Tivoli software

IBM

IBM Tivoli Software Business Partner Sales Guide - Security

Your Pocket Guide to Sales Effectiveness

Purpose of this Guide

How can you more effectively sell Tivoli Security Management solutions? What's the best way to introduce your customer to Tivoli?

This pocket sales guide can help you better understand and convey the IBM Tivoli value proposition when selling Tivoli Security solutions. From a sales perspective, the guide delves into each solution area within Security and identifies the benefits and ideal prospects per product. It offers strategies for selling and helps clarify the right messages.

Most importantly, this guide is designed to help you succeed by increasing sales and better penetrating accounts. Whether you are new to the Tivoli sales team, or a seasoned professional, this sales guide will give you valuable insight into how to position the latest products and enhancements for increased sales success.

Think of this sales guide as your cheat sheet for answering the following questions:

- What can Tivoli offer my customers?
- Why are Tivoli Security solutions better than the competition?
- How do I determine which solutions my customers need?
- How can I leverage IBM presence to cross-sell additional Tivoli solutions?

TIP: Tivoli's value proposition is best delivered to the "C" level executive in mid- to large-sized organizations.

Contents

In this sales enablement guide for Tivoli security solutions, you'll find:

Market Drivers and Overall Customer Pains

Organizations' user communities continue to multiply

As a result, managing identities throughout their entire lifecycle has become a complex, management-intensive process. Administrative costs, including help desk costs, and staffing requirements for user account provisioning and de-provisioning skyrocket.

To remain competitive, organizations must develop and deploy secure e-business initiatives fast

Incorporating security into new applications delays deployment and increases development costs. Organizations need a cost-effective security methodology that allows them to go to market faster with new e-business initiatives.

Security attacks are on the rise

According to Riptech, a Virginia-based security services firm, Internet attacks grew at an annualized rate of 64 percent during the period between January 2002 and June 2002. The average company experienced 32 attacks per week in the first half of 2002. Security is a problem that is not going away.

Failing security audits

More companies today are failing audits for not knowing or being able to identify or quantify attacks, virus spreads, or even the more basic "failed" logons or improper access to sensitive or confidential enterprise data.

The need for security is widespread

Security breaches happen in every vertical and in both private and public sectors. However, high tech, financial services, and power and energy industries lead with more attacks than any other industry vertical.

Security spending isn't commensurate with growth rate for attacks

According to Gartner surveys*, information security budgets average between 3 percent and 5 percent of overall IT budgets. As the threat and number of attacks outpace the resources dedicated to fighting breaches, organizations need to find more efficient and cost-effective methods for implementing and maintaining security measures.

* Gartner Letter from the Editor, "Safety First for Information Security Solutions," on June 14, 2002 by Vic Wheatman and Arabella Hallawell.

Elevator Pitch

The Tivoli pitch

Intelligent management software that integrates and automates

Tivoli strategy is driven by customer needs to 'do more with less'—focusing on Integrated Management, Autonomic Computing, Best Practices and Rapid Deployment to generate the greatest return on investment. IBM Tivoli software helps customers leverage their IT investments to achieve the greatest impact to their business by bridging the gap between the revenue-producing side of the business and the technology side. The focus of IBM Tivoli's solutions is on growing the business—improving predictability, lowering total cost of ownership, increasing accountability, and maximizing service levels—all to provide businesses the ability to work more efficiently. IBM Tivoli software helps traditional enterprises and e-businesses worldwide manage security, storage, performance and availability, and configuration and operations.

The Tivoli Security Management Solutions pitch

Tivoli security management solutions address the most prevalent business pains caused by the manual management of users across their lifecycle—higher help desk costs, higher admin costs, and higher development costs. Tivoli addresses these pains by automating and centralizing the management of users and perimeter network security administration, and in so doing, increases productivity and satisfaction through single sign-on and self-care for users and enforcement of security policy.

IBM Tivoli software for autonomic computing

Autonomic computing is the ability of systems to dynamically adapt to change in accordance with business policies and objectives. To be autonomic, a computing system needs to know detailed information on its various components, all available resources, current status, ultimate capacity, and connections with other systems. Tivoli's security management solutions include self-correcting functionality that reduce the need for human intervention and minimize the costs associated with enterprise security management.

What makes the IBM Tivoli Security Management Solutions Unique?

- Best-of-breed* integrated solutions for Identity Management and Security Event Management
- Fast ROI through industry-leading support for heterogeneous applications and systems
- Autonomic Computing

* based on Gartner Extranet Access Management Magic Quadrant Research Note (February 2002) and Gartner Provisioning Vendor Selection Tool (September 2002)

Why sell security solutions?

To make $$$$!

"This security focus will translate into an $80 billion market in 2002 and will cause worldwide spending on IT security/business continuity to grow twice as fast as IT spending in general. IDC believes spending will more than double in five years, growing from $66 billion in 2001 to $155 billion in 2006."

IDC Press Release, "IDC Finds IT Security and Business Continuity Market Poised to Double in Size by 2006," October 28, 2002

"Information security is not a discretionary purchase. It is as essential to the enterprise as the enterprise's mission and its employees' dedication."

Gartner Letter from the Editor, "Safety First for Information Security Solutions," on June 14, 2002 by Vic Wheatman and Arabella Hallawell.

Solution and Product Overview

Tivoli security solutions address our customers' security challenges across two different areas:

Solution	Description
Identity Management	The IBM Tivoli Identity Management solution directly addresses the need to manage an increasing number of users—customers, employees, partners and suppliers—despite having fewer resources. Through its automated and centralized approach to identity management, it enables faster deployment of new e-business initiatives. The products in this solution include: IBM Tivoli Identity Manager, IBM Tivoli Access Manager for e-business, IBM Tivoli Access Manager for Business Integration, IBM Tivoli Access Manager for Operating Systems, IBM Tivoli Privacy Manager for e-business and VeriSign Managed Services.
Security Event Management	The IBM Tivoli Security Event Management solution protects e-business infrastructures by improving response time to security threats—monitors IT resources across the e-business, filters and correlates alerts, and automates responses to security events. It enables centralized management for more efficient and cost-effective security. The products in this solution include: IBM Tivoli Risk Manager, IBM Tivoli Intrusion Manager and IBM Tivoli Enterprise Console.

Product Drill-down

Identity Management

Product	Ideal Prospects	Customer Benefits
Identity Manager *Tip:Since the Access360 acquisition, product functionality has improved considerably. Work with all current Identity Manager customers to upgrade them to v4.x and higher!*	• Are IT operations or IT security professionals • Are responsible for successfully completing security audits • Must lower user administration and help desk costs • Are CxOs and senior executives with initiatives to streamline costs and/or enhance revenues	• Reduces administrative costs with centralized user management • Reduces help desk costs and increases customer productivity through end-user self-help • Delivers fast ROI and operational productivity by automating the user management lifecycle through workflow and delegated administration • Decreases errors and inconsistency by auditing security policy implementations and automating business processes
Access Manager for e-business	• Have responsibility for IT application architecture, IT operations or individual business units • Are responsible for enterprise security • Are charged with incorporating security quickly into new e-business applications and getting new apps deployed faster • Are CxOs and senior executives with initiatives to streamline costs and/or enhance revenues	• Reduces deployment time and costs for new e-business initiatives through unified access management capabilities • Increases customer productivity and reduces help desk costs through single sign-on to e-business initiatives • Increases e-business connectivity through standards-based support for Web Services
Access Manager for Business Integration *Tip: Develop a good working relationship with the SAM rep for WebSphere MQ in your customer accounts to find out when MQ is sold. Focus on companies in industries that deal with sensitive information—finance, insurance, healthcare and the government sector.*	• Manage WebSphere MQ environments for large enterprises in finance, insurance and healthcare industries and the government sector • Are global system integrators working on WebSphere MQ integration projects • Are responsible for security • Need to ensure a high degree of security for e-commerce transactions • Must provide protection for messages in transit • Need to demonstrate HIPAA compliance • Are CxOs and senior executives with initiatives to streamline costs and/or enhance revenues	• Optimizes the use of development resources • Reduces costs by streamlining development of new applications • Enhances overall security • Minimizes business exposure and liability • Delivers immediate ROI upon deployment

Product	Ideal Prospects	Customer Benefits
Access Manager for Operating Systems	• Have responsibility for IT operations • Must protect critical production servers from security attacks • Are CxOs and senior executives with initiatives to streamline costs and/or enhance revenues	• Reduces administration costs • Speeds implementation via best-practices policy definitions • Increases systems integrity • Improves efficiency of administration
Privacy Manager for e-business	• Are responsible for minimizing corporate liability with respect to privacy issues and complaints • Must adhere to privacy policies and user preferences • Are CxOs and senior executives with initiatives to streamline costs and/or enhance revenues	• Minimizes risk and exposure for disclosing private customer data • Increases customer trust • Enhances corporate image • Lowers application development and administration costs
VeriSign Managed Services	• Are responsible for enterprise security management, but do not have sufficient resources in-house to deploy and maintain security solutions • Are CxOs and senior executives with initiatives to streamline costs and/or enhance revenues	• Improves user convenience and efficiency • Minimizes unauthorized users • Improves help desk productivity • Reduces operation costs and risks

Security Event Management

Product	Ideal Prospects	Customer Benefits
Risk Manager	• Are responsible for managing security across the organization and/or IT operations • Must improve audit compliance • Struggle to lower administration costs • Are CxOs and senior executives with initiatives to streamline costs and/or enhance revenues	• Speeds response times to threats • Helps avoid loss of revenue due to downtime • Mitigates security risks • Provides rapid time-to-value • Offers ability to more cost-effectively manage and address threats
Intrusion Manager	• Manage Internet and network security for mid-sized company • Must minimize security breaches • Need to more quickly pinpoint cause of breaches • Are CxOs and senior executives with initiatives to streamline costs and/or enhance revenues	• Simplifies monitoring by bringing together data from a variety of security products • Reduces response times to Web or network threats
Enterprise Console	• Manage massive interconnected systems • Struggle with resource constraints and staffing shortages • Are responsible for system and network performance and availability • Need to understand traffic patterns in order to create and maintain an optimal network • Face shrinking support budgets and staff • Are CxOs and senior executives with initiatives to streamline costs and/or enhance revenues	• Accelerates problem resolution and reduces reliance on experienced support staff • Reduces wasted network traffic • Maximizes system performance and availability • Enables efficient problem resolution without operator intervention

Sales Strategies

Successful selling of Tivoli's security solutions involves four key steps:

1. *Determine what the customer's compelling business issues are*
   Are they trying to reduce security-related administration and help desk costs? Do they need to improve audit compliance? Have there been privacy-related issues that caused negative publicity for the company? The best way to start a conversation with a prospect is by focusing on the immediate issues and challenges he or she is facing.

2. *Develop the unique business value for the preferred Tivoli solution*
   Once you've identified the customer's pains and have mapped those to a Tivoli security solution, make the business case for that solution. Talk to colleagues to find customers with similar challenges who have implemented the same solution. Use their experience, as well as Tivoli's ROI Analyst Tool to project ROI measurements for your particular customer.

3. *Construct an Evaluation Plan and gain the approval to proceed from the power sponsor at the prospect*
   Once you've demonstrated unique business value, including ROI, develop and obtain agreement on a detailed evaluation plan with your power sponsor that will enable them to successfully deploy the solution in their organization. Leverage useful tools such as the ROI Analyst, Gartner Provisioning Vendor Selection Tool, Gartner Extranet Access Management Magic Quadrant Research Note, and the other compelling sales aids available on eXtreme Leverage.

4. *Execute the Evaluation Plan and close the business*
   Customers who evaluate Tivoli security solutions are much more likely to buy. It's the perfect way to demonstrate Tivoli's value and take the customer to the next step in the sales cycle—product purchase.

Identifying Opportunities

Customer Need	Tivoli Solution	Sales Advantage
As my company grows and our user community expands, my help desk costs are getting out of control.	Tivoli Identity Manager and Tivoli Access Manager for e-business	Tivoli Identity Manager helps reduce help desk costs through centralized user management, password synchronization and end-user self-help for password resets and account updates. Additionally, Tivoli Access Management for e-business helps reduce help desk costs through single sign-on to Web resources.
I'm torn between the mandate to deliver new e-business applications quickly and make sure they are secure. I need a way to do both while supporting web services	Tivoli Access Manager for e-business, Tivoli Access Manager for Business Integration and Tivoli Access Manager for Operating Systems	Help your customers quickly deploy e-business initiatives by removing the need to write security rules in every application, while delivering single sign-on for users and Web Services support for developers. Extend this model to support messaging queues as well as the operating system level with Access Manager for Business Integration.
Our e-business presence is expanding rapidly. I need to make sure my portals and e-business applications are protected.	Tivoli Access Manager for e-business, Access Manager for e-Business and Access Manager for Business Integration	This product provides a single security model across WebSphere Application Server, WebSphere portal, WebSphere MQ, PeopleSoft Portal, Siebel 2000 and many other Web applications—something no other solution can provide.
Users have been complaining more and more about having multiple logins. I can't minimize security, but I need to improve user satisfaction.	Tivoli Access Manager for e-business and Tivoli Identy Manager	Tivoli Access Manager for e-business delivers secure single sign-on to e-business initiatives. If your customer is concerned about user satisfaction and the user experience, Tivoli Identity Manager provides a host of self-service functionality and automates workflow so users can quickly establish and update identities and access rights.
We are spending way too much time analyzing and chasing false alerts and we're failing security audits because we're not able to properly address everything. We struggle with identifying what is really occurring in our network and tracking unauthorized access.	Tivoli Risk Manager	Risk Manager provides an effective security dashboard for managing the massive amount of information that network security tools generate. Risk Manager can also work with several other Tivoli security products, such as Access Manager for e-business when audits are related to access control, Access Manager for Business Integration, Access Manager for Operating Systems, Identity Manager and Privacy Manager.

Handling Objections

Possible Objection	Your Answer
I currently have different products that collectively do the same things as your solutions. Why should I purchase Tivoli?	Right now you are using a variety of different products that require manual effort to get them to work together. Moving forward and adding new capabilities to this environment will continue to become more difficult and costly. Tivoli solutions are open for easy integration, plus they come with a data repository that is designed to capture data in a way that is easy to access and use. Additionally, Tivoli's solutions are recognized as best-of-breed solutions!
I know of some quality and functionality issues in the past with Tivoli products—what's different today?	IBM Tivoli has dedicated significant resources to ensuring quality and our goal is to offer solid, reliable, and highly functional solutions. Our acquisition of Access360 in 2002 is an example of our commitment to enhancing functionality.
I like the ROI story you're telling, but the cost of entry is too high for me right now.	Tivoli's approach is designed to lower costs and increase revenues both immediately and over the long term. Customers can recognize ROI immediately through capabilities such as single sign-on, self-help, and automated user provisioning, all while building a more cost-effective enterprise. And once the technology foundation is in place, synergies are created and benefits multiplied when implementing future initiatives.
If I go with an all IBM Tivoli solution, will I miss out on "best-of-breed" benefits?	Tivoli's security management solutions are best-of-breed today. Additionally, each component of Tivoli's solution in and of itself is highly functional, solid technology. Used together, the benefits increase dramatically. But, that's not to say that you can't add in other vendor's products to the mix. Our open architecture allows you to do just that.
The Tivoli solution may work with my current environment, but what about tomorrow?	Tivoli's solutions are highly scalable and are designed to grow seamlessly in any organization. Additionally, we provide tools that allow you to customize functionality and build special hooks that allow you to connect virtually any database, application, and middleware to our solution.
IBM WebSphere MQ V5.3 can secure my sensitive data using SSL, why do I need to license AMBI?	The native data protection services in WebSphere MQ are down at the transport level, not the application level. This leaves gaps in protection and audit ability while messages are being processed by WebSphere MQ. Access Manager for Business Integration can provide application-level data integrity and confidentiality, meaning it closes this security gap by securing messages before they are passed on to WebSphere MQ. It addresses this customer problem upon installation, providing an immediate ROI.

Competition–by Solution Area

The competition is heating up and they are attacking from four main fronts:

	Systems Management	Operational Security	Identity Management	Platform Architectures
	Vendors such as: BMC Software Computer Associates HP	**Vendors such as:** RSA Security Symantec Entrust	**Vendors such as:** Netegrity Oblix Business Layers Waveset	**Vendors such as:** Microsoft Sun Novell
Goal	Expand use of policy-based management infrastructure	Expand product portfolio within customer	Seed accounts with flagship product	Expand customer adoption of strategic architecture
Dynamics	Strategic deployment Enterprise pricing	Product deployment Price by product or portfolio	Quick deployment Tactical pricing	Strategic deployment Platform (partially embedded) pricing
Tivoli Advantage	Tivoli has best-of-breed solutions today.	These vendors lack strong focus and investment in identity management.	Tivoli delivers an integrated solution with proven and fast ROI.	Tivoli addresses complete user management lifecycle, while platform architectures only address limited requirements and require customized software development. Tivoli addresses the complete user management lifecycle, while the platform architectures do not.

TIP: Today's top threat is primarily found in the Identity Management space, while we anticipate the biggest threat for 2003-2004 to be in the Platform Architecture space.

Competition	Products	Strengths/Weakness	Tivoli Advantage
Symantec	Symantec Incident Manager, Symantec ManHunt, Symantec CyberWolf, Symantec SRM	**Strengths** • A large customer base and well-developed channel • Very strong in the SMB market **Weakness** • 3 overlapping products in this market and has not articulated a clear roadmap for convergence • Positions correlation as a tool for administrative actions and escalation, not for autonomic action and incident response • Lacks flexibility in heterogeneous environments as they are only provide a high degree of integration with their own components	• IBM Tivoli Risk Manager integrates with more third-party security solutions (over 50) • IBM Tivoli is neutral to point product vendors • IBM Tivoli provides automated, self-protecting responses
Netegrity	SiteMinder for Web-based authorization, Distributed Management Services v2 (a management tool for SiteMinder) and DataChannel Portal (a Web services portal)	**Strengths** • Quick time-to-value with easy installation and ease-of-use • First to release a SAML toolkit • Perceived market leader • Large customer list **Weaknesses** • Strategy focusing on portals has distracted the company from sufficiently focusing on identity management • Delegated management services require a proprietary application server • No support for multiple application server configurations (load balancing) • No support for clustering of applications servers for high availability • Does not protect URLs generated by Web proxy servers • Non-standard Java security implementation	• IBM Tivoli Access Manager has a complete, yet flexible identity management solution (access management + provisioning + privacy) • IBM Tivoli continues to invest in IBM Tivoli Access Manager, including building a new managed service offerings based on the software called the VeriSign Access Management Service

Competition	Products	Strengths/Weakness	Tivoli Advantage
Netegrity	IdentityMinder	**Strengths** • Large Netegrity customer base to sell into • Perception of a single-vendor solution **Weaknesses** • Customers must purchase SiteMinder and PortalMinder in order to use Identity Minder • Platform support is extremely limited • Java-based workflow engine lacks the integration and function of Identity Manager	• IBM Tivoli Identity Manager has broad platform support (over 70 platforms) • IBM TIM can be purchased as a stand-alone product • Highly integrated functionality • IBM TIM's administrative delegation model
BMC	• InControl for Security Management • Control SA-User account provisioning tool • Control SA Links – Event monitoring tool, responds with actions in Control SA • Control SA Passport – Password management tool • Control SA Workflow – Workflow tool	**Strengths** • Broad platform support • Leader in Gartner's Magic Quadrant • Ability to capture changes on local systems and update central repository • Ability to detect abnormal changes on systems outside of the "umbrella" • Intuitive Windows explorer type interface • Partnership with PriceWaterhouseCoopers **Weaknesses** • Not perceived as a serious security player by analyst and press • No command line interface • Workflow and password management functionality must be paid for a la carte • Central repository is an ODBC database rather than LDAP • No choice in databases • Script-based product is difficult to implement and use	• IBM Tivoli Identity Manager combines all functions of User Management and Provisioning into a single product • IBM Tivoli's solution has been constantly evolving and is the only Java-based tool on the market • IBM Tivoli can deliver a single vendor solution spanning Intranet and Extranet applications, as well as the merging identity and access management markets

Competition	Products	Strengths/Weakness	Tivoli Advantage
Oblix	NetPoint	**Strengths** • Identity management and access management functions are in a single product with single price point • Intuitive interface • Reporting capabilities • Cooperative relationship with Siebel **Weaknesses** • Requires manual editing of XML configuration files • Requires an extra server to process XML requests between plug-in and Access server • Limited native language support (French and German only) • Identity management is simplistic and limited to LDAP	• Administrative GUI is efficient and reduces errors • Fully internationalized for broad native language operation • Industry-leading platform support • Robust workflow • Widest options in user self-service
Computer Associates	CA eTrust Access Control, CA eTrust Web Access Control, CA eTrust Admin, CA eTrust Security Command Center	**Strengths** • Marketing presence around security • Exceptional user interface design with lots of “flash” **Weaknesses** • Focused on intrusion detection, anti-virus, and other operational components • Security management • Late to a very mature market with CA eTrust Web access control • CA Admin product has not evolved to keep pace with market leading solutions • Requires LDAP directory to fulfill a variety of purposes (user repository, workflow)	• IBM Tivoli is a leader in the security management market with best-of-breed products in both Access and Identity management • IBM Tivoli provides great flexibility of choice in operational components • IBM Tivoli offers customers proven mature products • IBM Tivoli's software portfolio shares a common foundation built on industry standards (WebSphere, DB2, and IBM LDAP) • IBM Tivoli's software portfolio shares a common foundation (WebSphere, DB2, and IBM LDAP)

Competition	Products	Strengths/Weakness	Tivoli Advantage
IBM	IBM WebSphere MQ	**Strengths** • WebSphere MQ includes security functionality • SSL-level security **Weaknesses** • Messages in queues are not protected	• IBM Tivoli Access Manager for Business Integration offers protection for messages in queues, which can help mitigate liability, ensure adherence to security legislation and help ensure successful audits

Customer Successes

Tivoli security solutions in action

Solution	Company Name/Basic Information	Synopsis
Access Manager for e-business	**AT&T** • A premier voice, video and data communications company • 50 million consumer customers • 4 million business customers	Since 1999, AT&T has been using Access Manager for e-business as the authorization backbone for their Common Security Platform service, in order to give its users (customers, suppliers, employees) access to corporate information and applications via the Web. Customer visits to AT&T partner sites and to AT&T Business Solutions (ABS) sites and AT&T employee access to HR sites and ABS sites are protected by Access Manager's WebSEAL proxy. Access Manager allows AT&T to not only control who accesses its Web assets (authentication), but also which resources each individual user can access (authorization). With a unified framework for Web security, AT&T can independently grow its customer security policies without making fundamental changes to back-end application architectures. Significant savings have resulted from using Access Manager, including application development and test savings (security services separate from the applications) and password reset savings. And Access Manager is up to the task of handling AT&T-sized loads.
Identity Manager (formerly Access360 enRole)	**E*TRADE Group** • Global financial trading organization • Provides Internet banking, mortgages, and financial assistance • Based in Menlo Park, California	E*TRADE needed to develop a high-level security infrastructure that would facilitate the growth of the company and keep it in line with standards of the financial industry. They looked to Access360's enRole (renamed IBM Tivoli Identity Manager) to not only automate these processes, but drive business objectives with a new sense of security and agility. E*TRADE is expected to meet high standards of accountability when faced with requirements from the financial industry auditors. E*TRADE relies on enRole (Tivoli Identity Manager) to help meet accountability for customer satisfaction sake and to comply with stringent federal regulations. Meeting service level agreements (SLAs) is a challenge, setting SLAs to meet an adequate level of productivity and efficiency is daunting. E*TRADE is able to do both with the workflow and agent system of Access360's enRole (Tivoli Identity Manager). Plus, with Access360's enRole (Tivoli Identity Manager), E*TRADE is able to instantly scale up or scale down according to market and customer demands.

Solution	Company Name/Basic Information	Synopsis
Risk Manager	**Blue World Information Technology, Inc.** • Helps clients solve IT security issues that hinder their e-business success • Serves North America from its headquarters in Vancouver, Canada	Blue World has bet its business on developing and deploying solutions based exclusively on IBM products, including Tivoli software. As an IBM Premier Business Partner, Blue World offers products and services associated with Tivoli Policy Director, Tivoli Identity Director, Tivoli Risk Manager, Tivoli Privacy Manager, IBM WebSphere, IBM MQSeries, and Lotus Domino. It has grown its business by offering consulting services that help clients apply these technologies to their businesses. Blue World uses Tivoli Risk Manager to help its clients deal with the overwhelming amount of data that can be generated when systems are being monitored for intrusion from hackers and/or viruses. Tivoli Risk Manager correlates data from firewalls, intrusion detectors, vulnerability scanning tools, and other security checkpoints, helping administrators eliminate false-positives and identify real threats. From an implementation stand-point, no other solution offers the integration and interoperability that come standard with IBM Tivoli security solutions.
Access Manager for e-business	**The Health Insurance Commission (HIC) of Australia** • 4,500 staff • 226 Medicare offices • Delivers health programs to the Australian community	With the introduction of their online Australian Organ Donor Registry and other e-business applications such as the Better Medication Management System, HIC required secure access control software that would provide the highest levels of security and confidentiality possible. While seriously considering a custom built solution, HIC also commenced assessment of Tivoli Policy Director (renamed IBM Tivoli Access Manager for e-business). An eight-month sales cycle, including a three-month trial, culminated in HIC's selection of Tivoli Policy Director and a sale worth $1.1 million. Tivoli Policy Director will be used for the B to B e-business customer environment to secure access to applications by external medical service providers, such as doctors and pharmacists. A number of contributing factors to the sale included: a highly successful three-month trial, persistence, professionalism, understanding the customer's requirements, strong customer relationship and excellent teamwork.

FAQs

IBM Tivoli Identity Manager

1. How has the Access360 acquisition affected the IBM Tivoli Security Portfolio?

Simply put, IBM acquired Access360 based on the superior capability that its enRole product provides in the critical areas of identity provisioning and life-cycle management. enRole (now Tivoli Identity Manager) provides Tivoli with a highly-competitive offering that includes key functions such as self-registration, automated approval processes via an easy-to-manage workflow capability, detection and correction of local provisioning settings and support for more than 70 managed targets.

2. What is the market position of TIM?

Industry analyst groups have started to estimate market shares in the provisioning space and Access360 has approximately 15% of the current market. Because of a long history in the provisioning market and a significant customer base, Access360 has enjoyed a deep knowledge of the space and put that knowledge into their 4.x version of enRole, which has been rebranded as Tivoli Identity Manager. This has paid off as we are widely credited for putting provisioning on the map and recognized as a leader in the space.

3. How does TIM implement Workflow?

TIM 4.0 has a drag-and-drop designer for creating and modifying workflow designs. This workflow is very flexible and can be used for multiple business processes. Clients frequently use the workflow as a mechanism to gather approvals and information for a wide variety of resources used in organizations. The workflow can be used in conjunction with the Universal Provisioning Agent (UPA) to provision virtually anything by sending the approved request to an administrator using e-mail. Additional workflow capabilities can be accessed by IBM Tivoli professional services or other trained people by including XML extensions into TIM.

IBM Tivoli Access Manager

1. How does IBM Tivoli Access Manager for e-business address Web Services-Security today? What can we expect in the future?

As one of the original authors of the WS-Security specification draft (along with Microsoft and VeriSign), IBM is vitally interested in bringing the technologies that will fulfill those specifications to market. We have begun doing so, with Access Manager for e-business support and testing for compatibility with SOAP transactions and with the Access Manager for e-business V4.1 Federated Identity Interface, which opens up the APIs for Access Manager's robust e-Community SSO capability. Custom code can be written to support token types such as SAML's. As for the future, IBM does not generally comment on unannounced products/releases. However, in general, IBM Tivoli Access Manager will be the vehicle for delivering Web Services and Federated Identity Management capabilities through tight integration with the WebSphere platform.

2. When will IBM Tivoli Access Manager for e-business be the security engine for WebSphere Application Server?

Presently, Tivoli Access Manager for e-business V4.1 is the recommended security solution for all WebSphere Application Server sales, except certain limited cases (the customer will only be using WAS or WPS-based resources in their e-business, or the customer will have less than 100 users, or less than four WebSphere servers). For the next major WebSphere Application Server release following 5.0, a limited-use Tivoli Access Manager for e-business will be part of the WebSphere Application Server package, and Access Manager will be able to be used as an alternative to WAS native security.

3. A competitive product to AMOS (CA's eTrust Access Control) has a Windows version. Why do we not provide AMOS on Windows?

Customers like the notion that eTrust Access Control “manages access” simultaneously across Windows and UNIX. The major administrative value of products like AMOS is the management of access control policy (i.e. defining in ACLs which groups/users get access). For IBM this function is performed by the best-of-breed product, Tivoli Identity Manager. Managing access on a per-resource basis for Windows (as in eTrust) is superfluous. Much of the capability of eTrust is already available in some form within Windows NT, 2000 and especially .NET and Active Directory. The major

AMOS (and eTrust) value propositions on UNIX (root control, secure audit etc.) are already provided for in a Windows environment. IBM's experience with access control policy management is that windows administrators prefer to administer access control policy (which is relatively static) using windows tools—a different access control model does little (if anything) to reduce administrative overhead. The same tools and capabilities are not available on UNIX. That's why the AMOS solution makes sense for UNIX but not Windows. If a customer is looking to provide value in a mixed Windows/UNIX environment, they can get the greatest ROI with Identity Manager manipulating Windows and Access Manager users and groups.

4. How do the Tivoli security management solutions relate to metadirectories and directory technologies?

Tivoli's security management solutions deliver value to customers based on their ability to automate and manage the business processes of managing user identities and security events. The underlying data that is used within these business processes is typically stored in a directory service such as the IBM LDAP Directory Server, RACF, Microsoft Active Directory, Novell e-Directory, and the numerous application-specific user directories that the traditional approach to application security generates. Tivoli's security management solutions integrate with the leading directory services on the market today. Additionally, because customers typically manage each directory service separately, inconsistencies in the underlying user attribute data are inevitably generated. Metadirectory technology addresses this issue, in that it synchronizes and rationalizes this underlying data. Obviously, if the underlying user data is consistent across all of a company's directory services, then the value that Tivoli's security management solutions provide can be extended more easily and further across the enterprise.

IBM Tivoli Access Manager for Business Integration

1. What platforms does AMBI support?

IBM Tivoli Access Manager for Business Integration V4.1 is supported on the following platforms:

- AIX 4.3.3 and AIX 5.1
- Solaris 7 and 8
- Windows NT 4.0 with SP6a or higher
- Windows 2000 with SP 2
- IBM Tivoli Access Manager for Business Integration – Host Edition V3.7.1 supports both IBM OS/390 V2 R10 and any release of IBM z/OS

2. Does Access Manager for Business Integration support WebSphere MQ Integrator or MQSeries Workflow?

Yes, in general, IBM Tivoli Access Manager for Business Integration V4.1 supports the following WebSphere MQ applications:

- MQSeries V5.2: Server only on AIX and Solaris
- MQSeries V5.2.1: Server only on Windows
- WebSphere MQ V5.3: Server only on AIX, Solaris and Windows
- WebSphere MQ Integrator (MQSI) V2.02 and V2.1
- WebSphere MQ Workflow V3.3.2

3. Which PKI credentials does IBM Tivoli Access Manager for Business Integration V4.1 support?

IBM Tivoli Access Manager for Business Integration V4.1 has been tested with PKI credentials from the following Certificate Authorities:

- Tivoli SecureWay PKI V3.7.1
- Entrust WebConnector V5.0
- Planet Certificate Management Server V4.2
- Baltimore UniCERT V3.5
- VeriSign

IBM Tivoli Privacy Manager

1. What does Tivoli Privacy Manager do?

Tivoli Privacy Manager is the first privacy management solution that helps enterprises:

- Build trust by managing consent: Privacy Manager allows organizations to collect and manage consumer and employee consent to privacy policies and preferences.
- Integrate privacy policies into applications: Privacy Manager digitizes privacy polices, categorizing policy into groups, purposes and data types.
- Track access to personal information through detailed reports: Privacy Manager is the first application that monitors access to personal information and evaluates permission based on who is requesting the data, for what purpose and which fields, depending on the translated categories in the privacy policy. A comprehensive access report details all disclosures of personal information according to policy conditions and customer consent.

2. How does Tivoli Privacy Manager work?

Privacy Manager fulfills five steps of privacy management. These are:

- Define your privacy policy into digital form with a Privacy Policy Wizard.
- Deploy the policy to IT systems and applications by posting the policy in P3P form to a central Policy Server.
- Record end-user consent and choices to the policy, by storing consent for all customers and employees in P3P format along with the policy on the Policy Server.
- Monitor and enforce compliance to the policy by users accessing protected information.
- Provide detailed reports on the usage of protected information.

3. What problems does IBM Tivoli Privacy Manager solve?

Enterprises face a challenge in ensuring that they are respecting end-user privacy preferences consistently and effectively across their environment. Not doing so exposes them to the risk of misusing personal and sensitive information, which causes a negative impact on customer retention, user experiences, loyalty and trust. By providing a platform for consistently enforcing end-user choices, Tivoli Privacy Manager can help enterprises keep their customers longer. Integrating privacy policies into applications allows enterprises to share data more effectively and to the scale that is needed to deliver positive ROI. In addition, detailed reports on data usage according to policy can help lower the cost of complying with regulations.

IBM Tivoli Risk Manager

1. How does Risk Manager enhance the current security infrastructure that is in place?

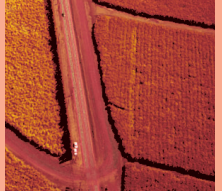
Risk Manager's value to the security team is in its ability to gather and analyze the information from the various security safeguards that are in place, by looking at the patterns of information, while determining and assessing the "good" from the "bad." This translates to an intelligent and scalable correlation technology which minimizes the time it takes to identify threats, while assisting in maintaining an audit trail of everything that has transpired.

2. Can Risk Manager help identify unauthorized access and illegal use of restricted commands in a Unix/Linux environment?

Risk Manager allows you to maintain control over the access to systems and files by recognizing what is happening on a critical resource based on the security policy. This becomes even more powerful when used in conjunction with Access Manager for Operating Systems (AMOS), which allows you to monitor exceptions to its security policy based on ACLs which have been established.

3. Which types of security appliances or products are supported by Risk Manager?

Risk Manager supports the top level and most popular set of firewalls (Cisco, Checkpoint, etc), IDS systems, routers, anti-virus software, databases, etc. In addition, it can monitor log files or audit files, which are created by operating systems or applications. The Risk Manager toolkit further allows you to extend its coverage to systems that may be unique to your enterprise.



Additional Resources and Tools

Looking for more information? Try these resources:

The Tivoli ROI Analyst Tool, co-developed by Tivoli Sales Enablement and Alinean Corp., is now available to help you make the financial case for Tivoli software solutions. Use the ROI Analyst Tool to help develop accurate and financially sound business cases, quantify specific operational savings, identify the strategic value of a proposed solution, deliver highly detailed reports outlining where value is realized and provide customers with compelling reasons for evaluating and possibly purchasing new software. The Tivoli ROI Assessment is only available for customers who are actively evaluating new or additional Tivoli solutions.

Register online to obtain access to the tool. Please go to the following URL to download the online training and executable file: http://www.ibm.com/software/tivoli/partners then Sales Tools

Tivoli Web site-provides information to customers on IBM Tivoli products, events and promotions

http://www.ibm.com/tivoli

Tivoli Business Partner Center Online (TBPCO) --provides central access to Business Partner information residing on PWSW, PWD, specifically for TBPCO, or other IBM sites.

http//www.ibm.com/software/tivoli/partners

Partner World for Software and the Business Partner Zone -direct access to IBM Business Partner Programs events, announcements, collateral and training

http://www.ibm.com/partnerword/software

http://www.ibm.com/partnerword/software/zone

IBM Passport Advantage-provides an easy way for Business Partner to acquire software- including eligible new versions and releases- and access to technical support

http://www.ibm.com/software/passportadvantage/

Signature Sales Resource -direct access to IBM Tivoli Tivoli product information and sales tools grouped under the Signature Selling Methods steps

http://www.ibm.com/partnerworld/ssr

Web demos-high-level overviews of Tivoli solutions and management concepts

http://www.tivoli.com/products/demos/index.html

TIP: Be sure to highlight IBM Tivoli's security solution leadership, and reference the industry awards we've won. Visit the Tivoli Web site for all the up-to-date information: http://www.tivoli.com/news/press/awards/

IBM®

Tivoli® software