

# Insider Threat Mitigation

Analyze whole-person behavior, not just network data



**The Haystax insider threat solution continuously measures the trustworthiness of personnel in an organization, pinpointing early indications of the most serious risk from IP theft, espionage, fraud and other harmful events.** Our analytics platform reasons like a team of expert analysts, but at a volume and velocity that no human could sustain. It performs true all-source analysis by ingesting data from a wide variety of sources and then applying expert models, machine learning and other artificial intelligence techniques to ‘connect the dots.’

## Proactive threat intelligence

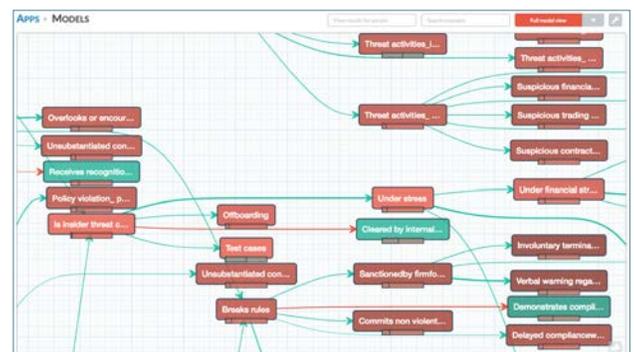
Conventional data analytics solutions typically detect hidden insider threats only after an adverse incident has occurred. The Haystax analytics platform dynamically identifies key personnel risk indicators, even in weak signals or subpar data sets, while filtering out 97 percent of the false positives. As a result, security operations center analysts have a clear picture of their highest-priority threats and can respond immediately as a threat is emerging — before any harm has been done.

## Model-driven analytics

Haystax data scientists have encoded the judgments of diverse insider threat experts into a probabilistic ‘whole-person’ model representing over 700 behavioral indicators of trustworthiness. Data fed into the model can come from internal repositories such as HR records, printer and access control logs and network security devices, and from public sources like social media feeds and criminal and financial records. The Haystax platform continuously analyzes new information to quickly discern when an individual starts trending in a negative direction.

## Analyst-friendly workflows

The Haystax solution supports collaborative workflows and adheres to existing organizational guidelines and best practices. With our easy-to-use interface, an analyst can discern trends or receive automated alerts to quickly identify the riskiest outliers – investigating their histories and records, conducting risk assessments, identifying related incidents and recommending tailored responses. And because the Haystax platform runs at machine scale and can be reconfigured on the fly, organizations don’t have to hire more analysts as their threats evolve.



# Customer Success Stories



“  
... the agency has  
gained tighter control  
over its evaluation  
processes while also  
improving threat  
alerting...”

**A large defense agency needed a better way to identify trusted insiders at risk of becoming active threats. Haystax deployed its analytics solution to continuously evaluate and rank insider threats at the agency. In the initial operational pilot 4,000 highly cleared personnel were analyzed, and the group was expanded to 100,000 personnel in a subsequent operational deployment.**

Our model was then validated by the agency, and Haystax is now extending the system across the entire agency, so that all personnel can be continuously evaluated. As a result of this deployment, the agency has gained tighter control over its evaluation processes while also improving threat alerting, investigation timelines

and information sharing across multiple functional areas. According to a recent evaluation briefing by the agency, the Haystax solution represents the “only known system for prioritizing personnel according to positive and negative nodes of trust.” One agency official called it the “the gold standard to be measured against when designing a tool.”

## The Haystax Advantage



### Preemptive

Decision-makers get immediate, continuously updated intelligence on high-risk individuals



### Holistic

Connectors make it easy to integrate existing data and system feeds



### Transparent

Behavioral model shows exactly how each individual's risk score is calculated



### Adaptable

Model can be tuned to account for new or evolving threats