

Go head-to-head against threats and fraud with a comprehensive security management solution.

Highlights

- Minimize the risk of threat and fraud by taking a best-practice approach to the online transaction life cycle
- Give consumers safe access to Web applications by making sure you know the user
- Verify what the user is allowed to do using rules-based authorization, single sign-on and strong authentication
- Optimize compliance and incident response by monitoring user behavior in real time
- Defend against and respond to threats and fraud rapidly and effectively
- Get closed-loop feedback on your security posture using a comprehensive, integrated solution that links defense and access mechanisms

Most businesses have robust firewalls and other security solutions to effectively address enterprise threats stemming from things like spam and viruses. But today, many organizations must vie for customer loyalty and increased retention by creating new sources of revenue and complementary offerings through collaborative partnerships.

As businesses open their network infrastructures to deliver new and enhanced services to consumers through the Web, internal and external exposure to threats and fraud soars. Unfortunately, many enterprises lack a proven methodology to address the risks that arise from increased numbers of diverse users.

Externally, there are now more access points and therefore more opportunities to penetrate a network perimeter. For

example, a “man in the middle” may use phishing tactics to illegally obtain confidential consumer information.

Internally, a rogue insider can find more opportunities to capture valuable consumer information. For example, a dishonest employee may try to steal customers’ credit card information or Social Security numbers. Unscrupulous insiders may even penetrate business partners’ networks and capture their sensitive, proprietary data.

To embrace the new business opportunities made possible by exposing high-value services to customers and partners, you must take proactive steps to counter threats and prevent fraudulent activities — before they cripple operations or create negative press. And, you must be prepared to respond swiftly

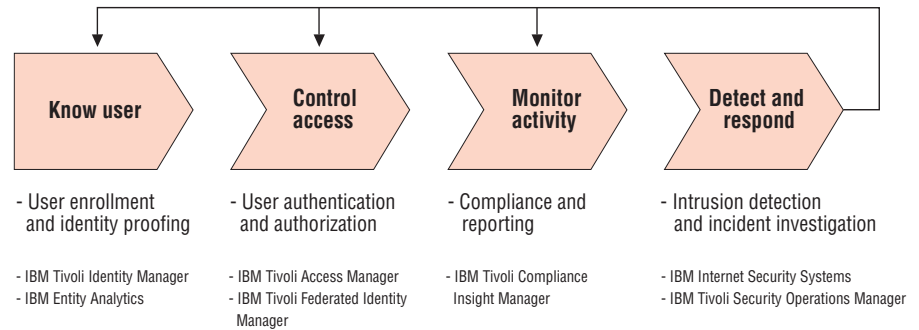
and effectively to any security breach that does occur. For ultimate success, you should link the solutions you use to defend your business with those that allow access to your IT environment.

IBM Tivoli® security management solutions offer a proven, comprehensive suite of tools and techniques that integrate threat and fraud protection with authentication. Use these solutions to:

- Establish a secure online transaction life cycle so you can confidently offer high-value services to customers and partners.
- Follow proven methods to verify and authenticate users.
- Know with confidence what users should and should not do.
- Monitor user behavior to mitigate risk and comply with internal and external policies.
- Pinpoint when and where a security event occurred, find out who did it and determine what damage was done.
- Link tactics that defend against security breaches with those that allow access for legitimate users.

Take a best-practice approach to the transaction life cycle

The demand for organizations to open their networks to consumers crosses industry bounds. Consider a government portal that allows citizens to pay



A best-practice approach to identity threats and fraud is with a comprehensive security management solution.

for toll roads online; a financial services firm that permits online stock trades; or an Internet merchant that sells thousands of books. To facilitate smooth, trusted online transactions, you must:

- Know the user.
- Verify the user and validate what the user is and is not entitled to do.
- Monitor the user's activity.
- Respond to threats and fraud quickly.

Tivoli security management solutions combined with IBM Entity Analytic Solutions give you a best-practice approach to building an end-to-end life-cycle solution that secures online transactions — from start to finish. As you reduce online risk by linking fraud detection with user authentication, you can confidently share information and applications with customers and business partners.

Know the user based on proven enrollment and proofing techniques

In the online world, you must make sure users are who they say they are, yet you don't want to frustrate legitimate customers with too many security layers. With IBM Tivoli Identity Manager, you can set up new accounts and passwords quickly to simplify the onboarding process. Then, use policy-based access control and automated user submissions and approval requests to decrease errors and boost efficiency. The software helps prove and manage identities through Web self-care, giving users smooth, trusted access to information and services.

Once you've enrolled someone, there are still opportunities for fraudulent users to capture an online identity, intercept a transaction and pretend

they're a legitimate customer. Imagine a customer who accesses an online merchant's site through a restaurant's wireless network. A dishonest person in the vicinity could intercept the real customer's user name and password to get access to their account information.

To ensure you know exactly who you're doing business with, you must employ strong forms of proofing. IBM Entity Analytic Solutions technology uses reliable proofing techniques based on real-time identity and relationship recognition and resolution in context with business applications to prove users' identities.

IBM Entity Analytic Solutions technology updates and manages evolving identities, detects and prevents fraud by recognizing multiple identities and accounts, flags suspect relationships and sends real-time alerts based on a user-defined rules engine. Incorporating industry-leading levels of security and privacy, the solution employs:

- IBM Identity Resolution to turn inconsistent, ambiguous identity and attribute data into a single, resolved entity across multiple data sets.
- IBM Relationship Resolution to link unique resolved identities to outside entities as a way to establish relationships and uncover criminal networks.

- IBM Anonymous Resolution to enable highly private and secure data sharing for customers, employees and partners.

Verify the user and understand what the user should and should not do

So you can confidently give customers access to Web applications, IBM Tivoli Access Manager for e-business uses single sign-on and a rules-based authorization engine as part of a common security model across the enterprise. This method automatically authenticates and authorizes users for appropriate transactions, and lets you centrally manage security and audit policies by collecting data at multiple enforcement points.

Because reliance on simple user names and passwords at login time is not sufficient to protect against "man in the middle" threats, IBM complements its authentication solutions with stronger forms of consumer and risk-based authentication from IBM Business Partners. For example, if a consumer logs into a bank's Web site to transfer money between accounts, the bank could use a transaction anomaly detection (TAD) engine to transparently assess the fraud risk of this activity.

The TAD engine collects information by fingerprinting the user's device, browser

and transaction behavior. Users who are considered high risk are prompted for further authentication or verification of the transaction. Legitimate users are not inconvenienced.

Fraud detection and risk assessment solutions can be driven by models, rules or a combination of both. When building a best-practice approach, businesses should consider a broad range of authentication and transaction verification methods to confirm — in real time — that users are who they say they are, and to make sure risky transactions are authorized. Enterprises should also consider integrating TAD engine scores into a cross-channel risk scoring engine that looks across channels like call centers and automated teller machines. And, they should select an appropriate site authentication tool to let users know they're not at a spoof site.

If your systems span multiple companies and security domains, you can use IBM Tivoli Federated Identity Manager to loosely couple identity and access management tools. With this software, different organizations can share identity and policy data about users and services to deliver a rich, secure experience for customers navigating between sites.

To stop illegal access, IBM Tivoli Access Manager for Operating Systems locks key applications, files and platforms — blocking insiders and outsiders from unauthorized access to and use of customer, employee and business partner data. The solution combines a full-fledged intrusion prevention firewall with user tracking and controls for auditing and compliance checks, so you can document compliance with government regulations, corporate policy and other security mandates.

Compare actual user behavior to policies using alerts and a dashboard view

By automatically monitoring user behavior and comparing it to established policies, IBM Tivoli Compliance Insight Manager helps you track, report and investigate noncompliance across the organization. Use the tool to monitor external users' behavior as well as the behavior of privileged users inside your organization who pose a major threat to your security. Through automatic alerts, you can ensure fast response to violations — whether information or technology assets are at risk, data or systems are accessed inappropriately or security policies are violated.

Tivoli Compliance Insight Manager includes a dashboard and reporting tools to help you measure security posture and respond to auditors' requests. The software gives easy-to-understand answers to key security questions such as who did what, when and where, where from, where to and on what. It also integrates with IBM Tivoli Security Operations Manager software and Tivoli identity and access management solutions to help you both recognize and optimize compliance and incident response.

Defend against and respond to threats and fraud quickly and cost-effectively

From IT managers to line-of-business application developers and enterprise architects, many people are caught up in the frenzy that follows a security breach. Because many companies rely on manual, disjointed solutions to protect against threat and fraud, the biggest challenge may be to determine when and where a breach occurred. Unlike piecemeal solutions, IBM security management solutions provide a comprehensive prescription for resolving security incidents that have touched your business. So you can respond rapidly and effectively to all types of events.

Leverage intrusion detection to identify breaches quickly

To rapidly identify breaches — from network perimeter points like branch offices down to the individual server level — use IBM Internet Security Systems (ISS) intrusion detection software. This software is particularly useful for protecting against the plethora of handheld devices that open new potential security “holes.” ISS also offers emergency response and 24x7 protection for companies that outsource security management.

Automate incident investigation across the enterprise

With the Tivoli Security Operations Manager platform, you can establish both a holistic and detailed view of security issues. The software stores relevant information from across the infrastructure in a centralized security event database, where it automatically analyzes the data and correlates security insights to detect threats and automate incident investigation and response.

Leverage the software's real-time dashboard to drill down and investigate attacks deeply. And use on-the-fly data mining, historical reporting, and

self-auditing and tracking capabilities to enforce security policies and support audit and compliance initiatives.

Tivoli Security Operations Manager software integrates with Tivoli identity and access management solutions to help ensure policies are enforced and misuse attempts are quickly detected and addressed.

Use closed-loop feedback to support a highly responsive security infrastructure

With comprehensive Tivoli security management solutions and IBM Entity Analytic Solutions technology, you can recognize and tackle a broad range of threats and fraud. Across the enterprise, our solutions link relevant security information that originates from individual applications and desktops to servers, networks and even business partner domains.

Because IBM solutions integrate fraud detection with user authentication, they deliver closed-loop feedback on your security posture. So, if someone steals John Smith's account number and starts to transact business using

that information, your defense solutions can detect the breach and notify your access solutions about the incident.

With an infrastructure that's highly resilient to a multiplicity of ever-evolving threats, you can confidently defend — and permit access to — high-value systems and applications.

Drive new, innovative business opportunities with confidence

Working together, modular IBM Tivoli security management solutions can help you win and keep new business, optimize resources and protect your IT infrastructure. Because they strengthen your ability to actively monitor, correlate and respond to IT security incidents, Tivoli security management solutions align security activities with top business priorities — and let you address broader security and privacy requirements, such as PCI, Sarbanes-Oxley, HIPAA and Gramm-Leach-Bliley requirements, EU privacy regulations and the U.S. Homeland Security "Know Your Customer" provisions.

Take advantage of a wide range of IBM services

IBM Identity and Access Management Services can provide extensive consultation, support and other services to help you manage growth and complexity, control escalating management costs and address the difficulties of implementing security policies across a wide range of Web and application resources. With IBM, you can develop appropriate policies for managing risk and build the capabilities needed to enforce those policies.



For more information

For more information about how your organization can use Tivoli security management solutions to help prevent threats and fraud, contact your IBM representative or IBM Business Partner, or visit ibm.com/software/tivoli/solutions/security/

About Tivoli software from IBM

Tivoli software provides a set of offerings and capabilities in support of IBM Service Management, a scalable, modular approach used to deliver more efficient and effective services to your business. Helping meet the needs of any size business, Tivoli software enables you to deliver

service excellence in support of your business objectives through integration and automation of processes, workflows and tasks. The security-rich, open standards-based Tivoli service management platform is complemented by proactive operational management solutions that provide end-to-end visibility and control. It is also backed by world-class IBM Services, IBM Support and an active ecosystem of IBM Business Partners. Tivoli customers and business partners can also leverage each other's best practices by participating in independently run IBM Tivoli User Groups around the world — visit www.tivoli-ug.org

© Copyright IBM Corporation 2007

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

Produced in the United States of America
9-07

All Rights Reserved

IBM, the IBM logo and Tivoli are trademarks of International Business Machines Corporation in the United States, other countries or both.

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

Disclaimer: The customer is responsible for ensuring 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 reader may have 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 or regulation.

TAKE BACK CONTROL WITH 