Building a Smarter Planet with
Advanced Identity Insight Solutions

Information Management software

Detecting Insider Threat & Collusion with IBM InfoSphere Entity Analytic Solutions

Highlights

- ***Uniquely identify individuals and differentiate between internal representations (employees, vendors, external entities, etc.)***
- ***Identify non-obvious relationships amongst the population of identities (employee-to-employee, employee-to-vendor, employee-to-external, etc.)***
- ***Automatically track, detect and alert on employee/vendor activities (on-site presence, network activity, etc.)***

US organizations lose an estimated 7% of their revenues to fraud. Insider schemes that involve two or more employees result in a median loss over four times higher than the amount lost in schemes committed by a single inside perpetrator. Developing and maintaining a deep understanding of your employees, vendors, external threats, and their respective relationships is key to pre-empting and preventing unwanted insider activity.

When it comes to developing and maintaining an understanding of your employees, vendors, customers, external threats and your interactions with them IBM Infosphere Entity Analytic Solutions (EAS) addresses three key questions:

"Who is Who?"
Automatic disambiguation with complete identity (people and organizations) context

"Who Knows Who?"
Real-time discovery of non-obvious identity (people and organizations) relationships

"Who Does What?"
Quantification of identity (people and organizations) activity across events (modified address) and transactions (employee withdrew $10K from customer account)

Pre-Empting Insider Threats for Over 20 Years

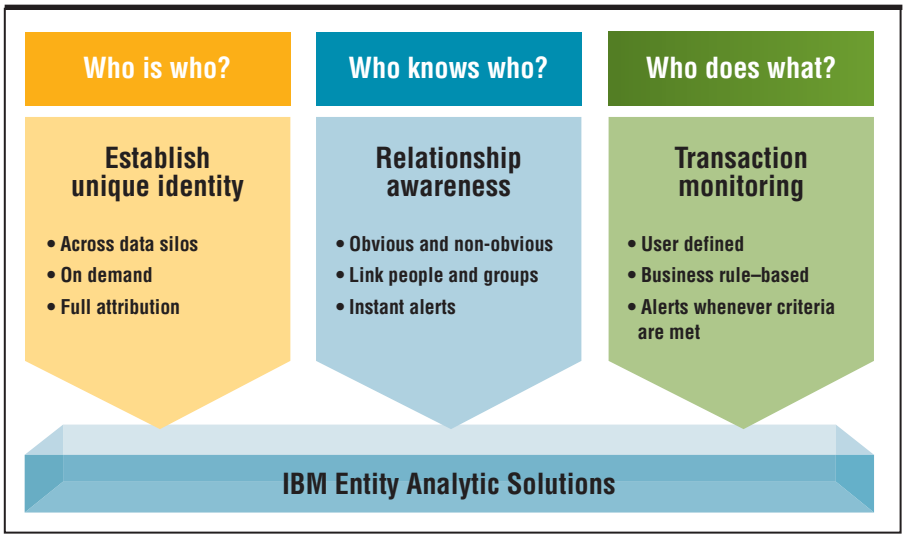
The frequency, variety, and sophistication of insider threats are increasing. Fraudsters have learned to work together and "Game" antiquated, batch-driven, silo-oriented processes used in the typical enterprise. EAS delivers real-time discovery of business interactions across the enterprise to aide the organization in pre-empting insider threats.

Consider this hypothetical example. Several years ago your enterprise put an employee behind bars for unlawful insider activity. Today one of your employees changes their payroll mailing address to the residence once inhabited by the jailed ex-employee. Perhaps another insider scheme is being hatched? With what method and how fast will you detect this relationship?

IBM Entity Analytic Solutions (EAS) has been pre-empting and preventing insider threats for nearly 20 years. The earliest deployments of EAS for insider threat were with casinos in Las Vegas. EAS' ability to discover suspicious relationships between Casino employees and "Big Winners" has been highly effective at preventing fraudulent outcomes.

Pre-empting an insider threat can be daunting unless you are properly armed in advance of the occurrence.

The IBM InfoSphere Entity Analytic Solutions Platform



The IBM InfoSphere Entity Analytic Solutions portfolio gives you a deep understanding of your employees, vendors, external threats, and their respective relationships is key to pre-empting and preventing unwanted insider activity.

EAS analyzes electronic data within the enterprise and builds an electronic activity dossier for each entity (identity/organization) in real-time. EAS is ideal for:

- Uniquely identifying individuals and differentiating between internal representations (employees, vendors, external entities, etc).
- Identifying non-obvious relationships amongst the population of identities (employee-to-employee, employee-to-vendor, employee-to-external, etc).
- Automatically tracking, detecting and alerting on employee/vendor activities (on-site presence, network activity, etc).

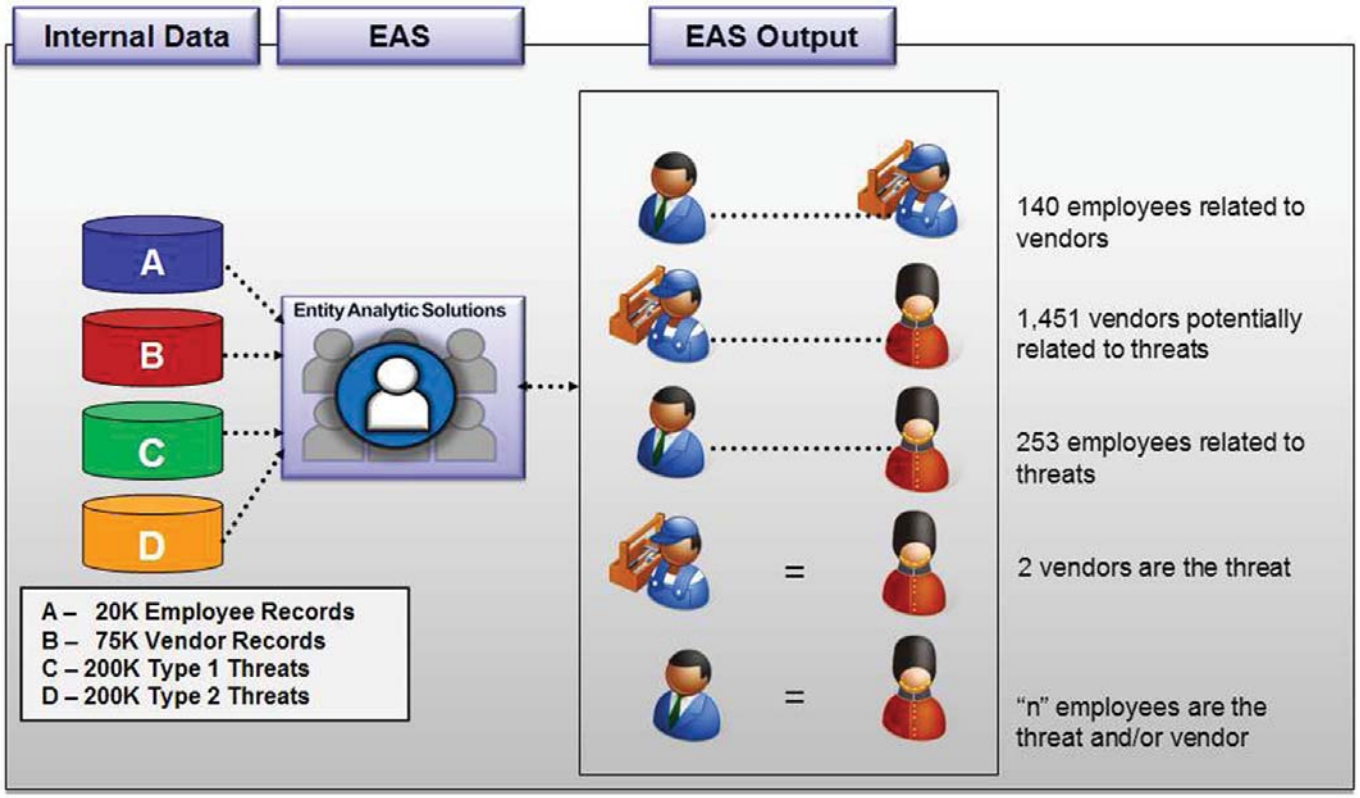
EAS in Action: Insider Threat Detection

InfoSphere Entity Analytic Solutions has been deployed across the globe to find threats from inside and outside an organization. Following are a few examples of the organizations using EAS for insider threat detection:

A large retail bank in the U.S. benefited tremendously from EAS' time to value. In just 3 weeks, EAS was installed, configured and loaded with 50M customer records. At the end of this brief period EAS delivered:

a) A complete electronic dossier for each customer and their accounts, including a 12% reduction in customer record duplicity

b) Relationship correlations from customer to customer



This figure illustrates how a large public sector enterprise enlisted IBM InfoSphere Entity Analytic Solutions to detect and prevent insider threats in real time.

c) Relationship correlations from customer to targeted watch lists.

A large US-based retail bank deployed EAS because knew they possessed insider (employee) threats as well as external (customer) threats. However, due to a reliance on legacy systems they were unable to address the problem. EAS was deployed for enterprise-wide discovery of employee fraud and collusion.

A large public sector enterprise enlisted EAS for help with detecting and pre-empting insider threats. The enterprise provided thousands of electronic data records internal to their organization describing employees, vendors and targeted threats of various severities. EAS ingested and analyzed the electronic data. The moment the data was loaded into EAS; actionable intelligence was generated and delivered to security analysts. The figure above illustrates the inputs, processing and actionable outputs:

For more information

Concerned about insider threats in your organization? Reach out to your IBM Infosphere Entity Analytic Solutions (EAS) specialist today to begin a dialogue on EAS for insider threat.

You may also learn more about IBM InfoSphere Entity Analytic Solutions by visiting: ***ibm.com/****software/data/ips/products/masterdata/eas*

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
May 2009