

**Information Management** software

## Recognize Nefarious Cyber Activity and Catch Those Responsible with IBM InfoSphere Entity Analytic Solutions



---

### Highlights

---

- **Cyber Security Solutions from IBM InfoSphere Entity Analytic Solutions... A One, Two Punch!**
- **Defense: Protect your critical applications from cyber attacks**
- **Offense: Catch those behind potential security breaches**
- **Turn an IP address/e-mail address/cookie pattern into actionable intelligence**

### Cyber crime in the 21st century

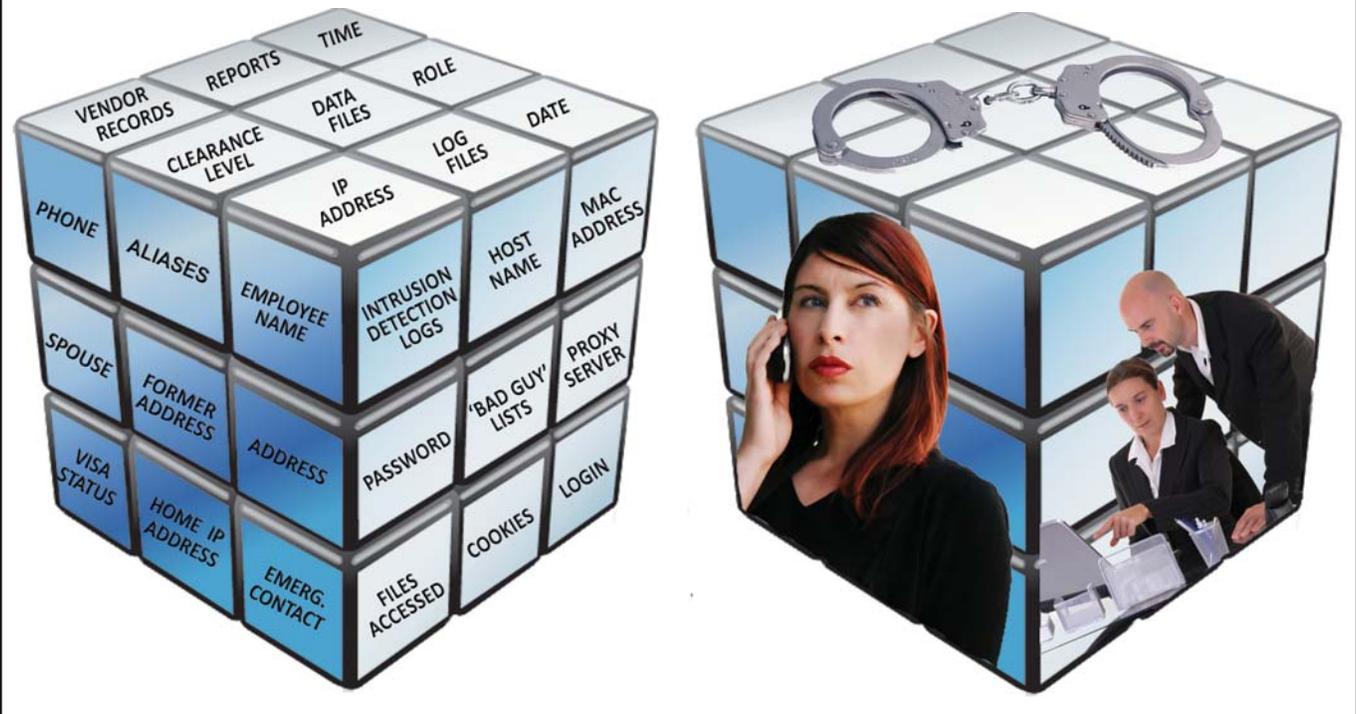
It seems as though every day there is a front page news story about a new cyber crime – somebody hacking into a network and stealing personal information, a potential breach against a utility infrastructure, a new frightening virus, or a thief compromising an online account with a stolen identity.

Most corporations and government agencies have addressed the physical security element of cyber crime. Virus software, firewalls, and access management have become staples in the network security/cyber crime fight. When done correctly, this is a critical step, but not the ONLY step.

No more is the lone hacker in a far off land the biggest threat. Instead, breaches in cyber security tend to start closer to “home”. According to a recent eCrime Watch study conducted by CSO magazine, cyber crimes have taken on some surprising new characteristics :

- “The use of social engineering techniques (gaining access through manipulation of a person or persons who can permit or facilitate access to a system or data) jumped to become the #1 method [of committing cyber crimes] (45% v. 38% last year) followed by individuals using compromised accounts (39%)” <sup>1</sup>

## Resolving data from throughout the enterprise to fight cyber crime



IBM InfoSphere Entity Analytic Solutions can resolve information from throughout the organization - including event records, employee and vendor records, log files, IP addresses... whatever information might be critical in linking an individual or a group of individuals to a cyber crime.

- “Most e-crimes, whether perpetrated by an insider or an outsider, are handled internally without involving legal action or law enforcement (67% for insiders, 66% for outsiders.) Given the growth in the number of crimes involving the theft of personally identifiable information, and the breach notification laws that have been passed, it is concerning to see that organizations continue to handle so many cases within their own walls. When asked why they had not referred these e-crimes for

legal action, respondents echoed last year’s findings that either the damage level was insufficient to warrant prosecution (40%), there was a lack of evidence (34%), or that they could not identify the individuals responsible (28%).”<sup>1</sup>

In short, disguising one’s own identity to gain access, and stealing somebody’s identity who already does have access make up over 84% of cyber criminal activity. And most cyber criminals are not brought to justice, almost guaranteeing that they will repeat

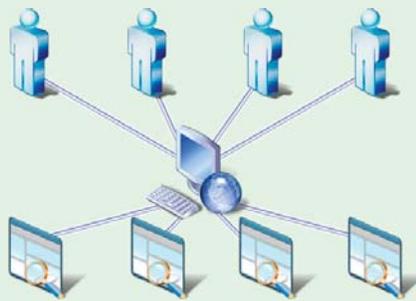
their crimes. Therefore, it is crucial to understand who – exactly – is gaining access to your network.

### **IBM InfoSphere™ Entity Analytic Solutions – a new approach to fighting cyber crime.**

Government agencies need to proactively protect their critical applications, data and processes from external and internal threats throughout their entire life cycle. By taking a comprehensive and integrated approach to application vulnerability management that includes understanding the identities that are accessing your network, agencies

## Can your cyber security system recognize...

- ... that an IP address that has just been blocked for suspicious activity was used two months ago to enter your department's intranet, with proper authentication and without cause for alarm?
- ... that the contractor who accessed the system 2 months ago has an H-1B Visa that is about to expire?
- ... that the contractor who accessed the system 2 months ago just moved to the same address as a former employee that was laid off for attempting to copy secure files?
- ... that the former employee's husband has just been indicted for cyber criminal activity?
- ... that the former employee listed a foreign national from an embargoed country as an emergency contact ?
- ... that the foreign national's name is a cultural variation of a name that appears on a highly sensitive watch list?
- **... and that they are all working together in an attempt to breach the network and uncover sensitive information?**



can measurably improve operational security, mitigate risks, and reduce costs.

Drawing on a deep understanding of today's security threats and backed by more than 40 years of leadership in IT security, IBM offers comprehensive solutions to help agencies build a complete cyber security solution. IBM offers advanced solutions that protect critical Web applications, data and processes throughout their entire life

cycle. It also offers groundbreaking identity resolution technology that can help with the identity aspect of cyber security.

IBM InfoSphere Entity Analytic Solutions can help governmental organizations recognize who exactly is on the other side of a transaction, providing real time identity and relationship recognition and resolution in context with existing cyber security applications. IBM Insight Solutions offer advanced,

comprehensive, real time, analytic capabilities to proactively detect and prevent these threats, risks, and vulnerabilities. Additionally, it enables governments to uncover individuals or groups masking their identities and to uncover the multi-identity relationships tied to organized threats, foreign-sponsored attacks, theft and fraud. Additionally, IBM Insight Solutions produces a continuous real-time repository of names, identities, and relationships that is searchable and available to multiple government agencies in order to facilitate optimal coordination and information sharing among federal/national, state/provincial, and local governments.

### **IBM InfoSphere Entity Analytic Solutions plays defense – Keep the bad guys out!**

Cookies, IP addresses, and email addresses can be a goldmine when it comes to cyber security. However, until now, these important attributes have been used in isolation and after the fact.

Entity Analytic Solutions enables an agency to realize how an IP address has been used in the past, maintains cookie values, and links them to the identities it already "knows". Additionally, once certain events are triggered (i.e. an IP address matches one that was used three months ago by an employee that was terminated last week), an

alert is generated, delivering real-time actionable intelligence to your investigation unit.

### **IBM InfoSphere Entity Analytic Solutions plays offense – Catch those responsible for cyber attacks!**

Your network security system can detect when someone has penetrated your network, but can it turn an IP address into actionable intelligence to help find out who is actually behind the attack? Can it figure out who they are working with? And will it help you build a case against them so they end up where they belong?

### **Who is Who? - Discovering true identity**

Entity resolution is the process of identifying who is who (for people and organizations). For example, in criminal circles it is accepted that individuals may possess multiple identities: the role of entity resolution is to establish all of the transactions that pertain to a single entity. For example, IBM InfoSphere Entity Analytic Solutions helped one organization determine they did not in fact have 120 distinct customer accounts, rather all these accounts belonged to one person. Understanding who is who is fundamental to understanding context.

### **Who Knows Who? - Uncover criminal networks**

IBM InfoSphere® Relationship Resolution establishes that there exists (or has existed) a relationship between

## **A Customer Example: Fighting cyber crime in the commercial world**



IBM InfoSphere Entity Analytic Solutions are deployed to fight cyber crime in non-governmental spaces as well.

For example, a major financial institution in the United States utilizes the technology to match new applicants' cookie value/email address to a historic "hot list". If found, the applicant's name, social security number, address and phone number are all added to the hot list for subsequent link analysis. If this "bad applicant" is related to existing active accounts then an alert is generated/delivered.

IBM's Identity Resolution solutions deliver real-time actionable intelligence to the bank's fraud investigation unit for these conditions:

- The rate of applications submitted by the same (email/cookie/IP) user is high.
- The sum of all accounts that are negative exceed a specified dollar amount.

- The number of applications that received an account number (approved or pending) is high.
- The number of applications that received an account number (approved or pending) is moderately high with a success rate less than 40%.
- A new application links to anything on the bank's hot list (email/cookie/IP) within the same 24-hour period.

This institution's research shows that, on average, each fraudulent new account opened via the internet results in a loss of \$1,880. In the first month of deployment, IBM Identity Resolution technology delivered over 700 suspicious alert, and identified 388 of these as confirmed fraud for a savings of approximately \$733K. On day two of production, it also identified and mitigated a fraudulent transaction in the amount of \$500K from taking place.

***In total, deploying IBM Identity Resolution solutions detected over \$1.2 million in fraud within one month.***

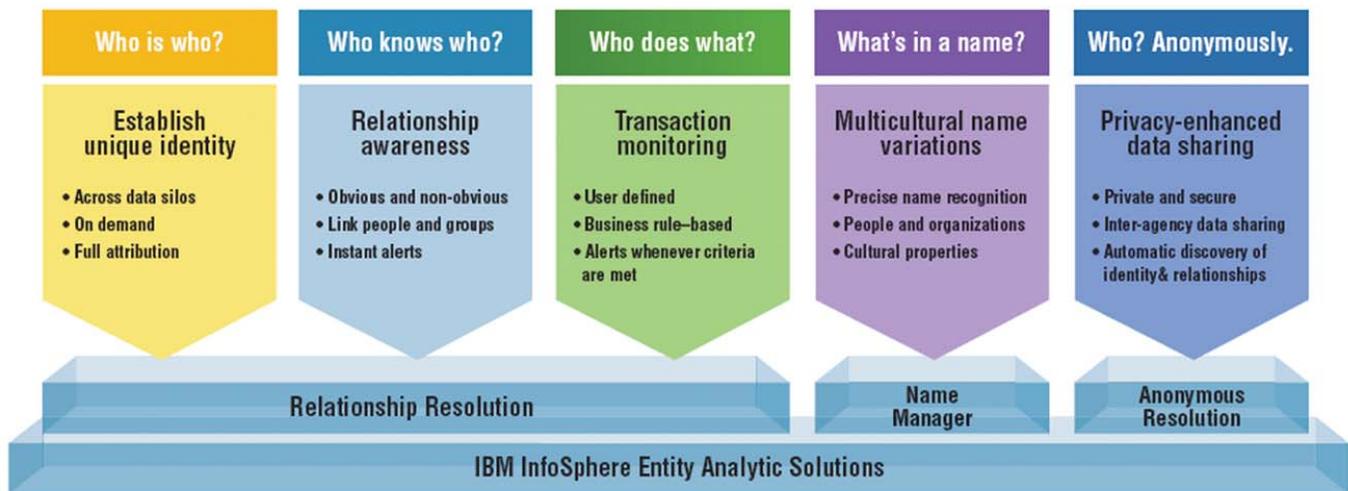
different individuals: for example:

- Two people lived in the same house at the same time
- A new employee's emergency contact information (in the payroll

system) is one and the same as the recently arrested criminal

- A network security analyst shares the same telephone number as an employee that was recently terminated.

## The IBM InfoSphere Entity Analytic Solutions Platform



While Entity Analytic Solutions learns of such relationships and remembers these over time, only discoveries of relevance are issued as alerts, e.g. your network security analyst lives with a former employee who was terminated for accessing classified files. IBM InfoSphere Entity Analytic Solutions understand expressed relationships (a reference on an employment application) and detects unexpressed relationships (roommates or people sharing an address or phone number).

### Who Does What? - Detecting potential threats through their transactions

IBM InfoSphere® Relationship Resolution offers real-time transaction/event processing capabilities based on customer-defined business rules. Using this capability, an analyst can receive an alert whenever a certain threshold or usage pattern is met. For instance, an analyst can specify that they want an

alert whenever the same sensitive files on the network are downloaded by “x” number of different IP addresses within a 24 hour time period, or if the same user ID is being used in multiple geographic regions during the same timeframe.

### What's in a Name? - Multicultural Name Variations

IBM InfoSphere® Global Name Recognition provides culturally-relevant insight about individual and business names that helps customers understand more about a particular name, such as culture, gender, and name parsing, as well as identify names that are likely to represent the same person in a list.

### Who? Anonymously. - Insight without divulging sensitive information

Information sharing across organizations can raise significant issues, regardless of the application. Often reputation, privacy and security concerns present

such large barriers to information sharing that information is simply not shared.

IBM InfoSphere® Anonymous Resolution answers the questions, Who is Who? and Who knows Who? in a manner that greatly reduces the risk of unintended disclosure. Anonymous Resolution helps organizations, both public and private, to meet the demands of secure information sharing in a privacy enhancing manner, and overcome geographic, cultural, and policy barriers that prevent information sharing due to the risk of unintended information leakage.

### For more information

To learn more about cyber security solutions from IBM, contact your IBM sales representative or IBM Business Partner, or visit:

[ibm.com/federal/security](http://ibm.com/federal/security)

## Enterprise amnesia versus enterprise awareness and why it matters in the world of cyber security

It is impossible to ask every important question about every piece of data that enters a system of record. As a result, information is not discovered or made available until the right questions are asked. Too often this information isn't identified until after the critical period of its highest utility has passed. This reality has rendered large data repositories ineffective when addressing real-time events resulting in a condition called enterprise amnesia.

Essentially, we don't know what we know, because we either don't know what questions to ask or we can't ask them quickly enough to make a difference.

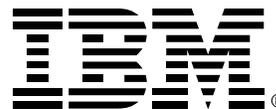
Moving from enterprise amnesia to enterprise awareness requires persistent context. For example, the same person can interact with your systems of record multiple times using different identities. Unless those identities are resolved to a single entity, during any given interaction you have no way of discovering whether the person you're currently interacting with is in reality a person of interest or concern. However, by pre-constructing the context (resolving multiple identities to a single entity and recognizing how people relate), and by maintaining that context over time, what was previously undiscoverable now becomes discoverable in real time.

There are three main principles of intelligent data discovery that an agency should consider in attempting to achieve true enterprise awareness:

- 1st Principle: If you do not process every new piece of key data first like a query, you will not know if it matters... until someone asks.
- 2nd Principle: Treat queries like data to avoid having to ask every question every day.
- 3rd Principle: Enterprise awareness is computationally most efficient when performed at the moment the observation is perceived.

By implementing these three information management principles, IBM InfoSphere Entity Analytic Solutions creates an environment where "the data finds the data and the relevance finds the user." In other words, as data is ingested, every important question is immediately asked about that new piece of data within the context of everything the system knows, and relevant alerts are instantly generated and sent to the associated analysts.

"Enterprise awareness" is critical for Cyber Security. Security analysts and investigators must be able to ask "smart questions" at any time - even if there is no answer yet. For example, an analyst should be able to query the system to see if a particular IP address or cookie pattern has been encountered by the system. Just because it hasn't yet been encountered doesn't make the query any less pertinent. When the system does encounter such a scenario, it should alert the analyst and provide a compilation of everything known about the person attempting to access the system.



© Copyright IBM Corporation 2009

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

Produced in the United States of America  
April 2009  
All Rights Reserved

IBM, the IBM logo, ibm.com, and InfoSphere are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

Other company, product, or service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates. The information contained in this documentation is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, it is provided "as is" without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this documentation or any other documentation. Nothing contained in this documentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM (or its suppliers or licensors), or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

Each IBM customer is responsible for ensuring its own compliance with legal requirements. IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

♻️ Printed in the United States of America on recycled paper containing 10% recovered post-consumer fiber.

### SOURCES

2007 E-Crime Watch Survey – Survey Results  
September, 2007  
Conducted by CSO magazine in cooperation with the U.S. Secret Service, CERT® Coordination Center and Microsoft Corp.  
<http://www.cert.org/archive/pdf/ecrimesummary07.pdf>