Tivoli software

IBM

Tivoli Software Business Partner Pipeline Building Kit—Security Management

Your Pocket Guide to Sales Effectiveness

Updated April 2003

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 Software?

This pocket sales guide can help you better understand and convey the Tivoli value proposition when selling Tivoli Security Management offerings, which together uniquely provide a solution for **Integrated Identity Management**. From a sales perspective, the guide delves into each solution area within Integrated Identity Management 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 Software offer my customers?
- Why are Tivoli Security Management 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 Software solutions?

TIP: Tivoli's value proposition is best delivered to the "C" level executive in mid- to large-sized organizations. But, don't forget the importance of the line-of-business, application architecture, and IT operations teams in selling Tivoli Security Management solutions.

Contents

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

Market Drivers and Overall Customer Pains

Organizations' user communities continue to multiply

Managing identities throughout their entire lifecycle has become a complex, management-intensive process, often involving many different user repositories. Administrative costs, including help desk staffing requirements skyrocket. Additionally, just keeping all of the identity repositories used by an e-business synchronized is a major manual process.

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.

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

IBM Tivoli Software

Intelligent Management Software for the on demand World!

We have entered a new era in business—the on demand era! An on demand business is:

- Responsive to the dynamic needs of customers, partners, suppliers and employees
- Resilient to withstand whatever comes along — changes in supply, pricing and customer preferences; fluctuations in sales, enrollments, oil prices and capital markets; or challenges we truly can't predict from hackers to hurricanes
- Efficient and effective despite shrinking budgets, access to fewer skilled resources, and increasing complexity

As businesses evolve to e-business on demand, IT must increase the level of integration and automation and move from cumbersome resource intensive processes to autonomic computing. This migration requires integrated management of IT resources, users and business processes.

Faced with the increasing competitive pressure of a globalized market and a tough economy, IT operations must optimize for business value, tightly linking systems and operations to business processes that deliver value to the organization.

In this on demand view, much of the underlying systems infrastructure is virtualized, taking advantage of autonomics and integrating technologies, so that the systems can adapt in response to dynamic business pressures.

- Integrated for efficiency—Moves customers beyond managing the individual components of their IT infrastructure and provides an integrated view from which to manage.

- Automated for productivity—Uses intelligent, autonomic technology to proactively manage users, business processes, and IT resources from end-to-end for a far more reliable, resilient business.
- Optimized for business value—Helps customers build an optimized IT infrastructure that keeps business processes operating at their peak.

IBM Tivoli provides solutions that help customers understand and proactively manage the business value of their IT resources in an on demand world. IBM Tivoli lets customers spend less time deploying solutions and diagnosing problems so they can more effectively and efficiently manage business operations while managing costs.

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 administrative costs, and higher development costs. Tivoli Software addresses these pains by:

- automating and centralizing the management of users and perimeter network security administration
- creating a high performance and highly-available identity data infrastructure that maximizes the value of identity management services
- keeping e-business identity repositories synchronized, providing authoritative data for critical security and e-business applications
- increasing productivity and satisfaction through single sign-on and self-care for users, as well as through the ability to address IT security according to a well-defined comprehensive policy
- securing sensitive transactions end-to-end
- monitoring and enforcing privacy policies

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 Tivoli Security Management solutions unique?

- Best-of-breed* integrated solutions for Integrated 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 Management solutions address our customers' security challenges across two different areas:

Solution	Description
Integrated Identity Management	The Tivoli Integrated 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, IBM Directory Integrator, IBM Directory Server, and VeriSign Managed Services.
Security Event Management	The Tivoli Security Event Management solution protects e-business infrastructures by improving response time to security threats, monitors security and 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

Integrated Identity Management

Product	Ideal Prospects	Customer Benefits
Tivoli 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
Tivoli Access Manager for e-business *Tip: Leverage Tivoli Access Manager's peerless support for:* • *Java 2/J2EE security, for both WebSphere and BEA WLS environments* • *Linux* • *The mainframe, including tight integration with RACF and TopSecret, and zLinux support.*	• 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 policy-based access control and single sign-on to e-business initiatives • Increases e-business connectivity through standards-based support for Web Services security • Ensures both security and availability of e-business transactions

Product	Ideal Prospects	Customer Benefits
Tivoli Access Manager for Business Integration *Tip: Develop a good working relationship with the Software Account Manager in your customer accounts, as this product is a natural companion sale to WebSphere MQ. Focus on companies in industries that deal with sensitive information—finance, insurance, healthcare and the government sector.*	• Manage security of a 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 • Have failed a security audit for problems related to the transmission of sensitive data • Need to ensure a high degree of security for e-commerce transactions all the way back to legacy systems • Must provide security for and the ability to audit data at the messages level • 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 needing to exchange secure messages • Extends the security model of WebSphere MQ to provide application level data protection • Provides remote administration of WebSphere MQ security policies • Minimizes business exposure and liability • Delivers immediate ROI upon deployment • Supports larger WebSphere Business Integration solution family
Tivoli 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	• Lock down product UNIX and Linux servers • Speeds implementation via best-practices policy definitions • Increases systems security/integrity • Improves efficiency of administration
Tivoli 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
IBM Directory Integrator	• Need to synchronize identity data within directories and databases across the enterprise to provide reliable, accurate user information to their enterprise security and e-business applications	• Lowers administrative costs by keeping user identities synchronized and rationalized • Allows e-business solutions to be deployed faster by more quickly providing needed user identity data • Increases ROI of security and e-business applications by providing authoritative data sources: OnDemand data for OnDemand computing

Product	Ideal Prospects	Customer Benefits
IBM Directory Server	• Need a high performance and highly-available identity data infrastructure to support enterprise security and e-business applications	• Lowers administrative costs by providing a single source for identity data • Provides more reliable and scalable e-business solutions, including Linux • Increases customer flexibility by supporting open standards and all leading platforms
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
Tivoli Risk Manager *Tip: Sell to existing TEC customers (leverage the existing relationship) and position Tivoli Risk Manager from the point of managing e-business services, such as access to applications, databases, etc.*	• 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 • Enables the use of existing people resources to augment current services
Tivoli Intrusion Manager *Note: This is an entry-level security product aimed at midsize companies to quickly implement an effective solution to help mitigate and manage intrusions.*	• Manage Internet and network security for mid-sized companies • 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	• 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 • Enables the use of existing people resources to augment current services
Tivoli 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 • Need 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 Management solutions involves five key steps:

1. *Determine what the customer's compelling business issues are*
   Are they trying to reduce security-related administration and help desk costs? Has the lack of SSO been a thorn in their side for a long time? Do they need to improve audit compliance? Have there been privacy-related issues that have caused negative publicity for the company? Do they need to pull together all of the directories and databases that contain user identities? Has their middleware team failed a security audit, due to passing sensitive data, unsecured, from application to application? 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. *Understand and communicate the entire Integrated Identity Management solutions portfolio, which consists of IBM Directory Server, IBM Directory Integrator, Tivoli Identity Manager, Tivoli Access Manager, and Tivoli Privacy Manager*
   Drive customer awareness of IBM's strength—the unique breadth of the IBM Integrated Identity Management portfolio, which adds value to each of the individual offerings. Success in each offering increases the potential for each of the other offerings across the portfolio. Do not allow competition to focus on just one piece of the overall solution and thus divide and conquer our greatest strength.

3. *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 Management 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.

4. *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.

5. *Execute the Evaluation Plan and close the business*

   Customers who evaluate Tivoli Security Management 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.

Target Audiences

Audience	The IBM Tivoli Advantage
Senior IT executive and Line of Business executive Other titles-Chief information officer (CIO), CFO, director of technology, director of MIS **Challenges** • Developing strategy of business and e-business • Determining impact of technology solutions on profitability • Extending organization into the e-marketplace • Managing personnel • Implementing technology to meet business goals	• Helps turn security from a cost center into an enabler for reaching business goals • Helps ensure a secure e-business through consistent application of security policy • Provides proven, quantifiable return on investment from many current reference customers • Largest customer base of access management software in the industry with the Tivoli Access Manager family • Includes IBM global reach for service and support
Senior IT manager Other titles-IT/IS director, senior network administrator, senior IT administrator, director of systems and/or application architecture, senior IT consultant **Challenges** • Developing, implementing and maintaining applications and infrastructure to meet e-business strategy • Tracking service level of IT organization • Managing personnel • Keeping mission-critical systems reliable • Predicting growth and matching it with IT resources	• Is the only vendor in a leadership position in both Gartner's Extranet Access Management Magic Quadrant and Gartner's Provisioning Decision Support Tool (February 2003) • Leads the convergence of the identity management market by providing the single-vendor solution • Is the leader and developer of major Web standards that provide ease of integration into Web initiatives
IT administrator Other titles-Senior IT/IS manager, LAN administrator, network administrator, software distribution and inventory coordinator **Challenges** • Finding instant solutions to systems, applications and network problems • Recommending technology for purchase • Conducting capacity planning • Supervising security audits	• Ranks as top performer in Mindcraft performance study (Tivoli Access Manager for e-business was 52 percent faster than the closest competitor) • Provides results, such as a 61 percent reduction in help desk costs for password reset at a major financial institution by centralizing asset management • Lowers costs, such as an 85 percent reduction in user administration costs at a major transportation firm by centralizing user management and provisioning

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 • Tivoli Access Manager for e-business • IBM Directory Integrator • IBM Directory Server	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. Tivoli Access Management for e-business helps reduce help desk costs through single sign-on to Web resources. IBM Directory Integrator allows user identity attributes to be automatically synchronized across many directories and databases and IBM Directory Server allows for a single, scalable source of user identity data.
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 • Tivoli Access Manager for Operating Systems • IBM Directory Integrator • IBM Directory Server	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 with Tivoli Access Manager for e-business. Extend this model to support messaging queues with Tivoli Access Manager for Business Integration and enable finer-grained security for UNIX/Linux systems with Tivoli Access Manager for Operating Systems. And by adding IBM Directory Integrator customers can quickly create an authoritative source of user identity data for new e-business applications and adding IBM Directory Server allows for a single, scalable source of user identity data.
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 • Tivoli Access Manager for Business Integration • Tivoli Access Manager for Operating Systems	The Tivoli Access Manager family 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 • Tivoli Identity 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.	• Tivoli Risk Manager	Tivoli Risk Manager provides an effective security dashboard for managing the massive amount of information that network security tools generate, can work with other Tivoli security products.

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 do not interact or integrate. Moving forward and adding new capabilities to this environment will continue to become more difficult and costly. Tivoli Software solutions are open for easy integration and offer a clear, unified, and policy-based approach for your entire enterprise. 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 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 acquisitions of Access360 and MetaMerge in 2002 are examples of our commitment to enhancing functionality. Plus, having a customer base of more than 1,100 speaks to the quality and effectiveness of our solutions.
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. Use them together and 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, middleware to our solution.
IBM WebSphere MQ V5.3 can secure my sensitive data using SSL, why do I need to license Tivoli Access Manager for Business Integration?	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 resident on a queue. Tivoli 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	Directory-centric 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.

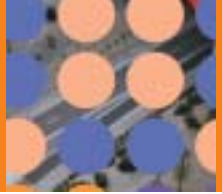
Competition	Products	Strengths/Weakness	Tivoli Advantage
Netegrity *Tip: VeriSign replaced SiteMinder with Tivoli Access Manager for their managed services offering because of SiteMinder's scalability issues.*	SiteMinder for Web-based authorization, Distributed Management Services v2 (a management tool 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 • Complex, limited, and non-standard Java security implementation • Company viability and support	Tivoli Access Manager for e-business offers the following: • 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 • Demonstrated scalability, performance, and reliability • Superior security via proxy-based architecture, with an option to secure niche areas via a plug-in

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

Competition	Products	Strengths/Weakness	Tivoli Advantage
Netegrity *Tip: They are dropping in Business Layers and calling it IdentityMinder. Ask for reference customers using IdentityMinder (not earlier, failed effort called DMS)*	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	Tivoli Identity Manager offers the following: • Broad platform support (over 70 platforms) • Tivoli Identity Manager can be purchased as a stand-alone product • Highly integrated functionality • Tivoli Identity Manager 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	Tivoli Identity Manager offers the following: • All functions of user management and provisioning into a single product • Exclusivity as the only Java-based tool on the market • 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 *Tip: Selling Tivoli Access Manager for e-business and a T's and C's limited version of Tivoli Identity Manager (referred to as "TAM Plus") has been effective in selling against 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	Tivoli Identity Manager and Tivoli Access Manager for e-business offer the following: • An administrative GUI that is efficient and reduces errors • Full internationalization 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)	Tivoli Identity Manager and Tivoli Access Manager for e-business offer the following: • Leadership in the security management market with best-of-breed products in both Access and Identity Management • Grater customer flexibility of choice in operational components • Market-proven mature products • A common foundation built on industry standards (WebSphere, DB2, and IBM LDAP)

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	Tivoli Risk Manager offers the following: • Integration with more third-party security solutions (over 50) • Neutrality to point product vendors • Automated, self-protecting responses
Watchfire	Privacy XM	**Strengths** • Website monitoring helps companies manage where on their Website they are collecting information that is not associated or consistent with a privacy policy • Easy implementation **Weaknesses** • Does not address data-handing auditory or enforcement • Does not fulfill 5 steps of privacy management	Tivoli Privacy Manager for e-business fulfills all 5 steps of privacy management: 1. Write a policy 2. Deploy a policy 3. Track user consent to the policy 4. Monitor and enforce access by data users to the policy 5. Generate audit trails for demonstrating compliance



Customer Successes

Tivoli Security Management solutions in action

Solution	Company Name/Basic Information	Synopsis
Tivoli 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 Tivoli 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 Tivoli Access Manager's WebSEAL proxy. Tivoli 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 Tivoli Access Manager, including application development and test savings (security services separate from the applications) and password reset savings. And Tivoli Access Manager is up to the task of handling AT&T-sized loads.
Tivoli 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 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
Tivoli 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 Tivioli Access Manager (formerly 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 Tivoli Security Management solutions.
Tivoli 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 Access Manager for e-business (formerly Tivoli Policy Director). An eight-month sales cycle, including a three-month trial, culminated in HIC's selection of Tivoli Access Manager for e-business and a sale worth $1.1 million. Tivoli Access Manager for e-business 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.
IBM Directory Integrator and IBM Directory Server	**Honeywell** • More than $10B in annual revenue • 100,000 employees • Sells products and services for the aerospace industry and focuses on automation and control systems, specialty materials, and transportation and power systems	Honeywell had a number of disparate systems that contained user ID's, passwords and other user information like addresses and telephone numbers. Keeping all of the systems up to date and in synch was nearly impossible. The company wanted to develop a central system that housed all of this data and was accessible to employees (for contact information updates and changes) and to administrators (for password resets and additions/deletions). The company also wanted to simplify access to its multiple applications while maintaining high security standards. To create a reliable and scalable enterprise directory, Honeywell turned to IBM and implemented the IBM z900 Linux Directory Server and the IBM z900 Linux Directory Integrator. IBM Directory Integrator connects disparate data sources to the IBM Directory Server data store to create a consistent view of enterprise identity data. The solution integrates data stores on different computing platforms, improves security and delivers advanced replication, and provides flexibility in the deployment of servers. With tens of thousands of users using the new system, Honeywell has realized significant savings in labor, ease of use, and time. And the system simplifies users' experiences by giving them a single point of entry and a single point of access to all approved systems.

FAQs

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 TIvoli Identity Manager?

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. Gartner currently rates Tivoli Identity Manager as the top provisioning solution.

3. How does TIvoli Identity Manager implement Workflow?

Tivoli Identity Manager4.0 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 Tivoli Identity Manager.

Tivoli Access Manager

1. How does 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 Tivoli Access Manager for e-business support and testing for compatibility with SOAP transactions and with the Tivoli Access Manager for e-business V4.1 Federated Identity Interface, which opens up the APIs for Tivoli 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, 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 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 (where 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 Tivoli Access Manager will be able to be used as an alternative to WAS native security.

3. When will Tivoli Access Manager for e-business be supported on Linux, including Linux for mainframes?

Tivoli Access Manager for e-business provides strong coverage of Linux. Specifically, the following are supported:

- RedHat Linux 7.1 and 7.2
- SuSE Linux Enterprise Server 7 and 8 for zLinux
- SuSE Linux Enterprise Server 8 for IA32 (Intel)

This support includes the ability to run the Policy Server, Authorization Server, and WebSEAL on these platforms.

4. A competitive product to Tivoli Access Manager for Operating Systems (CA's eTrust Access Control) has a Windows version. Why do we not provide Tivoli Access Manager for Operating Systems on Windows?

Customers like the notion that eTrust Access Control "manages access" simultaneously across Windows and UNIX. The major administrative value of products like Tivoli Access Manager for Operating Systems 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 Tivoli Access Manager for Operating Systems (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 Tivoli Access Manager for Operating Systems 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 Tivoli Identity Manager manipulating Windows and Tivoli Access Manager users and groups.

5. 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 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.

6: What platform support does Tivoli Access Manager for Business Integration offer?

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
- Tivoli Access Manager for Business Integration—Host Edition V4.1 supports both IBM OS/390 V2 R10 and any release of IBM z/OS

7. Does Tivoli Access Manager for Business Integration support WebSphere MQ Integrator Broker or WebSphere MQ Workflow?

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

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

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

- Entrust WebConnector V5.0
- iPlanet Certificate Management Server V4.2
- Baltimore UniCERT V3.5
- VeriSign

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: Tivoli Privacy Manager allows organizations to collect and manage consumer and employee consent to privacy policies and preferences.
- Integrate privacy policies into applications: Tivoli Privacy Manager digitizes privacy polices, categorizing policy into groups, purposes, and data types.

- Track access to personal information through detailed reports: Tivoli 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?

Tivoli Privacy Manager is an application built on Java and WebSphere Application Server. It consists of a server which maintains information related to privacy polices, and one or more monitors, which are placed and adapted to the application environment(s). Tivoli Privacy Manager observes data going into and out of monitored applications and storage systems; they essentially act like bridges between those systems and the PM server. In this way, Tivoli Privacy Manager fulfills the following five steps of privacy management:

1. Define your privacy policy into digital form through a privacy policy editor.
2. Deploy the policy to IT systems and applications by publishing the policy to the application monitors.
3. Record end-user consent and choices to the policy via the application monitors.
4. Provide auditing functions and enforce real-time compliance to the policy by users accessing protected information (via application monitors).
5. Provide detailed reports on the usage of protected information.

3. What problems does 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. Enterprises are also in need of solutions that can help them demonstrate compliance to their policies, regulations, or law. The audit logs that Tivoli Privacy Manager automatically generates significantly reduce the cost of auditing and compliance.

4. How do I place privacy monitors in my environment?

There are three basic strategies typically pursued in deploying monitors and each has both advantages and disadvantages. The first of these is probably the first one that most customers ask about, which is to locate the monitor close to the storage system (such as a DB2 or Oracle database). In a scenario like this, the monitor attempts to act like an extension of the database (or monitored storage system) instead of as an extension to the application accessing the database. If the monitor is deployed like that, it takes on one of two types: it's either used as a proxy that monitors traffic between applications and the storage system, or it is used behind the database as an extension that is notified whenever PII is accessed. Monitors near the storage system are highly transparent to accessing applications, but have the disadvantage of limiting the monitor's functionality (maybe just to visibility of access credentials).

The second strategy is to perform monitoring close to the application that uses the database. In cases like this, the application might need to be altered to enable privacy monitoring, such as enjoining a JDBC:ODBC bridge to facilitate communication. This is similar to the first strategy in that monitoring is conducted in the data path, but may differ by use of an add-on that makes a call to the monitor when PII is accessed. Advantages to this approach seem to relate primarily to the comprehensive information made available to the monitor—the application, after all, maintains the most information about who is accessing PII and why it is being accessed.

The third strategy is to monitor at the business process layer. This absolutely demands well-defined business processes, and may carry the disadvantage of necessitating changes to those processes that aren't so well-defined. By the same token, this strategy simplifies operation of the monitor.

None of these strategies is necessarily exclusive of the others. Multi-part monitors can be constructed to capitalize on what is required, what is expedient, and what is most desirable. In other words, you can very much control the employment of the monitoring system within its basic rules.

5. What do I need to use Tivoli Privacy Manager?

Tivoli Privacy Manager requires the following:

- WebSphere Application Server, Advanced Edition V4.03 (and associated DB2 and LDAP)
- IBM Tivoli Access Manager for e-business v 4.1

Tivoli Risk Manager

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

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

Tivoli 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 Tivoli Access Manager for Operating Systems, 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 Tivoli Risk Manager?

Tivoli 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 Tivoli Risk Manager toolkit further allows you to extend its coverage to systems that may be unique to your enterprise.

IBM®

Tivoli® software

a Copyright IBM Corporation 2003
Printed in the United States of America 4-03 All Rights Reserved

Tivoli and the IBM logos are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. All IBM product names are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. Lotus is a registered trademark, and Domino is a trademark of Lotus Development Corporation and/or IBM Corporation. Microsoft is a registered trademark of Microsoft Corporation in the United States, other countries, or both.

IBM internal use only. Z325-6947-01