

IBM® offerings addressing e-business Security and Privacy June 2001

This addendum highlights IBM offerings that address the key findings within the IDC brief entitled “Stenghtening End-to-End e-Business Security,” dated June 2001, posted to the IBM e-business Infrastructure Web site at <http://www.ibm.com/e-business>. This addendum also references IBM Web sites, where more detailed documentation is available to assist IT professionals.

Summary

IBM has built upon its core strengths with a scalable range of security and privacy management offerings for end-to-end, trusted e-business environments. In addition, IBM can respond, locally or globally, to a variety of trusted e-business situations with experienced solution expertise. Services are provided through IBM Global Services Security and Privacy Services, while program solutions are provided by IBM's Tivoli® business unit. Access the following IBM Web sites for more information on these topics, customer references, and offerings:

IBM Security and Privacy Services: <http://www.ibm.com/services/security>

IBM Tivoli Offerings: <http://www.tivoli.com/security>

IDC Finding: Enterprises need the ability to consistently enforce their security and privacy policies.¹

IBM's security and privacy solutions have been architected as a cohesive element of IBM's e-business Infrastructure. Using the IBM Framework for e-business approach as a major design element, Tivoli solutions can extend new or existing systems, based on open system standards, and can support scalable, multiplatform heterogeneous environments. For more details on this approach access the “IBM Framework for e-business: Security” paper at <http://www.ibm.com/software/ebusiness/>

Tivoli SecureWay® Policy Director is designed to define and manage security policies for e-business applications and other managed resources, while transparently enforcing authorization policies to Web applications. Policy Director supports a broad range of browser and wireless identities, addresses multiple levels of trust, and leverages a common security policy model that extends to other resources, such as the IBM WebSphere® family of products.

IBM's Security and Privacy Services focuses on delivering services and solutions to build trusted electronic relationships among a client's customers, employees, business and trading partners, and shareholders. These end-to-end services include assessments, planning, architecture and design, implementation and management of a security-rich environment. For example, IBM's Security Policy Definition service offering investigates the requirements for information security, the associated priorities and, thereafter, creates a custom security policy to clearly demonstrate management's commitment to an enterprise security program and creates the first step to implement a enterprisewide security program. IBM Security Specialists are trained and experienced in consulting within environments that include multiplatform heterogeneous systems, and where integration of existing and new applications and systems is required.

IDC Finding: Enterprises need offerings that can assist in establishing Security and Privacy policies.¹

IBM Security and Privacy Services Specialists can review an enterprise's security strengths and vulnerabilities, then work with IT management to develop a coordinated, end-to-end set of policies, based on IBM's global experiences, resources, and proven methodologies and practices, supported by IBM Research and the IBM Global Security Analysis Lab.

IDC Finding: Enterprises need to monitor external connections and internal activities, and identify vulnerabilities.¹

Tivoli SecureWay Risk Manager assists in proactively managing risks by alerting security administrators of attacks on their systems from viruses, hackers, and denial-of-service intruders. Risk Manager is designed

to provide coordination, correlation and reporting to allow administrators to understand the data received on suspicious activities, assess the severity of the attack, and manage the risks proactively.

IBM Security Specialists offer a broad and rich portfolio of security services including consulting, ethical hacking (for an effective measure of possible vulnerabilities), and Network Operations Centers (for remote handling of intrusion detection services).

IDC Finding: An enterprise's security infrastructure needs to have the following basic capabilities:¹

- [Identification/Authentication/Authorization](#)
- [Administration](#)
- [Asset Protection](#)
- [Assurance](#)
- [Accountability](#)
- [Availability](#)

The combination of Tivoli SecureWay Policy Director and Privacy Manager provides the underpinnings of an authentication/authorization solution that allows only authorized users to access resources, according to preestablished policy. Policy Director supports multiple identity mechanisms and addresses authorization for resources, such as applications, middleware and operating systems. For example, through use of Java™ 2 standards-based authentication and authorization services, Policy Director supports IBM WebSphere, and other J2EE conforming application server offerings. Policy Director for MQSeries manages MQSeries® applications in a consistent fashion.

Tivoli SecureWay Privacy Manager addresses asset protection. This access control solution can enforce privacy policies and protects consumers' personally identifiable information. It also extends Policy Director to implement dynamic data privacy policies. In addition, asset protection features are included in IBM DB2®, IBM WebSphere, Lotus® Notes®, Tivoli SecureWay offerings, and other IBM resource managers.

Tivoli SecureWay Privacy Manager and Policy Director for MQSeries, working in conjunction with Policy Director, address accountability for e-business transactions. Policy Director for MQSeries also supports digital signing messages addressing integrity and non-repudiation.

Tivoli SecureWay User Administration addresses administration by providing an automated, security-enhanced way to manage user attributes and user services across heterogeneous, distributed networks. User Administration is designed to provide policy-based management, management by subscription, and secure delegation. These control and security-rich capabilities greatly improve the productivity of administrators.

Tivoli SecureWay Risk Manager addresses assurance by providing comprehensive event/alert consolidation, correlation, reaction and reporting.

Tivoli SecureWay Policy Director addresses availability through its replication, caching, and its ability to handle millions of users. In general, Tivoli SecureWay offerings are built to address enterprise requirements for availability and scalability.

IDC Finding: A trusted e-business environment requires the combination of security infrastructure and a sound privacy policy, and that privacy elements be built into the security infrastructure.¹

Tivoli SecureWay Privacy Manager is an access control solution developed for e-businesses needing to enforce privacy policies to protect consumers' personally identifiable information. Privacy Manager integrates into the security infrastructure by leveraging Tivoli SecureWay Policy Director standards-based authorization services to provide access control consistently across the entire enterprise.

IBM Security and Privacy Services provide assessment services and workshops on policy development, based on standards, and management architecture principles. In addition, an essential element in an enterprise's privacy strategy should be to document and publish its policy on privacy. As an example, to view IBM's Privacy Statement & Policy access <http://www.ibm.com/privacy>

IDC Finding: Implementing a security/privacy solution takes 3 steps: 1) Creating a Blueprint, 2) Selecting Skills & Resources, and 3) Selecting & Deploying the Solutions.¹

IBM Security and Privacy Services can conduct an assessment of an enterprise's security and privacy to aid in the development of a blueprint through a broad range of activities, such as assessments on security health, security process, application security, network security, system security, site security, internal security; ethical hacking, privacy strategy development, and information asset profiling. For example, an IBM Security Health Check review can identify both the strengths and weaknesses of an enterprise's IT security controls. It will provide an overall view of how effectively an enterprise's security plan is working. It checks that the appropriate IT security controls are in place to protect the information that is critical to an enterprise's business. It checks security safeguard coverage of the enterprise, including mechanisms used by hardware and software systems, networks, databases and human-resource systems. These services are based on the IBM Enterprise Security Architecture offering, which provides a comprehensive, standards-based framework for managing an enterprise's security program, and is designed to align with business objectives. For more information on this architecture access <http://www.ibm.com/services/e-business/archspec.html>

IBM Security and Privacy Services can support an enterprise's resourcing strategy with a variety of offerings. Besides serving in consulting and training capacities, as previously mentioned, IBM can implement and manage a wide-range of security services and solutions within an enterprise or serving in an outsourcing capacity. These management services span intrusion-detection services, alarm generation and notification, escalation procedures in the case of an intrusion, vulnerability scanning, firewall management, monthly reporting, policy recommendations, virtual private networks (VPNs), antiviruses, Web filtering and content blocking, and routers. Security specialists from IBM Managed Security Services can work to identify and overcome realtime security risks using a proven, continuous management process— all backed by a proven track record of successful engagements. Again IBM Security and Privacy Services can provide end-to-end services that include assessing, planning, designing, implementing and managing a customer's environment.

Tivoli SecureWay solutions comprehensively address security and privacy requirements and have been designed to be easy to plan, deploy, and operate.

Call to Action:

IBM is ready to assist an enterprise in developing and deploying a trusted e-business environment with a broad range of services and solutions. With IBM Security and Privacy Services, and IBM's Tivoli SecureWay solutions, IBM can help an enterprise strengthen its end-to-end e-business Security and Privacy capabilities to meet the challenges of a trusted e-business environment. To contact an IBM e-business specialist call 1-800-IBM-7080 extension INFRA000. Toll-free in the US and Canada.

¹ Refer to "IDC's "Stengthening End-to-End e-Business Security" brief, dated June 2001

Somers, New York 10589
U.S.A.

Produced in the United States of America
06-01
All Rights Reserved

IBM, the IBM logo, the e-business logo, DB2, MQSeries, SecureWay and WebSphere are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Lotus and Lotus Notes are registered trademarks of Lotus Development Corporation in the United States, other countries, or both.

Tivoli is a registered trademark of Tivoli Systems, Inc. in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc., in the United States, other countries, or both.

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

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.