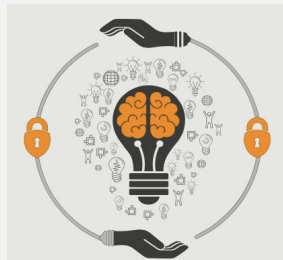




INTEGRATED RISK MANAGEMENT



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



INTEGRATED RISK MANAGEMENT

INSIDER THREAT DEFENSE
CONTINUOUS ADAPTIVE RISK EVALUATION
INVESTIGATIONS MANAGEMENT
PERSONNEL SECURITY

November 2020



Gartner



Private Sector

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 and privacy requirements, cyber-attacks on Intellectual Property (IP), organizational guidelines / procedures and corporate / consumer 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 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 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, operations, vendors, assets, networks, and management. This allowing 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 United States Government (USG) and many corporations 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 corporations 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.

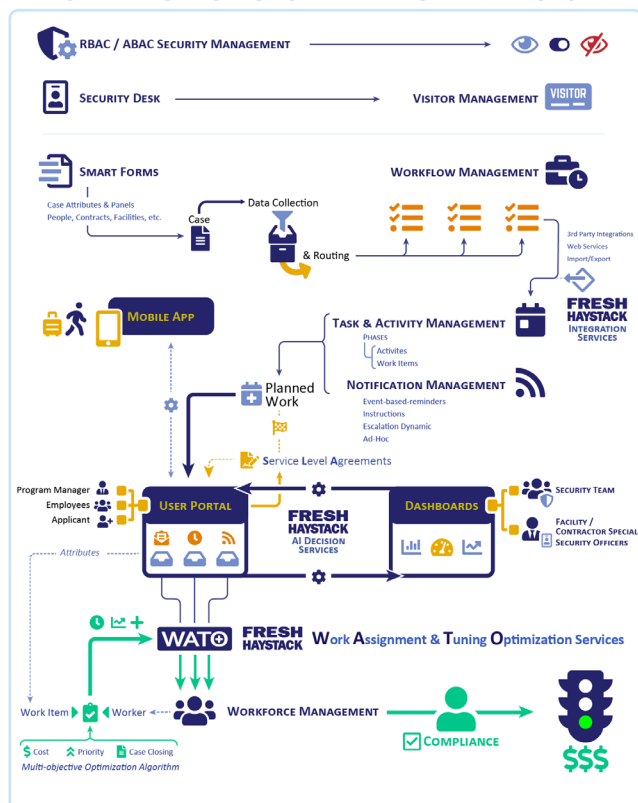
America's leading Government and Corporate position in the world is supported by protecting our intellectual property and trade secrets from cyber-attacks, espionage, critical technologies, assets, sensitive programs, key personnel, counter-intelligence activities, and insider threat defense. An accurate 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 our Government and American Corporations.

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 gathering relevant data from inside and outside of your organization to protect the business and bring risk visibility to the decision 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)

The current corporate climate and enterprise risk requires nuanced strategies that will require Executives to roll up their sleeves and learn by implementing crucial steps towards enterprise cyber defense. Their goal must be removing operational silos, connecting business functions to ensure that modernization does not digitize old ways of thinking and hinder adaptability. Adopting a wait-and-see approach, hoping that the current storms will pass is not viable.

Our out-of-the-box CARE platform aligns an enterprises' risk baseline to prioritize programs, personnel, facilities, suppliers / vendors / subcontractors, assets, etc. within the Fresh Haystack ecosystem to access, manage, investigate and *continuously mitigate risk*. This methodology builds up company resilience, maps potential risks, runs scenarios and conveys "business continuity" capacity.

We provide a necessary layer of integrated data from multiple risk streams, to support decision making related to operational and technology risks. This is highly valuable in proactively managing risk and could yield cost-savings by making redundant processes and technology obsolete.

“

85% of executives agree human vulnerabilities cause the most detrimental security breaches.

Economist Intelligence Unit, September 2019
[Cyber Insecurity: Managing Threats from Within](#)



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

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.

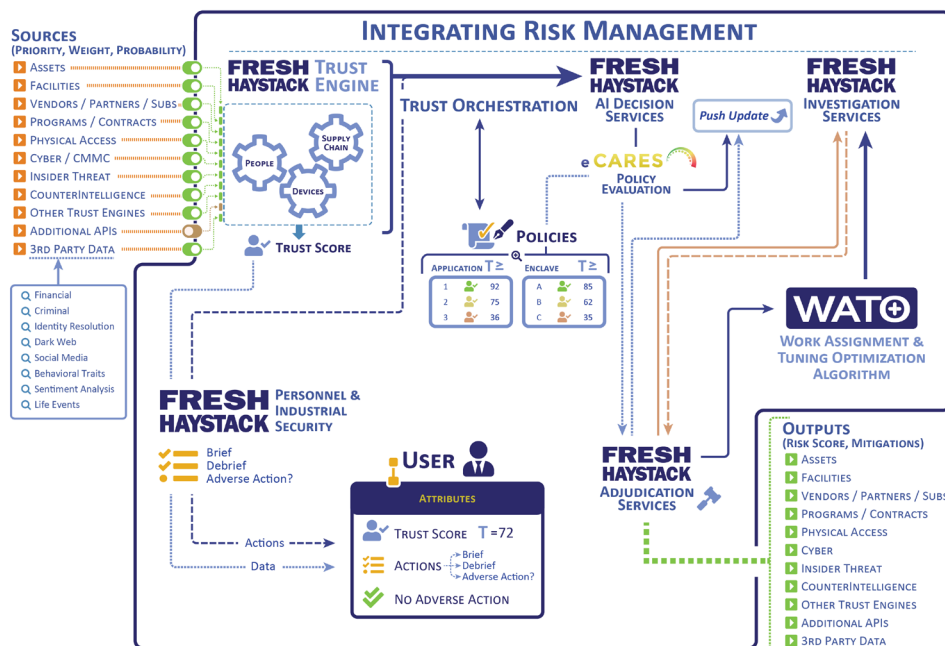
Additionally, the Fresh Haystack platform provides Insider Threat Defense via Continuous Evaluation & Vetting (CE & CV) and the platform supports many employee Self-Services functions including Foreign Travel, Self-Reporting, Training, and Security Incident Management.

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.

CONTINUOUS ADAPTIVE TRUST FOR ENTERPRISE



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



- [Onboarding & PreScreen](#)
- [CARE](#)
- [Personnel Security](#)
- [Investigations Management](#)