



Maximizing Return on Investment with Tivoli Security Management Solutions

— IBM, Tivoli Software

► Hurwitz Report



Maximizing Return on Investment with Tivoli Security Management Solutions

— IBM, Tivoli Software

iii Executive Summary

The Tivoli Security Management solution lends order to chaos by providing a security infrastructure from which to manage the many types of functions and needs in a security management program.

1 e-business Infrastructure Landscape

While a pieced-together foundation may satisfy short-term requirements, it is the carefully planned and designed infrastructure that provides the strategic benefit for tomorrow.

1 e-business Security Risks and Returns

Any e-business capability can be “peeled” to expose a number of complex layers, each with its own set of vulnerabilities.

3 Identity Layer ROI: IBM Tivoli Identity Manager

Identity management is the “bread and butter” of any enterprise security group and IT environment.

5 Network Layer ROI: IBM Tivoli Risk Manager

An effective deployment of IBM Tivoli Risk Manager can lead to the successful reduction in operating costs for any incident response team.

7 Application Layer ROI: IBM Tivoli Access Manager for e-business

IBM Tivoli Access Manager for e-business provides the access management capability to link together different types of users of a web site to the thousands of resources that are made available through the web application.

9 Transaction Layer ROI: IBM Tivoli Access Manager for Business Integration

IBM Tivoli Access Manager for Business Integration is designed specifically to provide scalability in access management to ensure that end users and other systems can make use of the functionality of real-time transactions in an appropriate manner.

10 Tivoli’s Benefits

The Tivoli Security Management solution provides foundational capabilities to protect an organization’s infrastructure.

11 Getting to Return with Tivoli Security Management

With IBM Tivoli Identity Manager, IBM Tivoli Risk Manager, IBM Tivoli Access Manager for e-business, and IBM Tivoli Access Manager for Business Integration, the benefit is realized through the common infrastructure.

12 Conclusion

Tivoli Security Management solutions provide a modular approach to security, offering building blocks that can be implemented in a consistent way.

A Hurwitz Group white paper written for:

IBM, Tivoli Software
11301 Burnet Road
Austin, TX 78758
1 877 TIVOLI1
Fax: 512 794 0623
www.tivoli.com/security

Published by:

Hurwitz Group, Inc.

111 Speen Street, Framingham, MA 01701 ► Telephone: 508 872 3344 ► Fax: 508 872 3355

Email: info@hurwitz.com ► Web: www.hurwitz.com

May 2002

© Copyright 2002, Hurwitz Group, Inc.

All rights reserved. No part of this report may be reproduced or stored in a retrieval system or transmitted in any form or by any means, without prior written permission.

EXECUTIVE SUMMARY

Security is an ongoing process. It is a state of dynamic events that requires constant attention. Often today, the attention provided comes in the form of literally tens to even hundreds of point solutions to individual security problems. These point solutions contribute to a highly complex security monitoring environment which only serves to exacerbate the problem.

The Tivoli Security Management solution lends order to chaos by providing a security infrastructure from which to manage the many types of functions and needs in a security management program. This Security Management solution provides a return on investment to organizations that deploy a standard solution for managing security events and controlling their e-business environment.

e-business Infrastructure Landscape

With the burst of the dot.com bubble, e-businesses began the next stage of their evolutionary lives. The overindulgence in all things “e” has led to a period of retrospection; a time to strategize on an enterprise e-business approach that is consistent with business goals. This business perspective, then, is reflected in the choice of technology architecture. These goals intersect in important areas.

Building a Sustainable Infrastructure

An unsustainable infrastructure is an oxymoron — sustainability is a crucial element to anything that can be called an infrastructure. While a pieced-together foundation may satisfy short-term requirements, it is the carefully planned and designed infrastructure that provides the strategic benefit for tomorrow.

Focus on Return

Clearly, “need for speed” has been replaced with “yearn for return.” Justification has become the mantra of e-business activities, providing the basis for moving forward with a project. Any strategic move within e-business must be properly evaluated.

Maximize Effectiveness

The complexity of e-business applications creates many areas where improvements are needed. The many individual point products “behind the scenes of” a web application are often overlapping or redundant in capabilities. Organizations must review their portfolio of products and code to identify key functional areas that will allow them to maximize their effectiveness, often through shared usage or enhanced applications.

Security Enables the Infrastructure

The need for security is indisputable. In the long-term, the trust and comfort that comes from a strategic, long-term investment in security, such as infrastructure, lays the foundation for solid business relationships with customers, suppliers, employees, and partners.

It is security that must be addressed in order to strengthen infrastructure and lead enterprises to the next stage of their evolution. Some important e-business security risks and returns are described below.

e-business Security Risks and Returns

Security Layers

e-business risks must be evaluated individually. Like compartments on a boat that are designed to limit the impact of hull damage, security must be designed to protect different

aspects of a computing environment, while at the same time helping a business generate quantifiable business returns. To better understand these aspects, it is useful to look at the several layers of e-business (see Figure 1), each with its own set of vulnerabilities — and potential for generating business returns.

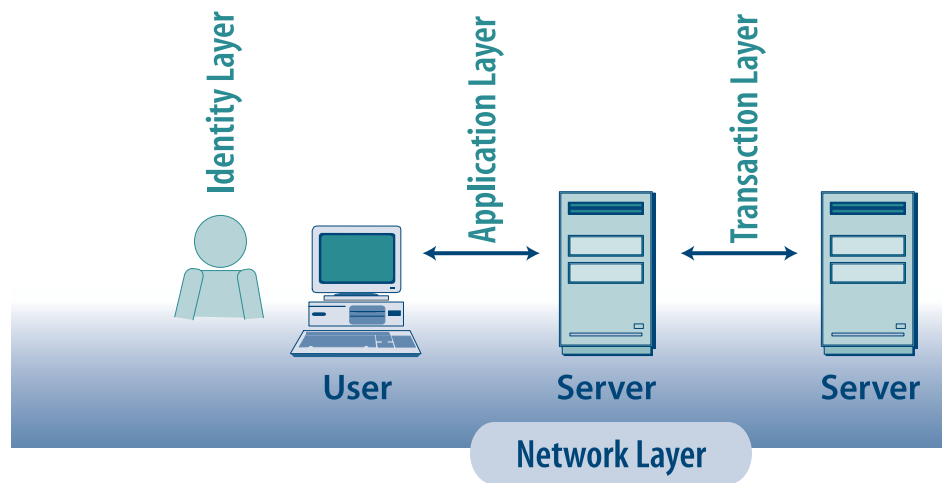


Figure 1: Security layers within an organization.

Identity Layer

Many firms today struggle with managing identities consistently across their portfolio of applications and servers. Because a given customer, employee, or partner typically has unique electronic identities created and administered individually for each of these platforms, the risk of inefficiencies and high costs is significant.

From the security perspective, identity fraud happens all the time. Sometimes we don't call it identity fraud; we call it "borrowing somebody's user account." Often an identity can be misappropriated due to weak password controls. Regardless, identity management is about efficiently providing access to authorized users while eliminating the possibility or capability that the user's identity will be misappropriated due to process errors. User identities are the primary form of online credential, and the system only "knows" a user based on these identities and their corresponding passwords (or other authentication form, such as digital certificates or token cards). The workflow and provisioning capabilities of managing user identities must be evaluated to ensure that only properly verified individuals receive and retain an identity on the system throughout that user's lifecycle, and that passwords (or other authentication forms) are managed appropriately.

Network Layer

At its core, a network facilitates the breaking down of information into millions of data packets

that are transmitted and reassembled at their destination. For this process to work effectively, with billions and billions of packets flowing across the Internet, protocols are designed and control information must be passed along with each packet. These packets can be created with malicious intentions, modified in transit, intercepted and “spoofed,” or acted upon in some other way that attempts to impact the appropriate communications to some inappropriate end — and hence impact business availability. There are thousands of known and uncountable unknown ways to exploit damaging activities occurring at the network layer.

Application Layer

Web portal applications comprise the primary path into organizations today, whether it is through the Internet or an intranet. One reason for this popularity is that web applications are made of a number of different components, making them highly flexible and adaptable to many different development environments. But this flexibility also makes them difficult to control. So the numerous programs that manifest themselves to the end user as a series of web objects and pages must each be evaluated for the appropriate access rules to ensure that end users only gain access to those objects to which they are authorized. Unfortunately, businesses have traditionally accomplished this task by writing customized security code into each program, which increases deployment time, application development costs, and ongoing administrative costs.

Transaction Layer

The transaction is quickly becoming a core element to web applications. New technology and the maturing of a collaborative environment like the Internet have combined to enable real-time transactions as a way to pass data. What was once a closed application environment, often with functional layers residing on the same server, has turned into the passing of real-time transactions from server to server across the Internet. Individual transactions must now be evaluated as purchase orders, balance transfers, treasury functions, and other request and response activities being transmitted to business partners, suppliers, vendors, and other entities. The infrastructure must support ways to ensure that these transactions remain safe from source to destination, to protect against spurious activity.

Identity Layer ROI: IBM Tivoli Identity Manager

Overview

Identity management is the “bread and butter” of any enterprise security group and IT environment. User identities are the primary authentication vehicle for authorized users to get to appropriate resources. It also tends to be a process ripe with inefficiencies born from lack of technical knowledge on the users side — they just want to do their job; and lack of specificity for IT administrators — they need specifics to provide the appropriate access. Identity

management automates process and workflow to provision identities across multiple systems based on rules that are defined in the system.

Capabilities

IBM Tivoli Identity Manager covers critical aspects of identity management:

- ▶ **Self service.** Because the user identity is the credential of choice online, a problem with the credential requires immediate attention. The best way for support environments to provide this is through self-service that allows end-users to tend to their needs automatically so they can return to a productive work state. Self-service is also important for routine user profile maintenance, such as updating a user's telephone number.
- ▶ **Workflow.** When new identities are created or new systems are implemented, workflow ensures that the appropriate people approve the request. Application owners, system administrators, and other functional "gatekeepers" likely have a stake in who is requesting access. Workflow keeps the process flowing smoothly.
- ▶ **Provisioning.** User identities must often be created on multiple systems to support application functionality and standard user requirements. A provisioning system can "kickstart" this process by creating the identities necessary on the appropriate systems.
- ▶ **Centralized management and user data storage.** Organizing the user data and providing delegated administration capabilities that map into the everyday management of the environment are essential for the deployment of a strategic solution of this kind.

Benefits

The benefits are clear:

- ▶ **Lifecycle management.** Users change jobs and responsibilities constantly. IBM Tivoli Identity Manager helps control and manage their respective user identities from creation to termination.
- ▶ **Increased responsiveness.** A problem with a user identity puts a worker out of action. A typical example is a problem with passwords, or the need to reset a password. Responsiveness to these problems is key to productivity in the computing workplace.
- ▶ **Automated routines.** Human error in processes and judgments often occur when timeliness is important. To automate routine functions ensures that the programmed decision is always made and the correct process is followed for every transaction.
- ▶ **Leveraged identity information.** Identity information must be manually gathered for many activities, such as security audits, access reports, and even billing transactions. Centralizing and consolidating validated user identity data creates an efficient process when these management activities take place.

Elements of Return

The return for IBM Tivoli Identity Manager can be significant since every organization must issue user identities and the process can be complicated. Identity fraud and “social engineering” are common techniques in security attacks because systems don’t know who is actually using a specified user identity.

Service and support centers interact with users, and a large percentage of the calls they receive are associated with user identity issues. Return is quickly realized in a number of ways:

- ▶ **Speeds up time-to-productivity.** New customers, employees, or contractors must wait for identities to be created. Real-time productivity gains occur when these identities are provided quickly, with little opportunity for errors or “cutting corners.”
- ▶ **Reduces administrative errors.** Help desks and user administration teams are deluged with problems to be solved. Sometimes the expedient way to get things done is to “bend the rules” or interrupt a process. When processes fail, errors occur. An automated system consistently follows the same process.
- ▶ **Eliminates help desk calls.** Help desks calls are easily quantifiable. With costs often reaching \$20 or more per call, reductions can be measured easily in the nature of the calls. Routine calls can be replaced through self-service, thus allowing help desk employees to refocus their efforts on more significant system problems.
- ▶ **Optimizes administration needs.** Applying the capabilities for delegated administration and self-service, while retaining central control, can create an optimal identity management approach — creating identities at the business unit level and terminating identities from a central place.
- ▶ **Makes identity information useful and usable.** User identity information can be valuable for audit and billing purposes. A central administration tool makes it easier to identify usage information, resulting in a more efficient process for the many scheduled and ad-hoc reporting needs of an organization.

Network Layer ROI: IBM Tivoli Risk Manager

Overview

Risks at the network layer are often addressed through the use of intrusion detection systems (IDS). With the complexity of networks today, sensors or agents must be deployed by the dozens. In addition, other devices like firewalls and network routers have their own alerting capabilities. The way to maximize effectiveness in this space is through the consolidation of the event logs into a single database and the correlation that links together similar events from multiple devices.

Capabilities

IBM Tivoli Risk Manager collects events from devices and sensors throughout the environment. Key capabilities include:

- ▶ **Support for a multitude of devices and sensors.** Aggregating events from sensors throughout an enterprise reduces the number of management interfaces to one. There is no need to constantly refer to many consoles while troubleshooting or diagnosing a problem.
- ▶ **Centralized correlation of intrusion alerts.** Because multiple devices have differing views of the environment, the ability to collect data and relate events to each other provides critical insight into individual attacks. Correlation ensures that significant events are not lost in a sea of unimportant ones.
- ▶ **Centralized archival of security alerts.** Time provides context in intrusion events that helps ensure the lasting security of an environment. Archival capabilities ensure that activity can be reviewed for trends that assist with future planning.
- ▶ **Support for all intrusion detection standards efforts.** Standards efforts in intrusion detection ensure that necessary event information will be passed from multiple sensors to aggregation points. IBM Tivoli Risk Manager supports the common intrusion detection format (CIDF); intrusion detection exchange format (IDEX); and the common vulnerability and exposure (CVE) standards.

Benefits

- ▶ **Quicker response during an attack.** The correlation of events turns information into knowledge. This knowledge, in turn, allows for a quick response. Overall, response effectiveness is improved.
- ▶ **Higher event visibility.** Visibility is perhaps the key ingredient to understanding events across a network. The expanse and complexity of networks creates a dormant confusion that can be overcome through correlation.
- ▶ **Strengthened security.** The end result of enhanced intrusion detection and response capabilities is an increased ability to identify and respond to threats. This threat response strengthens the overall level of security in an environment. In addition, the consolidated information that this solution offers enables easier compliance with security audits.

Elements of Return

Return on investment for IBM Tivoli Risk Manager is most obvious for organizations that have invested in firewalls, intrusion detection devices, and other tools that create event logs. These logs provide insight into the activities of an organization, but their usefulness is limited amidst the multiple consoles and individualized approach to the events. The centralized approach of IBM Tivoli Risk Manager provides return on investment in a number of areas:

- ▶ **Quickens intrusion response time.** With the ability to immediately evaluate the context of an attack, enterprises should be able to speed up responses, and focus efforts well. Efforts may be reduced by 10% or more — a significant amount in the face of real-time threats.
- ▶ **Reduces forensics time.** One of the more difficult aspects in intrusion detection is fully identifying the impact of an incident. In a large-scale enterprise, time may be reduced by over 40%.
- ▶ **Eliminates “false alarms.”** More correlation provides better insight into the probability that an attack is taking place. The numbers of false alarms will differ greatly in an enterprise, depending on deployment of sensors, but a target of 25% to 50% reduction in false alarms is reasonable.
- ▶ **Eliminates multiple consoles and user interfaces.** As logging devices increase in numbers, a single interface increases in value. Enterprises should target savings that are consistent with the “straight line” reduction in a number of consoles, i.e., moving from three consoles to one should result in 66% savings in time/effort, plus a buffer for follow-up work.

An effective deployment of IBM Tivoli Risk Manager can lead to the successful reduction in operating costs for any incident response team.

Application Layer ROI: IBM Tivoli Access Manager for e-business*

Overview

For all of their easy-to-use features on the user side, web sites are tremendously complex “under the covers.” Markup languages, scripts, servlets, and other objects can statically or dynamically drive the presentation of web pages to a user. Different sections of the page can be pulled from multiple servers and sites, even legacy systems. On the user side, job functions and relative location to the resources can drive complexity. Certainly, when users must access some subset of all the different objects and resources from multiple sources, access control becomes a critical issue.

IBM Tivoli Access Manager for e-business provides the access management capability to link together different types of users of a web site to the thousands of resources that are made available through the web application. IBM Tivoli Access Manager for e-business gives critical visibility into the access rights that are granted to users of any particular resource.

* These same benefits and returns are available to applications running natively on many of the popular UNIX and Linux servers through IBM Tivoli Access Manager for Operating Systems, a companion product to IBM Tivoli Access Manager for e-business.

Capabilities

IBM Tivoli Access Manager for e-business has several key capabilities:

- ▶ **Web single sign-on.** Web applications are everywhere. Individuals are launching browsers as their primary interface to enterprise and e-business applications. IBM Tivoli Access Manager for e-business eliminates the need to re-authenticate to individual applications.
- ▶ **Centrally-defined security policy.** A single interface for all web applications provides consistency in security policy. Rules can be set within a central location to be applied across applications.
- ▶ **Transparent access control policy enforcement.** The transparency of approved access requests allows users to remain productive even with the enhanced security. The result of a successful access request is non-interfering, going completely unnoticed by users.

Benefits

- ▶ **Stronger security life cycle.** The increased visibility that comes with centralized web access control provides a better way to control user access to resources. The consistent approach provides security strength by making the control elements accessible and manageable.
- ▶ **Controlled e-business environment.** Organizations must retain control over the entire e-business environment as they migrate management to a standard operations staff, as part of normal capabilities for information services departments.
- ▶ **Centralization and integration in a security environment.** Security is about ongoing management. IBM Tivoli Access Manager for e-business provides the level of centralization and integration required to enhance management throughout the e-business environment.

Elements of Return

Developers often act independently of each other, with specific projects being managed separately from others. As a result, applications are written with completely different security mechanisms and vulnerability potential that is difficult to measure. IBM Tivoli Access Manager for e-business allows the standardization of access control that not only strengthens security, but also ensures visibility into the environment. Savings can be gained in the following ways:

- ▶ **Reduction of application development and deployment time.** No matter how many applications are developed, the security mechanism is only developed once. Savings

should be consistent with the number of applications being developed, with savings of over 50% in the application development time devoted to security reasonable for large-scale enterprises.

- ▶ **Reduction of labor costs of access management and administration.** Labor is a function of training and process. With IBM Tivoli Access Manager for e-business, training is only required on one security system, and the process remains the same for any new applications. Savings are again greater with larger deployments due to scalability gains, with 50% being a good target. One customer surveyed reported a 61% reduction in help desk calls for web password resets.
- ▶ **Reduction of routine maintenance and upgrade costs.** As with the other savings, the benefits are derived from providing a single source rather than multiple places to perform activities like maintenance. Based on customer feedback, 50% savings can be gained in the time spent maintaining security systems.

The return to the e-business group is apparent when many different applications are being developed and challenges across applications are similar. IBM Tivoli Access Manager for e-business embraces those similarities to make security support consistent and efficient.

Transaction Layer ROI: IBM Tivoli Access Manager for Business Integration

Overview

In the newest generation of the Internet, web applications are transaction-oriented. That means that transactions must be passed in real-time or near real-time from a local host to any of a number of repositories and sources. IBM WebSphere MQ provides the scalability and failover capabilities necessary to ensure that all transactions get to their destination but stops short of maintaining the integrity of the data in the transaction.

IBM Tivoli Access Manager for Business Integration is designed specifically to provide data protection and access management services to ensure that end users and other systems can make use of the functionality of real-time transactions in an appropriate manner. These services are provided in a way that does not impact a customer's existing WebSphere MQ applications or the WebSphere MQ environment itself.

Capabilities

- ▶ **Controls entrance and exit points.** Queues provide the waystations for transactions. IBM Tivoli Access Manager for Business Integration provides the control over the source and destination queues that ensures the safe transfer of data.
- ▶ **Authenticates the message.** Any attempt to spoof the origin of a message is thwarted through the authentication of the message source.

- ▶ **Ensures message integrity.** Spoofing a message's contents is also addressed, since IBM Tivoli Access Manager for Business Integration verifies message integrity by employing message hashing and digital signatures.
- ▶ **Protects confidentiality.** Encryption can be deployed for any messages that are confidential. This ensures that organizations can pass messages over unprotected networks like the Internet without revealing data that may be sensitive.

Benefits

- ▶ **Message security.** At the transaction layer, the message is the data. IBM Tivoli Access Manager for Business Integration provides strong security over messages transferred within a WebSphere MQ environment.
- ▶ **Centralized management.** As messages are used to share data among many different applications, the complexity is increasing geometrically. IBM Tivoli Access Manager for Business Integration provides central management over access control for the critical message queues that control message traffic.
- ▶ **Visibility.** Again and again, visibility ensures the appropriate level of security. Insight into the message traffic enhances visibility and provides for future security planning.

Elements of Return

The return on investment with IBM Tivoli Access Manager for Business Integration is gained in the same way as with IBM Tivoli Access Manager for e-business. The difference is in the resources that are being managed. IBM Tivoli Access Manager for e-business manages URLs and objects, while IBM Tivoli Access Manager for Business Integration manages messages. Accordingly, the return is associated with ease-of-management and -maintenance.

IBM Tivoli Access Manager for Business Integration derives its specific return information directly from the complexity of an environment, with more complexity resulting in greater returns, due to the consistent, single management interface.

Tivoli's Benefits

The Tivoli Security Management solution provides foundational capabilities to protect an organization's infrastructure. In many ways, security is a horizontal requirement, providing an infrastructure of support across all applications and systems. Tivoli Security Management embraces this breadth by providing a management platform to support it.

Multiplatform Support

Perhaps the most important criterion for any management software is platform support. Platforms can include any operating system, database, or application that provides critical

information processing for an organization. Tivoli Security Management supports many different platforms and routinely adds new platforms.

Enhanced Management Controls

Organizations today are seeking out ways to limit redundancies and reduce costs. The breadth of the solution that is offered along with a management platform also provides visibility into an organization's management functions. This visibility can highlight various areas that are redundant or inefficient. The Tivoli Security Management solution can also take silos of processing functions and centralize them or redistribute them for maximum effectiveness.

Security Life-Cycle Management

The Tivoli architecture also leads to enhanced life-cycle management for security functions. In a typical operational environment, security functions are highly reactive — the threat du jour becomes the focal point of activity. Often, there is little time to get ahead of daily activities to create a more strategic approach to these threats. Tivoli Security Management solutions provide the insight into many security functions so that activities can be tracked and deployed in a strategic fashion.

Security Infrastructure Building Blocks

The Tivoli architecture is designed to provide building blocks that scale in alignment with business processes. This architecture leads to lower administrative costs over time. In addition, it provides the control and comfort necessary to enable the use of new technologies. The long-term investment in security provides a return to the entire computing environment.

Getting to Return with Tivoli Security Management

Generating a return with security solutions is a difficult proposition. Often, the goal is to reduce risk, which can be a nebulous concept not easy to quantify. With IBM Tivoli Identity Manager, IBM Tivoli Risk Manager, IBM Tivoli Access Manager for e-business, and IBM Tivoli Access Manager for Business Integration, the benefit is realized through the common infrastructure. The specific benefits include:

- ▶ **Efficient development of business applications.** Reinventing the wheel is a common problem in development, particularly with security. This creates the likelihood of a large variance in quality, which subsequently contributes to vulnerabilities. Tivoli Security Management takes away the guesswork in security development by providing a consistent interface from which to develop and manage applications.
- ▶ **Reduced cost of security management efforts.** There are numerous activities in security management that must be routinely completed to ensure strong security. These activities are consistent throughout the computing environment, thus, a

security infrastructure solution provides a best practices approach to act consistently with all platforms.

- ▶ **Reduced cost of security deployments.** Once a security infrastructure is implemented, security deployments become less complex to implement. Within a short period of time, savings can be significant, and the corresponding security coverage enhanced drastically.
- ▶ **Reduced security life-cycle costs.** Upgrades, new additions, and standard maintenance are easier when working with a console that provides a comprehensive view of the security environment. Tasks associated with security, such as monitoring for intrusions or managing access rights to the Web or messaging environment are simpler to perform, and therefore less costly.

Conclusion

The need for security is apparent, but the need for a security infrastructure can be even more important. Infrastructure provides sustainability — a consistent approach to security that can be replicated time and again across networks, applications, and transactions.

Tivoli Security Management solutions provide a modular approach to security, offering building blocks that can be implemented in a consistent way. User identities are consistently created and managed by IBM Tivoli Identity Manager, which provides workflow and provisioning for a controlled identity management process. Addressing network layer risks, IBM Tivoli Risk Manager makes sense of numerous security events from multiple devices. For the application layer, IBM Tivoli Access Manager for e-business offers control over user access to resources on the Web. And in the high-risk area of transactions, IBM Tivoli Access Manager for Business Integration lends the control necessary to ensure that messages get safely from origin to destination.



About Hurwitz Group

Hurwitz Group, an analyst, research, and consulting firm, is a recognized leader in identifying and articulating the business value of technology. Known for its real-world experience, consultative style, and pragmatic approach, Hurwitz Group provides strategic guidance to its clients by delivering analysis, market research, custom content, and consulting services. Clients include Global 2000, software, services, systems, and investment companies.