management (EIM) capability for Background Checks, Workplace Violence or Insider Threat investigations demand an integrated and collaborative top-down and bottom-up approach.

With limited budgets, resources, and legal/compliance issues, our solution addresses privacy, exponential growth of compliance requirements, cyber-attacks on Intellectual Property (IP), organizational guidelines / procedures and USG / DIB data losses resulting in the demand to process large volumes of heterogeneous data from diverse systems; all while maintaining resilience, security, sustainability and the proper levels of access control.

The Fresh Haystack (FH) platform addresses these unique challenges by orchestrating relevant data and alerts across distinct, overlapping functions of:

- ✓ Investigations Management
- ✓ Personnel / Industrial Security
- ✓ Cyber Security
- ✓ Physical Access
- ✓ HR
- ✓ Legal
- ✓ Continuous Vetting (CV)
- ✓ Counterintelligence (CI)
- ✓ Insider Threat Defense (ITD)

Both in-house misconduct and outside threats to your organization create the necessity for corporate investigations. Fraud and abuse could take various shapes, but corporate misconduct could significantly impact any size company. From the bottom line to your brand reputation, a corporate scandal could be detrimental to your Enterprise now and affect business in the future.

Better investigations allow to safeguard your proprietary information, confirm the trustworthiness of employees and partners, and maintain the security and safety of your company and employees. It is crucial that both proof and context are an important part of your investigation.

Solely gathering data to prove a certain action took place is simply not enough, you also need to have context of why it happened and understand collective risk activities to get a holistic view of critical programs and personnel, suppliers, subcontractors, vendors, cyber and physical security, assets, facilities and contracts.

Through its capability, FH leverages trust orchestration to quantify human generated risk in a non-evasive manner with the goal of tracking mitigation opportunities across your organizations. This allows management actions on anomalies via case management, investigations, and reporting.

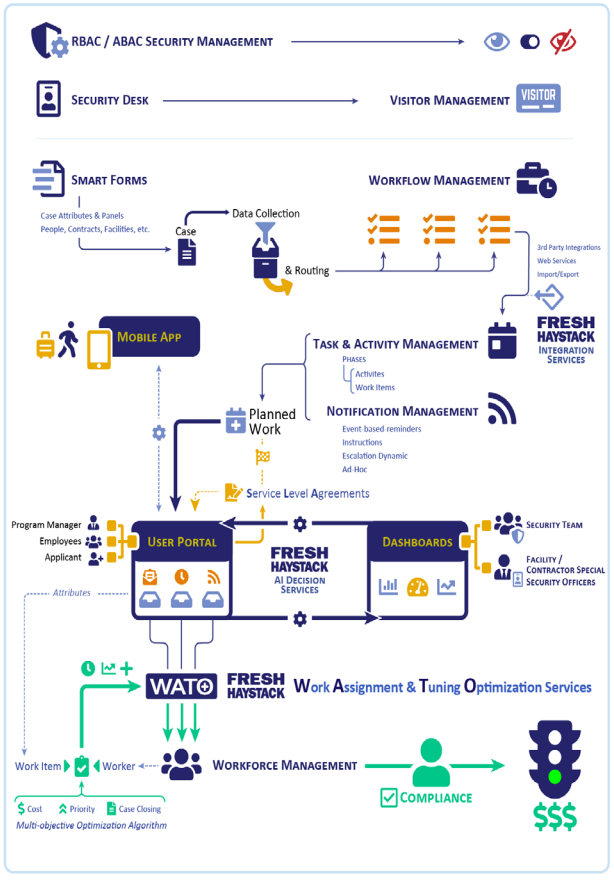
SCHEDULE A DEMO

OVERVIEW

Fresh Haystack (FH) is the first commercial robust case management platform designed specifically to address Integrated Risk Management for the Enterprise by combining Industrial/Personnel Security, Insider Threat Defense and Investigations Management in a risk-based, analytical decision making via aggregating relevant inside and outside of work data to protect Government and Corporations, bringing risk visibiltiy to the decision makers. CANDA has been enhancing its case management platform for various Investigations Service Providers (ISPs) since early 2010 with focus on multiple case types and workflows for Agencies with delegated background investigation authority. As such, we have focused on end-to-end investigative case management. Throughout this time, we have collaborated with various personnel security and investigations SMEs including retired government and industry executives to automate and eliminate much of the inefficiencies in these investigations with the focus on increasing ISP productivity, improving speed and timeliness while decreasing the underlying cost of each investigation.

This has resulted in a modular platform that contains core BI (Background Investigation) case management services that can be configured and tailored to meet core investigative functions but flexible enough to apply Agile development practices to address specific business requirements and complex integration touchpoints. The platform is provided Software as a Service (SaaS) or on-premise to the industrial security community today hosting up to Controlled Unclassified Information (CUI) level. Examples of existing core case management functions within Fresh Haystack are:

FRESH HAYSTACK CASE MANAGEMENT SYSTEM



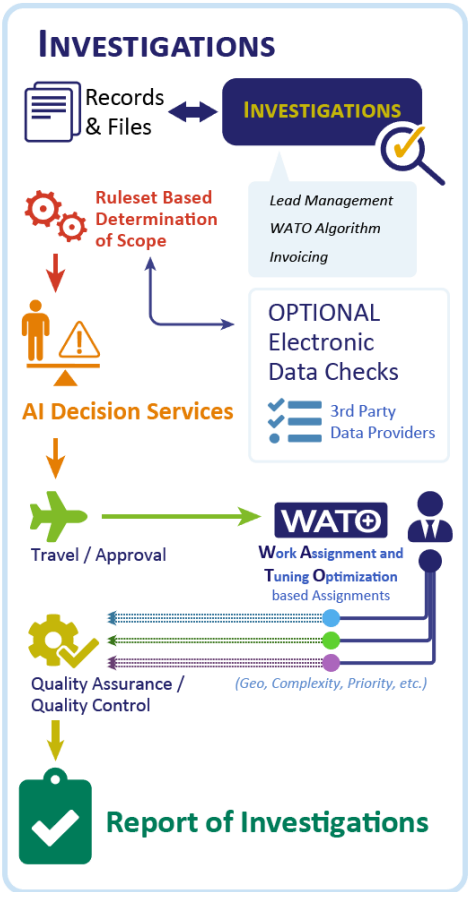
- ✓ Messaging Notifications and Escalations; email integration; Transactional timestamping for performance metrics, process optimization and ease of auditing
- ✓ Service Level Agreement (SLA) configurability between each task or step within workflows; color coded for ease of identification and priority
- ✓ Configurable Workflows. Intent-based. Role-based access and delegation capable
- ✓ Configurable AI (Artificial Intelligence) Decision Engine; e.g. for Tiers 1-5, scoping and Federal Adjudicative criteria
- ✓ Multi-Variable Optimization Workflow and Scheduling Engine based on a Pareto algorithm
- ✓ Role-Based (Case Assigner, Case Manager, Investigator, QA, etc.) Dashboards
- ✓ Integration for file-based, Web Service-based APIs
- ✓ Continuous Evaluation/Vetting Enrollment, Integration & Case Processing
- ✓ Developed with Privacy by Design standards
- ✓ Canned, ad-hoc & scheduled Reporting allows drill-down & segmentation measuring operational performance and trend analysis.

Enterprise Investigations Management (EIM)

Fresh Haystack EIM was built to decrease investigation timeline, improve overall investigation management, reduce paper and labor-intensive activities by using automation and removing manual touch points. EIM is already designed and constructed as the enabler of such capabilities. EIM provisions evolving requirements at the global case inventory level universally, from high demand at the region level down to the case and work item (aka lead) level.

During an investigation, EIM provides an environment for the Background Investigator (BI) to upload individual investigative artifacts and Reports of Investigation (ROI). Flexibility is built into the environment so the queue of investigation work items can be managed in a way to prevent investigator overload and increase efficiency, but control and/or redirect investigations to alternate investigators based on investigative performance, case workload, case complexity, geography, etc.

This method and structure of Investigations Management allows the entire investigative workload of cases to be distributed across multiple Investigators in any manner deemed appropriate and ultimately speeds case completion and reduces the cost of the each completed BI.



EIM Features

- ✓ Investigation initiation and assignment: geography-based, complexity, priority, and other factors
- ✓ Investigation Scoping: auto-scoped based on Federal Investigative Standards (FIS) Tiers 1 – 5
- ✓ Investigator Travel: minimized travel based on geo-assignment approach
- ✓ Investigator Sourcing: Flexible sourcing via controllable queue
- ✓ Investigator Assignment: automated, with flexibility to manually adjustments
- ✓ Investigator Review and Quality Assurance (QA): QA checks built into workflow
- ✓ Investigation Invoicing

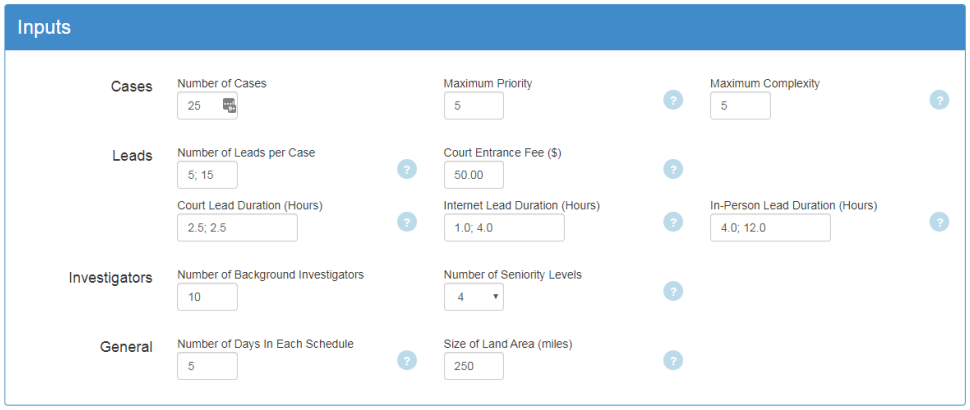
WATO

Work Assignment & Tuning Optimization

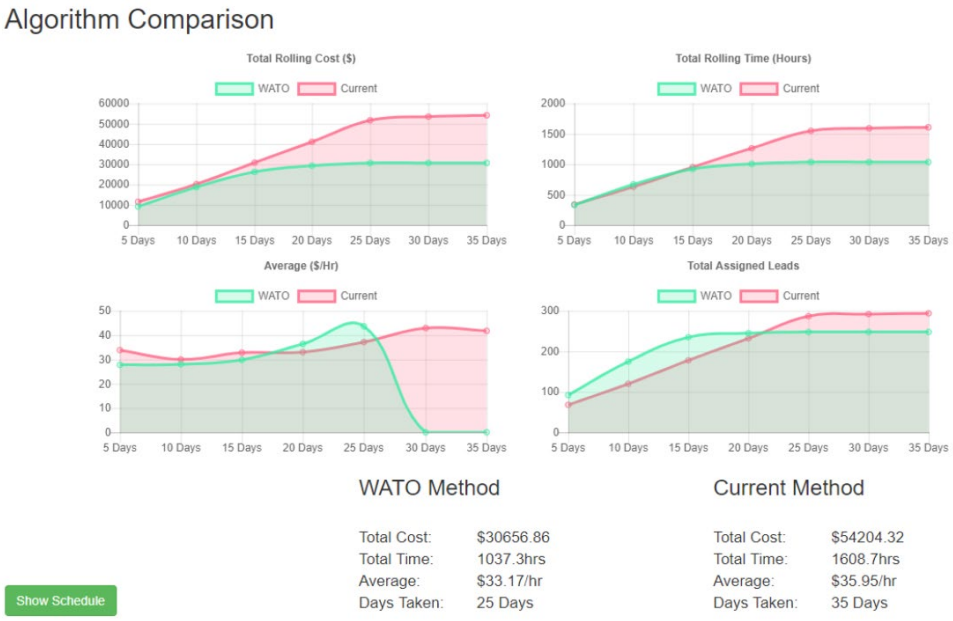
Scalability and optimal efficiency are achieved at scale by using a technology called Work Assignment and Tuning Optimization (WATO). WATO is using FH AI (Artificial Intelligence) Decision Services to assign work items (i.e. subject interview, reference interview, document retrieval, etc.) based on the case item, investigator experience, geography, travel distance, complexity, priority, and the other case-mandated attributes.

The result is increased case completion rates and greater accuracy/quality across all investigative operations. Change of investigative procedures would have minimal impact on FH processes in support of how information is being collected.

WATO Case Investigation Parameters



WATO Method vs Traditional Case Investigation Scheduling



Conclusion

Fresh Haystack EIM was built to increase visibility and collaboration into Enterprise Risk by combining Investigations, Insider Threat Defense, Personnel Security and flexible case management capability.

Fresh Haystack fosters multiple lines-of-business typically operating in silos to accelerate the development and integration process with a proven, low-risk system that is operational today and is built with growth in mind.

For White Papers on the relevant subjects and deeper dive, pick titles below:

- CARE
- Insider Threat
- Zero Trust
- Personnel Security
- Onboarding
- IRM

> *Our experience working with CANDA Solutions development team while standing up our Fresh Haystack Investigation system was overwhelmingly positive. They listened to our needs and found creative ways to make our unique requirements work within the system. The team made themselves available on short notice throughout the development, training and deployment process. This customer service exceeds expectations today through their customer service portal.*