CANDA Solutions
THINGS DONE

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

855.55.CANDA (22632)
info@candasolutions.com

INTEGRATED RISK MANAGEMENT

*Delivering Enterprise Risk by bridging the gap between the personnel, their profiles, **critical** facilities, programs **and assets**, networks and **cyber** activity to continuously deliver trust while minimizing organizational risk exposure.*

FRESH HAYSTACK

INTEGRATED RISK MANAGEMENT

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

April 2020

WfMC Awards for Excellence in Case Management WINNER 2017

Inc. 5000 HONOREE

2018 GREATER WASHINGTON INNOVATION AWARDS™ FINALIST

Gartner

Defense Industrial Base

SUMMARY

Many organizations today are struggling with Enterprise-wide Risk visibility. To facilitate, centralize, improve and simplify Risk Management across different parts of any corporation there is a key necessity for an integrated and collaborative top-down and bottom-up approach. Unfortunately, multiple factors, including human ones can generate a high-risk profile whether intentional or not. Thus, any Integrated Risk Management (IRM) solution deemed successful must leverage the interdependencies of multiple Enterprise risks, internal and external factors, audits, prioritization, measurement, mitigation, and reporting of consolidated threats to the Enterprise.

With limited budgets, resources, and legal/compliance issues, the IRM solution needs to address 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:

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

These collective risk activities provide a holistic program and picture of individuals, vendors, suppliers, subcontractors, cyber, 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.

Our solution places all elements of enterprise risk into a single, contextual, easy-to-use platform. Your organization will improve risk mitigation effectiveness by integrating the components of enterprise risk into a Common Operating Picture (COP) while complying with organizational policies, Federal / State regulations, and ethics standards.

All risk-related data discoveries can be reviewed while respecting employees' privacy, and simultaneously enable analysis of workforce generated risks across people, facilities, contracts (special programs, operations, etc.), assets, networks and management. This allows for action on anomalies via case management, investigations, and reporting.

The FH AI (Artificial Intelligence) Decision Services engine processes relevant data sets enabling automated risk assessments. Personnel receives alerts in near real-time of anomalies or behavior that might require immediate attention by HR, Legal, IT/CISO or Security teams.

SCHEDULE A DEMO

OVERVIEW

The Defense Industrial Base (DIB) and the United States Government (USG) are facing more challenges and threats by multiple state and non-state actors. In order to anticipate and mitigate these perilous threats, the USG and DIB have to work as partners to improve and protect the ability to develop effective technology, superior weapon systems and products, all which maintain our vigilance and expand military, political, and economic advantages for our Nation over global competitors and adversaries.

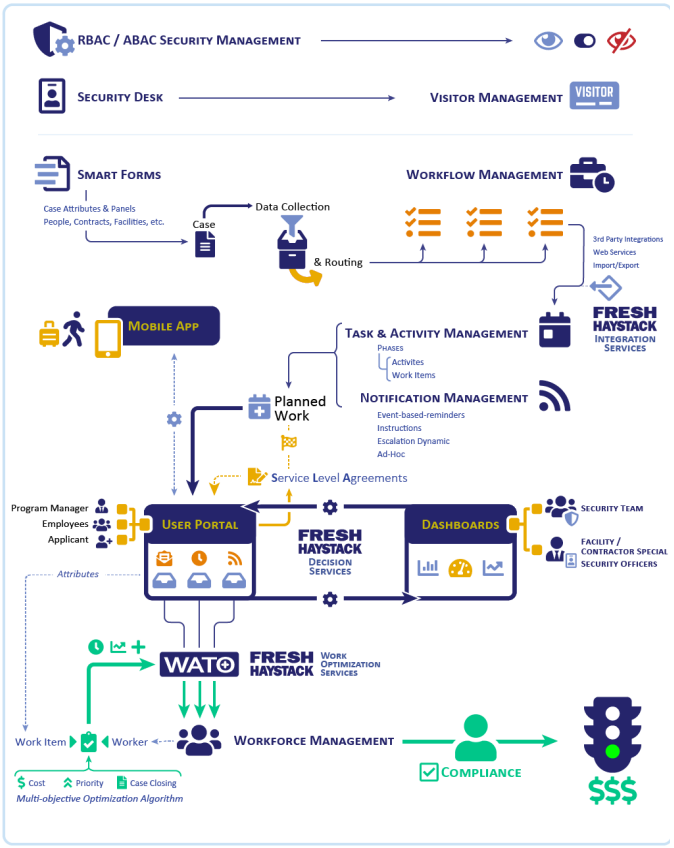
America's leading Government and Corporate position in the world is supported by protecting U.S. sensitive and classified information from cyber-attacks, espionage, critical technologies, assets, sensitive programs, key personnel, counter-intelligence activities, and insider threat defense. An accurate picture of Enterprise Risk is essential to meet these challenges. The solution should be continuous, enabling new risks to be factored as they arise. It should also be adaptive to allow for an evolving risk complexity. Our success will be determined by our ability to leverage innovative and flexible technologies to help us mitigate these evolving threats and demands across the enterprise.

Fresh Haystack (FH) is the first commercial robust case management platform designed specifically to address Integrated Risk Management for the Enterprise by utilizing risk-based, analytical decision making via aggregating relevant inside and outside of work data to protect Government and Corporations, bringing risk visibiltiy to the decsion makers.

The complexity of inter-relationships and interactions that take place through normal work, business meetings, personal visits, events, training, conferences, and projects make personnel as critically relevant as cyber-attacks.

In order to reduce the threat to the Enterprise and the workforce, today's program owners require an automated capability for full workforce lifecycle management, from onboarding to retirement, including integration of key instant internal / external alerts and risk analysis tailored to the specific needs of an Enterprise. Our approach does not intrude nor generate mass data from a query type approach that will exhaust budgets , instead it allows for a truly *continuous* program rather than periodic (monthly, quarterly or yearly) checks.

FRESH HAYSTACK CASE MANAGEMENT SYSTEM



Today's solutions rely on a query model that provides a snapshot of information that looks backwards and that is usually delivered without context. This requires an increase in resources to sift through massive amounts of data (false positives or true negatives) and flush out a small percentage of the population that requires attention while covering costs for the entire workforce.

Our system allows any organization to configure and automate security focused case management processes, add adjudicative requirements, setup risk baseline factors by applying weights and measures to various risks, and automatically present relevant risk scores and alerts for analysts to review, mitigate, and resolve.

By utilizing "push" technology rather than a "pull or query" approach from multiple external and internal data sources, we implemented Privacy by Design practices which protect an individual's rights by not collecting or looking at potential adverse actions for no reason.

Continuous Adaptive Risk Evaluation (CARE)

Security as a 4th pillar of the acquisition is an important DoD (Dept. of Defense) initiative. CMMC (Cybersecurity Maturity Model Certification) implementation is a necessary step towards enterprise cyber defense, but it is only a partial answer since many agencies and enterprises still operate in silos and many business functions are disconnected. Our out-of-the-box CARE platform aligns to 4 out of 5 pillars of the National Counterintelligence Strategy released in February 2020.

The CARE module is based on the enterprises' ability to baseline and prioritize critical programs, personnel, facilities, suppliers/vendors/subcontractors, assets, etc. within the Fresh Haystack ecosystem to access, manage, investigate and continuously *mitigate risk*.

CI Strategy Alignment

- ✓ Protects the National Security Infrastructure
- ✓ Reduces threats to Key US Supply Chains
- ✓ Counters the Exploitation of the US Economy
- ✓ Counters Foreign Intelligence Cyber & Technology Ops

Each Risk Stream is prioritized using a guided wizard, all issues are documented, audited, weighted and probability is added. The risk score is calculated for each risk stream and the total enterprise risk (eCARES) is a weighted mean of the individual risk streams.

If eCARES surpasses the acceptable baseline (i.e. 85 in red higher than 80) then the system will prompt for mitigation steps and dates, triggering creation of the Technology Security Plan version, allowing to track and report metrics and corporate risk over time.

> *Enable risk management teams to move beyond yearly "risk management" checklists to make **continuous, adaptive**, and intelligent risk-optimized security control decisions.*
>
> "Seven Imperatives to Adopt a CARTA Strategic Approach" Gartner, Inc. | 3871363

Integrated Risk Management (IRM)

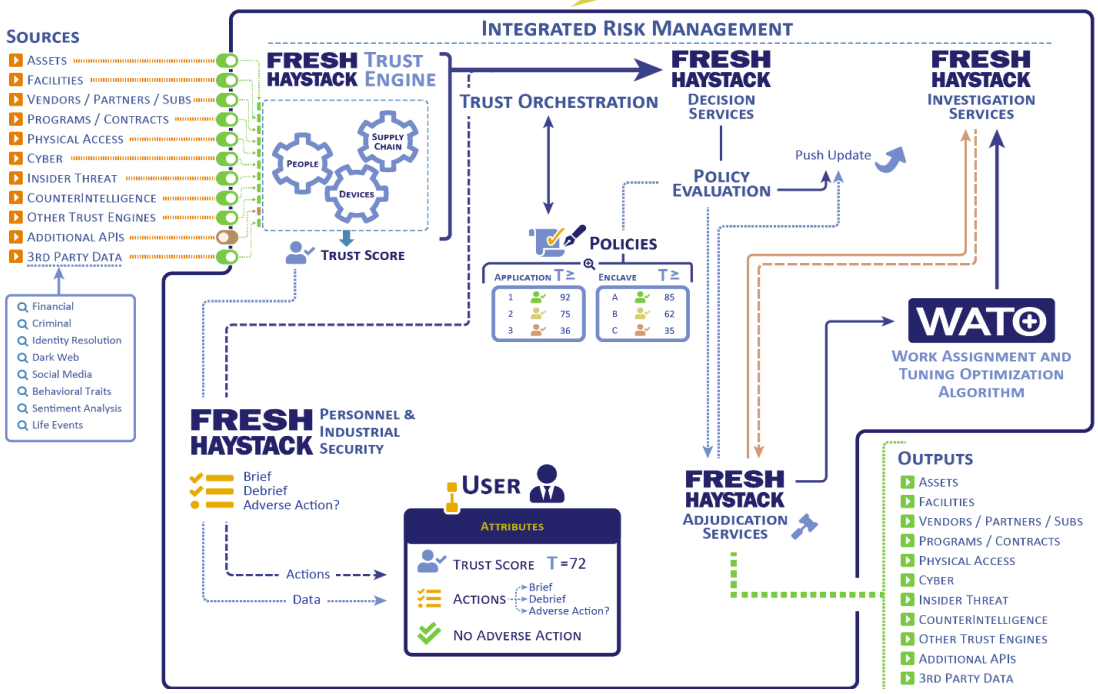
Fresh Haystack brings together Personnel Security demographic data, contracts data, and facilities data. Cyber Security meta data and alerts are pulled into the platform, along with outside work data such as criminal, financial, social media, etc. All combined enables a "whole person" view across the enterprise allowing for addressing/mitigating prioritized risks in a logical manner through security case management technology.

Additionally, the Fresh Haystack platform provides Insider Threat Defense via Continuous Evaluation & Vetting (CE & CV) and the platform supports many employee Self-Services functions including Foreign Travel, Self-Reporting, Training, and Security Incident Management.

Fresh Haystack is meant to function as a composite application; Combining data and information from various sources and platforms, enabling trust orchestration while presenting a common view that does not own or steward the information.

The platform uses various ingestion, mapping, linking, and Artificial Intelligence (AI) techniques; to automatically determine and notify on relevant alerts or issues in real-time. Usually, cyber and physical security data is treated differently, but they should be considered as major threat vectors, and included in the enterprise risk profile.

Our IRM approach enables security convergence and provides an understanding of operational workforce risk by integrating Physical Access, Cyber, HR and Personnel / Industrial security.



The Fresh Haystack modular ecosystem enables a continuous picture of enterprise risk and a trusted workforce previously limited by technology. We believe our IRM solution bridges the technology gap by converging individuals, their profiles, access, networks and activity into a single, consolidated view for agencies and corporations. Risk exposure can be accurately evaluated by consistently making intelligent data-driven decisions to access, track and capture mitigation opportunities while continuously delivering trust and minimizing enterprise risk.

For more on the relevant subjects and deeper dive, click title below:

- ITD
- Industrial Security
- Investigations Management