Government intelligence, homeland security and law enforcement agencies struggle to tap into large and growing data sources in their effort to detect, predict and prevent both insider and external threats.

The threat prediction and prevention solution framework from IBM provides a proven set of solution components to help analysts and officials master and make sense of this information, in order to uncover and respond to non-obvious and emerging threats. IBM has assembled a set of best-of-breed, open-architecture anti-threat solution components that are scalable, flexible and that can be combined to address virtually any threat detection and prevention use case.

**Threat prediction and prevention solution framework from IBM**

Some key components of the solution include:

- IBM® InfoSphere® Identity Insight for non-obvious identity and relationship resolution as well as real-time alerting.
- InfoSphere Global Name Recognition for sophisticated, multi-lingual, multi-cultural name matching.
- InfoSphere Guardium to monitor trusted user activity and to protect high-value structured data from suspicious or unauthorized access and use when insider collusion is a risk.
IBM Initiate® for probabilistic records matching and policy-conformant records integration and sharing across multiple sources.

- IBM DB2® Anonymous Resolution to enable two agencies to detect possible links and establish the probable cause necessary to authorize direct sharing of controlled information.
- IBM SPSS® for predictive modeling and deep statistical analysis.
- IBM Netezza® for extremely high-speed, appliance-like, in-memory analytical processing.
- IBM i2® and IBM Cognos® for data visualization, presentation and reporting.
- IBM ILOG® for role-based application of business rules and automated support for business processes to ensure coordinated, policy-compliant response to analytical insights.
- IBM Content Analytics for semantic-based contextual understanding of massive amounts of unstructured text.
- InfoSphere Streams for real-time analysis and disposition of large volumes of streaming (in-motion) data.
- InfoSphere BigInsights for Hadoop-based MPP analytics against massive at-rest data sets.
- The family of InfoSphere Server products to coordinate and improve ETL, data quality, data standardization, data architecture design, metadata management, data governance and more.

Configurable to match an agency’s mission, use case and workload, various combinations of these solution components can help clients address emerging threats by:

- Uncovering connections that perpetrators try to hide.
- Finding and presenting the information that matters, but is buried within huge volumes of data.
- Providing real-time, prioritized, understandable, role-based and actionable information based on a “single version of the truth.”
- Helping agencies move from a reactive to a preventive posture for combating both internal and external threats.

Shining a light on non-obvious relationships and patterns of behavior

As criminals grow more sophisticated, governments must leverage more powerful tools to keep up. Offerings like InfoSphere Identity Insight and InfoSphere Global Name Recognition help resolve concealed or obfuscated identities and establish relationships among them. Analytical tools such as those provided by SPSS Statistics workbench work in tandem with Identity Insight to help uncover additional non-obvious patterns of behavior. And while no analytical tool can ever fully replace the judgment of a trained analyst or investigator, it can suggest which facts stand out and which are most likely to be important; and it can gather and present candidate “needles” from the proverbial “haystack,” so that they aren’t overlooked.

Finding what matters in oceans of data

Never before have government agencies felt the needle-in-the-haystack challenge more acutely. As sources of information grow in number, kind and size, what seemed like a haystack can start to look more like a mountain. And with social media, biometrics, geospatial data and other new, explosively growing data types, what should be a gold mine of new sources of insight can seem to analysts more like they’re being buried alive. Expert analysts and subject matter experts will always be in short supply, and leveraging their attention and maximizing their efficiency will always be priorities. This means that it’s not enough for analytics to be clever—they must sort through prodigious amounts of data extremely. Products such as InfoSphere Streams and InfoSphere BigInsights help agencies filter and sift through these oceans of data—whether it is in motion or at rest—to find and relate the nuggets of information that really matter for a given investigation. Additional tools such as Content Analytics can find sense in vast and under-exploited internal and external sources of unstructured text by going far beyond keyword and Boolean searches and instead applying semantic and contextual analysis to extract meaning and find otherwise undetectable patterns of meaning.
Sharing trusted data, drawing conclusions and taking action

A major inhibitor to taking effective action against developing threats are a lack of confidence in the data at one's disposal, and an inability to share it with others. Lack of data cleansing, standardization and integration are root causes of both problems. Information management tools like the InfoSphere family of software offerings comprehensively address this need, and help cooperating agencies—and sections within a given agency—share and act upon “one version of the truth,” and coordinate their data resources, stewardship and policies. Once data is trusted and shared, the very analytics that can find and collect these nuggets of information that matter most can also be enlisted to help analysts make better sense of them. The analytics can also enable colleagues to act upon their conclusions appropriately, while providing auditable evidence that decisions were arrived at legally and responsibly.

Tools such as i2 and Cognos can exploit the output of tools like Identity Insight and SPSS to help analysts visualize, explore and make sense of the relevant data they are presented with and then communicate it to others for subsequent actions, whether they are adjudication, intervention or further monitoring. Cognos and ILOG can apply role definitions, process flows and business rules—which themselves can include legal requirements, privacy constraints and administrative and jurisdictional restrictions. These applications can help ensure that the right results are communicated to the right people in the right form and sequence, and that insight is applied in a timely, appropriate, auditable and policy-compliant way. Appropriate actions are always important, but can be especially vital when circumstances such as an unfolding incident or significant change in patterns of suspicious activity cause spikes in activity that require optimized responsiveness.

Prediction and prevention—staying a step ahead

Bad actors are constantly changing their tactics, which means government agencies must have a system that is “smart” enough to continually learn something new. The factors described above—increasing velocity, variety, and volumes of data—that challenge authorities and are exploited by perpetrators, will increasingly require that agencies anticipate and pre-empt emerging trends in threatening activity if they are to maintain, let alone increase, acceptable levels of response. Predictive modeling tools such as SPSS Modeler can help with this, and can exploit analytical “inputs” provided by other offerings like Identity Insight, Global Name Recognition and Content Analytics, among others. Products such as Cognos that facilitate improved performance management can work with SPSS to help organizations track and review their predictive capabilities over time, and spot and respond to trends they might be missing.

Predictive capabilities not only help authorities increase their rate of discovery of suspicious behavior, but also help agencies make best use of increasingly strained budgets and resources, ensuring that the expert human analysts who will always be in short supply focus on the signals of potential threats that most warrant their attention.
**How IBM can help**
For decades IBM has led the way in helping government agencies make the most of their data assets. We offer a fully integrated solution framework for threat detection and prevention, bringing research, intellectual capital, mission and technology experts, and a comprehensive software solutions portfolio together to help agencies detect internal and external threats before they can be realized. Our solution framework and its underlying portfolio of solution components together enable government authorities to apply advanced composite analytics to take advantage of both new and traditional data sources in new ways. In doing so, they help ensure that agencies charged with the protection of the country, its people and its assets are able to achieve their mission.

**For more information**
To learn more about the threat prediction and prevention solution framework, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/government