IBM SecureWay FirstSecure Version 2, Policy Directory, and Boundary Server — Open for Trusted e-Business

Overview

SecureWay™ FirstSecure is the premier security solution for deploying secure e-business. With FirstSecure Version 2, IBM delivers the security enhancements companies need to achieve their e-business goals and enable them to:

- Transform core business processes
- Rapidly deploy e-business applications
- Operate effective and secure IT infrastructures
- Leverage critical business information and experience to create faster, smarter organizations

SecureWay FirstSecure enables companies to build and operate a secure environment in which to conduct trusted e-business. FirstSecure offers an integrated, policy-driven solution to meet IT security needs. It provides digital identity authentication support, network boundary and virus protection, intrusion detection, and tools for developing secure applications.

SecureWay FirstSecure enhancements include:

- SecureWay Policy Director — additional integration, enhanced scalability and standards compliance through use of Lightweight Directory Access Protocol (LDAP) and Public Key Infrastructure for X.509 (PKIX) certificates, improved access control through use of an authorization framework, and streamlined administration achieved through an integrated management console.
- SecureWay Boundary Server — simplified administration, support for the latest industry standards, improved protection, and logging and content filtering.
- SecureWay Trust Authority, included in FirstSecure, is a new public key infrastructure based on the Internet Engineering Task Force’s (IETF) Public Key Infrastructure (PKI) Working Group specifications. Trust Authority is targeted for use in medium risk environments.
- Intrusion Immunity — expanded to include an intrusion detection offering — Tivoli Cross-Site for Security
- SecureWay Toolbox — includes additional application programming capabilities.
- FirstSecure Implementation Services — support FirstSecure Version 2 capabilities.

SecureWay Policy Director, Boundary Server, and Trust Authority are included in SecureWay FirstSecure and are also available as separately orderable security solutions.

Key Prerequisites

The SecureWay FirstSecure offerings are supported on:

- RISC System/6000® with AIX 4.3.2 (5765-C43), or later
- Intel-based system with Microsoft™ Windows NT™ 4.0
- Sun SPARC system with Solaris 2.6

Refer to Hardware and Software Requirements for component specific requirements.

Planned Availability Date

October 29, 1999

At a Glance

SecureWay FirstSecure:

- Reduces exposure to an ever-increasing number of internal and external threats by providing end-to-end security
- Permits secure communication with customers, suppliers, and partners which enables personalized e-business services
- Extends and scales for e-business growth and enhancement
- Reduces the resources required to develop and manage secure e-business applications
- Delivers a comprehensive and extensible security framework based on open industry standards
- Extends and enforces permissions policy at the application and network level across multiple platforms without changing existing applications
- Allows permissions policy to be centrally defined and administered
- Minimizes user and group administration efforts with an easy-to-use graphical interface
- Offers implementation services to jump-start trusted e-business

For ordering, contact:
Your IBM representative, an IBM Business Partner, or IBM Americas Call Centers at 800-IBM-CALL

Reference: YE001
SecureWay FirstSecure provides a comprehensive, modular framework to help companies establish a secure e-business environment. By reducing complexity, FirstSecure helps reduce the total cost of security ownership, enables security policy to be implemented more easily, and increases the effectiveness of the secure e-business environment.

FirstSecure includes virus protection, access control, traffic content filtering, multiple levels of encryption, digital certificates for strong authentication, firewall and virtual private network (VPN) technology, and software development kits.

**Implementation Services**

FirstSecure Implementation Services are recommended to help customers get the FirstSecure framework up and operational quickly and efficiently. These separately billable services are provided by IBM and are performed by a team of consultants. The consultants have close ties to the IBM product development organization improving the level of effective resolution of implementation issues. The FirstSecure Implementation Services include a FirstSecure Implementation Workshop and product level QuickStart installation services. IBM can also provide FirstSecure system integration services that are customized to the environment of an individual customer. Visit Web site:

http://www-4.ibm.com/software/secureway/services/

for additional information.

**SecureWay Policy Director**

The SecureWay Policy Director provides a comprehensive solution to secure access to application resources within corporate intranet and extranet environments. It is also designed to secure access from public networks to these same application resources and can scale to support hundreds of thousands to millions of Internet customers. The Policy Director provides an authorization server accessible via an easy to use Authorization API that is the basis of the aznAPI specification being standardized by the Open Group.

Policy Director components, WebSEAL and NetSEAL, use the Authorization API to provide fine-grained access control for Web applications and resources without requiring modifications to your existing Web-based applications. This enables organizations to authorize and secure traditional Internet services such as Telnet and POP3.

The Policy Director includes IntraVerse technology and has been enhanced by IBM to include “out of the box” support for PKI based authentication, including CRL checking using IBM Trust Authority, IBM Vault Registry, or Entrust certificates. Policy Director is translated into French, German, Italian, Spanish, Brazilian Portuguese, Japanese, Korean, Traditional Chinese, and Simplified Chinese.

Additional Policy Director enhancements include:

- SecureWay Directory support for user and group credential information storage
- The latest updates to the Authorization API as specified by the Open Group
- Ability to define and edit IBM Firewall proxy user credentials using the Policy Director Management Console
- A Credential Acquisition Service (CAS) enables use of external authentication services as well as client-side certificate based authentication
- The ability to write your own customized Credential Acquisition Service using the Interface Definition Language (IDL) interface between WebSEAL and the Policy Director CAS. Policy Director also provides the general server framework that handles Policy Director CAS functions such as startup, server registration, and signal handling.
- A Secure Sockets Layer (SSL) tunneling mechanism in addition to generic security services (GSS) tunneling.
- Use of the Policy Director Management Console or the command line interface to manage login and password policies and single sign-on users, groups, and targets.
- A utility to assist Policy Director Version 1 users migrate their user and group credential data to the SecureWay Directory Server (LDAP).
- An integrated installation process.

The SecureWay Policy Director includes a number of components that work together to deliver its services. These components are:

- WebSEAL
- NetSEAL
- Management Console Server
- SecureWay Directory Server (LDAP)
- Authorization Server
- IBM DCE Directory and Security Services
- NetSEAT Client

You will need to install some or all of these depending on your environment and the product features you plan to use.

**WebSEAL Server**

The WebSEAL server is used to secure and manage intranet-based resources. Access to these resources is available to users through Web-based intranets and to remote users via the Internet. WebSEAL is a high performance authorization engine for Web applications. The unique value of WebSEAL is that it provides a consolidated point of control for heterogeneous Web environments. It authorizes and manages an entire Web site, regardless of how many different servers and server types are involved.

WebSEAL uses innovative technology to extend fine-grained security to IBM, Apache, Netscape, and Microsoft supported Web servers. WebSEAL forms logical connections between itself and these Web servers, allowing the creation of an expanded Web space made up of resources from each of these servers. WebSEAL can be used as a smart and secure front-end to an existing intranet implementation.

WebSEAL implements a highly scalable, highly available, multi-tiered, model for the Web. The tiers are composed of clients, junction servers, and Web servers. As the authorization engine for the Web, WebSEAL allows fine-grained access control to all Web objects including HTML pages, graphics, CGI, Java™ applications, and database queries.

WebSEAL also includes a CAS that supports the use of external acquisition services. One CAS module supports client-side certificate based authentication. Customers can develop their own CAS modules to support other authentication types.

WebSEAL provides user level client/server security on a per-connection basis. WebSEAL is independent of network topology and location. Security credentials are based on who your user is, not where your user is.

WebSEAL can be configured to complement and extend SecureWay Boundary Server or your existing firewall. By
using WebSEAL with the Boundary Server, business policy, not geography, determines your access policy.

**Key Features and Benefits:** WebSEAL provides security in the following ways:

- **Authentication** — User identities can be positively established through the use of either a user id and password or PKI based authentication using IBM Trust Authority, IBM Vault Registry or Entrust certificates
- **Authorization** — Once the user’s identity is positively established, access to sections of your Web is granted or denied based on the user’s identity through the use of the Authorization API. Access controls can also be used to allow unauthenticated users access to an extranet or other parts of your intranet. Access controls are placed on the individual Web objects rather than the entire Web application.
- **Data privacy and integrity** — SSL encryption technology can be employed to minimize the risk that your sensitive information could be intercepted or read by unauthorized users or suffer undetected corruption.
- **Auditing** — Attempts to access your intranet through WebSEAL can be audited and logged.

**NetSEAL Server:** The NetSEAL server is used to secure traditional Internet services including Telnet and POP3. NetSEAL also authorizes and secures third party applications including database systems, network management tools, and object request brokers. NetSEAL even enables you to extend access to in-house applications with authorization.

Managed access to these network resources is provided to users through the enterprise intranet and to remote users via the Internet. This is accomplished in a non-intrusive manner since no changes need to be made to existing applications on the client or server. NetSEAL separates the authorization policy and the application, providing a level of abstraction between physical and logical views of your security policy for network data.

NetSEAL provides user level client/server security on a per-connection basis and is independent of network topology and location. Security credentials are based on who, not where, your user is.

NetSEAL can be centrally managed for the entire enterprise and configured to complement and extend your existing firewall product.

NetSEAL is a fully extendable authorization engine that allows end-to-end tunneling. By using architecture independent plug-ins, fine-grained authorization can be applied to new applications. NetSEAL allows integration with third-party authorization infrastructures and provides authorization for applications including conferencing, database, and EDI.

etSEAL is enhanced to support the SSL protocol. This allows NetSEAL to work better with your firewall by minimizing the number of ports needed to allow NetSeat/NetSEAL communications.

NetSEAL provides a complete secure authorization and network management solution. It enables you to effectively manage your network environment and provide secured information access to internal and external users.

**Key Features and Benefits:**

- **Authentication** — User and server system identities can be positively established through the use of a user id and password, or PKI based authentication using SecureWay Trust Authority, IBM Vault Registry, or Entrust certificates
- **Authorization** — Once identity is established, access to network based applications is granted or denied based on the user’s identity. Authorization is available at the application level on the client and the server.
- **Data privacy and integrity** — Encryption technology can be employed to minimize the risk that your sensitive information could be intercepted or read by unauthorized users or suffer undetected corruption.
- **Auditing** — Attempts to access a resource secured by NetSEAL can be audited and logged.

**Authorization Server:** The Authorization Server provides an API that can be used from within an application to provide sophisticated access control processing. This API, aznAPI, is the first production implementation of the new Open Group standard for cross-platform authorization services. The Authorization Server allows custom applications to make fine-grained application and authorization level authorization decisions. Using the aznAPI, you can build security and authorization directly into your corporate applications. This leverages the Policy Director services helping reduce application development time and cost. By taking advantage of this capability, you can have your network managed centrally by Policy Director, which can significantly reduce the total cost of ownership and the likelihood of security breaches. You can customize your users’ network view to match their access privileges and create customized menus based on authorization information.

**Additional Policy Director components:**

- **Management Console** — a graphical Java-based application used to add and delete users or groups and apply access controls (ACLs) to the objects and resources secured by the Policy Director. An enhancement enables the Console to be used to define and edit user credentials for the SecureWay Firewall Version 4.1.
- **Management Server** — maintains the primary authorization policy database for the secure domain. It is also responsible for updating all authorization database replicas. The management server also maintains location information about the other policy director servers.
- **SecureWay Directory** — a powerful enterprise directory used to securely store Policy Director user and group credentials as well as credential sets for target Web servers. It is an open, cross-platform program optimized to support LDAP enabled applications. The SecureWay Directory uses DB2 Universal Databases as its transaction store for directory data extending the performance and availability of the Policy Director.
- **NetSeat Client** — a small, lightweight network services module located on a client machine that proxies the communication between TCP/IP based client applications and the server. NetSeat supports SSL protocol to work better with your firewall by minimizing the number of ports that need to be opened to allow NetSeat/NetSEAL communications. It can be easily delivered over the intranet or Internet helping reduce software distribution and management costs.

Description in continued in the **Supplemental** section.

**Euro Currency**

These programs are not impacted by euro currency.
Product Positioning

The SecureWay FirstSecure solutions are targeted for Global 2000 companies — large companies with 1000 or more employees and revenues of more than 200M U.S. dollars — and medium sized firms — companies with 500 to 1000 employees — that are planning to connect to the Internet, expanding their use of the Internet by deploying more Web-based applications, and/or deploying an extranet to connect business partners, customers, and remote employees.

Statement of Direction

IBM intends to provide the following modules and/or enhancements in future product releases or as separately priced products.

- **CORBA Support** — IBM plans to deliver a Policy Director module that will provide single sign-on and authorization management for enterprise CORBA environments. It is planned to support secure interoperability between Object Request Brokers (ORBs) available from Inprise and IONA, providing users with the flexibility in their development and deployment of CORBA applications. IBM plans for the module to provide a CORBA Security Service to implement controlled delegation. This function is intended to provide the ability to pass user and server information with a transaction request, enabling extremely fine-grained access control.

- **MQSeries® Support** — IBM plans to deliver a Policy Director module that will provide customers with the ability to create authentication policies, data protection policies, and authorization policies for MQSeries.

- **Tivoli Integration** — IBM plans to provide support that will enable customers to use Tivoli User Administration and Tivoli Security Management to manage Policy Director users and access control policies.

- **Enhanced Single Sign-On support** — IBM intends to enhance Policy Director’s Web credential mapping service to support PKI and other stronger authentication systems.

- **SecureID Token Support** — IBM plans to enhance Policy Director to provide support for authentication using Security Dynamics SecureID tokens without requiring any customer level customization.

- IBM intends to provide support of FirstSecure on AIX 4.3.3 and Policy Director support on Solaris 2.7

These statements represent the current intent of IBM and are subject to change or withdrawal without notice.

Trademarks

SecureWay and WebSphere are trademarks of International Business Machines Corporation in the United States or other countries or both.

RISC System/6000, DB2 Universal Database, AIX, Netfinity, OS/2, NetView, and MQSeries are registered trademarks of International Business Machines Corporation in the United States or other countries or both.

Microsoft, Windows NT, and Windows are trademarks of Microsoft Corporation.

Java is a trademark of Sun Microsystems, Inc.

Lotus Notes is a registered trademark of Lotus Development Corporation.

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

SecureWay™ Trust Authority Version 3.1: Trust Authority Version 3.1 is an integrated PKI solution that enables e-business by issuing digital certificates worthy of trust. It is a cross-platform, easy-to-use offering with manual and automated registration capabilities. It is targeted at medium and large enterprises and ISVs. It provides the capability to perform complete lifecycle management of certificates through the Trust Authority Client or a standard Web browser. Trust Authority issues standard certificates such as S/MIME, IPSec (for VPNs) and server certificates. It also provides the flexibility to add user defined extensions.

The Trust Authority application adheres to the PKIX standards. The CA includes advanced features such as cross-certification certificate extensions. Trust Authority uses IBM KeyWorks for cryptographic and key store functions.

The Trust Authority is supported on AIX® 4.3.2 and NT 4.0.

The SecureWay Trust Authority Version 3.1 is included in the FirstSecure product and is also separately available. The Trust Authority Version 3.1 product is not the replacement product for IBM Vault Registry. Refer to Software Announcement 299-317, dated October 26, 1999, for additional information about IBM SecureWay Trust Authority and plans for IBM Vault Registry.

Key Features and Benefits

• Enables organizations to issue, publish, and administer digital certificates in accordance with their registration and certification policies
• Provides support for PKIX and Common Data Security Architecture (CDSA) cryptographic standards enabling vendor interoperability
• Provides digital signing and secure protocols enabling authentication of all parties in a transaction
• Provides browser and client-based registration capabilities for maximum flexibility
• Provides encrypted communications and secure storage of registration information for confidentiality
• Supports very large numbers of users by using advanced cross certification and hierarchy support
• Supports custom applications by issuing user defined extensions in certificates

SecureWay Boundary Server

SecureWay Boundary Server includes the following:
• SecureWay Firewall Version 4.1 including a two user license of ACE/Server from Security Dynamics
• MIMEsweeper for SecureWay Release 2 from Content Technologies
  - MAILsweeper
  - WEBsweeper
• SurfinGate 4.05 from Finjan
  - SurfinGate Server
  - SurfinConsole
  - SurfinGate database
  - SurfinGate WTE Plugin

SecureWay Firewall Version 4.1: The SecureWay Firewall enables safe, secure e-business by controlling all communications to and from the Internet. This firewall technology was developed by IBM research and has been protecting IBM and global corporations’ assets for more than 10 years. Unlike most other firewalls, the IBM firewall contains all three critical firewall architectures — filtering, proxy, and circuit level gateway — to provide customers a high level of security and flexibility.

The SecureWay Firewall protects your networks from outsiders by allowing only explicitly permitted traffic through the firewall. The server that the firewall is running on is “hardened” to remove potential security vulnerabilities of the underlying operating system. The IP addresses and configuration of the internal network are hidden from the untrusted network. All traffic through the firewall is logged and can be used to generate user activity and audit reports. Firewall Enhancements for the Windows NT and AIX Platforms

HTTP Proxy is upgraded to an implementation based on the WebSphere™ Performance Pack Web Traffic Express (WTE) component. Capabilities of this robust proxy include:

• Support for the HTTP 1.1 protocol
• URL blocking via a wildcard text matching technique
• SNMP subagent and MIB support
• Enhanced logging capabilities
• Support for user authentication

Socks V5 is upgraded to Aventail Corporation’s level 3. The Socks Version 5 protocol provides a general purpose proxy function for TCP and UDP applications including:

• HTTP
• FTP
• Telnet
• NNTP
• RealAudio
• RealVideo
• CU-SeeMe
• VDOLive
• Archie
• Finger
• Gopher
• SNMP
• WHOIS

Socks V5 also provides user authentication and supports inbound connections from non-secure domains. More granular logging and a real time Traffic Monitor are included with this upgrade. Socks 4 connections are
Secure Mail Proxy is enhanced with a number of unique key features to protect messaging networks:

- Helps verify fraudulent communication (anti-spoofing — protections reduce the risk of forgery or impersonation)
- Helps protect against the theft of resources (anti-relay — disallow the use of the messaging system for relay)
- Filters objectionable or undesired communications (anti-spamming — detection and rejection of SPAM).

Additional enhancements for AIX Platform:

- Symmetric Multi-Processor (SMP) support for RISC System 6000 computers running the AIX Firewall provides the price/performance associated with SMP processor configurations.
- VPN Support for the AIX Firewall is upgraded to the IPSec Standards. Triple DES encryption is supported as well as 56-bit DES encryption.
- Expert Filters processing of packet filter rules is implemented with significant enhancements to improve performance and ease administration:
  - Activation of filter rules and scanning the rules for packet matches is now more efficient.
  - The frequency of rules matched during packet filter processing is maintained to enable better tuning of the firewall.
  - Dynamically activated rules (for IPSec and Real Audio connections, for example) can be displayed for easier administration.
- Many-to-one Network Address Translation (NAT) is implemented to enable multiple internal IP addresses to be mapped to a single registered IP address so the internal IP addresses are not visible while in transit over a public network. A technique called Network Address Port Translation is employed to implement this function.

The VPN and Many-to-one NAT support described above is functionally similar to that provided in the Version 3.3 release of the IBM Firewall for Windows NT and is maintained in Version 4.1 SecureWay Firewall supports two-and four-way Intel-based SMP processors such as Netfinity®. The configuration wizard and German language translation support available for the Windows NT Firewall is now available on the AIX Firewall.

**Key Features and Benefits**

- Three firewall technologies — by providing support for all three standard firewall architectures (expert filters, application proxy, SOCKS circuit-level gateway) you have great flexibility in enforcing your security policy.
- Isolation of subnets — keeps multiple subnets within a network securely separated from each other letting policy be set on how subnets can communicate. It allows a demilitarized zone to service Internet users without the users having to enter the secure network.
- Expert filters — controls traffic by time-of-day, address, port number, direction, protocol. Expert filters make it easy to configure the firewall to disallow inappropriate bandwidth-consuming traffic.
- Hardening — provides a secure platform for the firewall. Hardening reduces configuration errors that can lead to security exposures and security holes from unneeded operating system services or applications.
- Network Security Auditor — helps increase security by proactively scanning the firewall for security exposures. It generates easy-to-read HTML-formatted reports, allowing the administrator quickly find configuration errors.
- SOCKS Watcher — graphically displays real-time performance statistics, throughput, and bandwidth utilization by service (for example, Telnet, FTP, and HTTP), connection, userid, port, and address.
- Reporting/Logging — provides the data to allow you to manage and audit your Internet connection.
- Alerting — provides automatic and immediate notification of security breaches via e-mail and pager.
- Secure Mail Proxy — supporting SMTP and mime extensions, it complements SendMail applications while eliminating security problems of SendMail. Mail is not stored on the firewall and private domain names are hidden on outbound mail.
- Administration through a Java-based GUI — enables one or more remote firewalls, or a local firewall, to be administered. Different levels of product functions can be specified for individual administrators, with logging of administrator actions.
- Enterprise Firewall Manager — enables multiple firewalls to be configured from a single point, helping reduce the cost and complexity of managing multiple firewalls.
- Strongly Authenticate Firewall Administrators — the Security Dynamics ACE/Server (two-user license) and two SecurID tokens, both included at no additional charge, provide strong authentication capability.
- Setup Wizard in Firewall 4.1 for NT — helps reduce administration time and associated costs to configure the Firewall.

**Security Dynamics ACE/Server:** Packaged with the SecureWay Firewall is a two user ACE/Server that provides strong authentication services to authenticate firewall administrators and remote users connecting through the firewall’s Windows™ 95 VPN client. In conjunction with its patented SecurID token technology, ACE/Server creates a barrier against unauthorized access. It helps protect your network and data resources from potentially devastating accidental or malicious intrusion.

**MIMEsweeper for SecureWay Release 2:** MIMEsweeper is a compliment to Firewall and anti-virus network security solutions. MIMEsweeper provides Content Security, by analyzing the data passing through the Firewall via electronic mail or the world wide web. Content Security allows organizations to effectively manage business issues related to the use of e-mail and the world wide web. These issues can be divided into two categories of business threats.

**Network Integrity:**

- Identification and removal of viruses in incoming and outgoing e-mail.
- Filtering of undesirable file types.
- Management of oversize files.
- Protection from network congestion or loss of service from mail-bomb attacks.

**Business Integrity:**

- Prevention of confidentiality breaches and loss of trade secrets.
- Control of exposure to legal liability.
• Productivity loss from employee misuse of e-mail and world wide web services.
• Protection from loss of network service through misuse and hostile attacks.
• Threats to network integrity can corrupt or erase data, disrupt e-mail flow and ruin system hardware; all of which can resulting in network downtime, lost productivity and high cleanup and recovery costs.
Threats to business integrity, however, can be far more destructive, resulting in enormous legal costs, lost intellectual property, and damaged corporate reputation and credibility. Business integrity issues can bring your commercial operations to a standstill.
MIMEsweeper is the industry leading product for protecting organizations from the Network and Business Integrity issues posed by organizational usage of e-mail and the Internet.
MIMEsweeper is comprised of two content filtering components — MAILsweeper for email threats, and WEBsweeper for other threats originating in the World-Wide Web. As mail and other Web files enter MIMEsweeper, MIMEsweeper verifies the from and to addresses and then recursively disassembles the files into their component parts.
MAILsweeper and WEBsweeper analyze these parts to minimize the risk that threats could enter the private network.

Key Features and Benefits:

MAILsweeper
• Works with virus scanners to verify that the disassembled component parts are free of viruses.
• Scans for key words and:
  − Can help block harassing or otherwise libelous mail that might originate from employee’s work e-mail accounts
  − Helps protect valuable data from leaving the company
  − Blocks incoming e-mail spam, leaving the network less congested and saving employee time
  − Can block individuals or groups from sending or receiving certain types of files, such as AVIs or MPEGs
  − Blocks or delays files by size until the network can better accommodate the traffic.

WEBsweeper
• Blocks employees from certain sites likely to be non work-related
• Helps detect and if necessary, blocks dangerous Java and ActiveX code before it enters the network
• Helps prevent attacks to extract documents via HTML, or e-mail addresses and site information via cookies

Enhancements in this release for MAILsweeper for SMTP:
• MAILsweeper version 4 for SMTP is the new standard in content security policy enforcement. This major upgrade to Content Technologies flagship MIMEsweeper product offers many significant new features like:
  • An easy to use, hierarchical policy architecture provides the flexibility to apply policies at the appropriate organizational level right down to the individual user.
  • An intuitive, industry standard graphical user interface simplifies software configuration, policy creation, and administration.
• The new Split Delivery feature is a function of the hierarchical policy implementation of version 4. For messages with multiple recipients, policies are applied to each recipient. Authorized recipients receive the message while unauthorized recipients are denied.
• Multi-threaded message processing improves throughput and adds robustness by allowing message processing to continue, using remaining threads, if an error occurs on one or more threads.
• In conjunction with other vendors’ antivirus products, MIMEsweeper provides full support for virus detection and cleaning of messages and attachments. Content security is easier to manage using attractive reports, graphs, and charts for e-mail traffic.
• Advanced text analysis using NEAR, AND, NOT, and OR expressions provide tremendous flexibility in creating comprehensive, effective scenarios based on message syntax or architecture.
• Support for the “Real-Time Black List” (RBL) server which lists sites that are known to send out junk e-mail. MAILsweeper can refuse to accept connections from any host in this list.
• Enhanced auditing tools that can send data to any ODBC-compliant database or text file allowing users to easily monitor critical message processing metrics.
• Delivery Service Notification (DSN) now supports SNMP and NT Alerter.

Enhancement to this release for WEBsweeper:
• WEBsweeper now provides full support for web based e-commerce applications via a new HTTPS proxy solution.
• Additional performance enhancements improve data processing speed as compared to previous versions.

SurfinGate Version 4.05:
SurfinGate 4.05 is a mobile code security tool for any business using the Internet, extranet, or intranet for business transactions. Through content inspection of mobile code, including JavaScript, SurfinGate helps protect computer networks from hostile or unintentional damage including industrial espionage, data modification, and information deletion.
SurfinGate’s content inspection process inspects Java, JavaScript, and ActiveX mobile code content at the gateway level, away from critical resources, and assigns a unique ID and applet security profile (ASP) to code, noting any possible security breaches. SurfinGate identifies potentially problematic code before it can enter the network.

SurfinGate 4.05 components:
• SurfinGate Server
• SurfinConsole
• SurfinGate database
• SurfinGate WTE Plugin
SurfinConsole is a user-friendly interface for managing and setting a central corporate security policy for mobile code. SurfinConsole can control multiple SurfinGate Servers on the network and can enforce mobile code rules throughout the organization per user, per group, or through custom lists or unacceptable/acceptable code.
The SurfinGate database stores details of Applet Security Profiles (ASP), including information regarding user and
groups and their corresponding security policies. The database can use a built-in Access database engine or an existing Oracle database. Since SurfinGate inspects content of all mobile code on the fly, the database is not required for security, but does help improve performance in large-scale operations.

With SurfinGate, you have control over Java, JavaScript, ActiveX, and other mobile code activity in the corporation. SurfinGate helps prevent undetected, costly mobile code attacks such as political hack attacks, corporate espionage attempts, and Web graffiti damage. SurfinGate provides detailed logs and mobile code reports that help prove “minimum level of care” security often legally required in public companies. You can safely surf the Internet/intranet/extranet while taking full advantage of Java, JavaScript, and ActiveX technologies.

SurfinGate Version 4.05 enhancements:

JavaScript Content Inspection
- Looks for potentially problematic JavaScript operations and stops JavaScripts that conflict with corporate security policy.
- Allows administrators to centrally set and enforce a policy for JavaScript, Java, and ActiveX, with smart filtering for VisualBasic Script and cookies.

Mission-Critical Performance Monitoring
- Includes an automatic tool that detects abnormal behavior (such as runtime errors) and re-starts SurfinGate in case of failure. This is an essential security feature for mission-critical areas.

Increased Policy Management
- Enters unresolved applet profiles into the database for automatic blocking. Administrators can edit the list of applets/controls.

Support for FTP and HTTPS Protocol
- Monitors File Transfer Protocol (FTP) channels for mobile code, keeping watch on code that could otherwise sneak in unannounced from the Internet.
- Monitors HTTP.

Intrusion Immunity

Norton AntiVirus Solution Suite Version 3.04:
Norton AntiVirus Solution Suite components:

Desktop Solutions
- Version 4.08 for DOS
- Version 4.08 for Microsoft Windows 3.1
- Version 5.02 for Microsoft Windows 95/98
- Version 4.08 for Microsoft Windows NT 3.51
- Version 5.02 for Microsoft Windows NT 4.0
- Version 5.0.3 for Macintosh
- Version 5.02 for OS/2®

Server Solutions
- Version 4.08 for Microsoft Windows NT 3.51
- Version 5.02 for Microsoft Windows NT 4.0
- Version 4.04 for NetWare
- Version 2.0 for Lotus Notes® (Windows NT & OS/2)
- Version 1.52 for Microsoft Exchange

Gateway Solutions
- Version 1.02A for Internet E-mail Gateways for Windows NT
- Version 1.04 for Firewalls

Administration
- Version 3.1 Norton System Center
- Version 5.03 for Macintosh Administrator
- Version 5.0 for NAV Plus for Tivoli IT Director
- Version 5.0 for NAV Plus for Tivoli Enterprise

Key Features and Benefits
- Quarantine — isolates infected files in a safe corner of your computer until you’re able to repair them. This quarantine area helps you make sure that your other files stay clean and that you don’t accidentally send infected files to anyone else.
- Scan and Deliver — Scan and Deliver wizard makes it easy to send quarantined, or other suspicious, files to Symantec for evaluation.
- The Symantec AntiVirus Research Center (SARC) staff will reply swiftly with helpful advice and any needed virus definitions.
- LiveUpdate — enables Norton AntiVirus to automatically retrieve new virus definitions from Symantec as often as once a week. This software downloads only the newest definitions, so updates are small, fast, and efficient.
- Surf the Internet safely — provides the industry’s most complete protection against malicious codes. Besides thousands of viruses, it can detect and remove dangerous forms of ActiveX code, Java applets, and Trojan horses. SARC personnel are constantly searching the World Wide Web for malicious code updating Norton AntiVirus to protect against it.
- 24-hour protection — Norton AntiVirus can run constantly in the background to keep your computer safe from viruses that might come in from e-mail attachments, Internet downloads, floppy diskettes, software CDs, or a network. Built-in Bloodhound technology “sniffs out” new viruses that might arise between virus updates.

Tivoli Cross-Site for Security Version 1.1: Securing your network from external and internal intrusions is essential to the success of your e-business. Tivoli Cross-Site for Security enables you to detect, log, and respond to unauthorized or suspicious activities in real time. Tivoli Cross-Site for Security components:
- Tivoli Cross-Site for Security agent
- Tivoli Cross-Site for Security management server

The Tivoli Cross-Site for Security agent monitors network traffic and detects attack signatures in real-time. The matching of a default or customer defined attack signature generates an alert to the management server. The agent is highly configurable and the customer can specify the parameters that trigger alerts, such as activity type, source, destination, or time of day. The alerts are categorized into one of three degrees of severity — critical, serious, or non-critical — to allow staff to react appropriately. The Tivoli Cross-Site for Security server receives the alerts from the security agents and enables you to manage the security events in the network. A current view of the alerts and pre-defined reports is available from the administrator’s console, which can be run securely on virtually any system in the network. In addition to managing the alerts, the management server
handles standard and custom reports and client configuration updates. Security alerts can be forwarded to the Tivoli Enterprise Console, Tivoli NetView®, and other management systems for a scalable, three-tier environment.

**Key Features and Benefits**

- Non-disruptive deployment: This deployment mechanism uses technology licensed from Marimba, Inc. Customers have production networks that they have spent lots of energy in designing, installing, and maintaining. A key design goal is to enable you to deploy the lightweight intrusion detection agents into these production environments in a non-disruptive manner.
- Scaleability: Tivoli integration and scalability are key features of Tivoli Cross-Site for Security. Customers need their network/system management capabilities to be tightly coupled with intrusion detection to have a clear picture of real-time intrusions. The Tivoli Enterprise Console can be used to build a three tier intrusion detection management system.
- IBM validates attacks and distributes new attack signatures: IBM security skilled employees (our best security development and research skills) are engaged to identify and validate new attacks and rapidly distribute those attack signature definitions to customers.
- Encrypted communications between client and server helps prevent malicious intervention. This is provided via 128-bit SSL for the US and Canada as well as specific business sectors in approved countries.
- Fine tuning — each agent can be configured for a specific system or area of the network to help minimize false alarms and lower the cost of administration.
- New attack signatures can be deployed rapidly to clients from the management server.
- Extensive pre-defined reports available along with customized report capability.
- Custom attack signatures can be created and deployed.

**SecureWay Toolbox**

The SecureWay Toolbox is a collection of software development toolkits (SDKs) that let you build on and customize your security implementations. These related security and cryptographic toolkits, and APIs allow enterprise and other customers (such as OEMs) to customize and interface applications and middleware with FirstSecure components such as Trust Authority and Policy Director.

The Toolbox includes:
- IBM KeyWorks Toolkit Version 1.1.3
- IBM Key Recovery Service Provider Version 1.1.3
- IBM Key Recovery Server Version 1.1.3
- SecureWay Policy Director Authorization API
- Secure Sockets Layer (SSL) Toolkit — a Java based SSL toolkit
- Trust Authority Toolkit — a PKI toolkit
- SecureWay Directory Client Toolkit and Security Enabler

**IBM KeyWorks Toolkit:** The IBM KeyWorks Toolkit provides developers an open, extendable, and standards-based approach of accessing cryptographic, trust, and other security functions across different operating environments using an extendable and adaptable middleware framework. The Toolkit is based upon The Open Group’s Common Data Security Architecture (CDSA).

Standard interfaces enable organizations to select and change cryptographic and trust implementations to best suit their needs without requiring changes to the applications that use the security services. The toolkit enhances programmer productivity by providing standard means of accessing cryptographic and other security functions across different operating environments.

The IBM KeyWorks Toolkit provides an insulating layer between an application program and security functions. The toolkit consists of a framework and Service Provider plug-in modules with a standard set of Application Programming Interfaces (API).

The functionally rich Common Security Services Manager (CSSM) API based on the CDSA is extended to include key recovery functions. The Service Provider — the standard Service Provider Interface (SPI) based on the CDSA —includes key recovery support.

The KeyWorks Toolkit provides function to:
- Encrypt and decrypt information
- Verify a digital signature
- Retrieve a certificate from a directory
- Create key recovery fields
- Decide if a certificate can be trusted.

The IBM KeyWorks Toolkit provides critical “administrative” functions including:
- “Non-circumventability”
- Tamper proof service providers
- Restricting Service Provider “plug-in” use to framework only
- Support of country and enterprise specific usage policies

Plug-in Service Providers are also included with the IBM KeyWorks Toolkit. These modules support open standards including:
- PKCS#11
- RSA’s cryptographic functions
- X.509v3 certificates
- Trust policies of Entrust and Verisign
- LDAP

The framework provides seamless integration of the security functions provided by each independent service provider module.

**Key Features and Benefits**

- Enables the change or substitution of service provider modules with minimum impact on the application
- Provides support for hardware encryption
- Supports LDAP directories and the DSA signature standard
- Does not require use of a particular certificate authority

It is essential that an enterprise that undertakes to use the IBM KeyWorks Toolkit has systems engineering and cryptographic programming staff with the experience and background to program to the extensive API set in KeyWorks.
**IBM Key Recovery Service Provider:** The Key Recovery Service Provider is a specialized service provider for the KeyWorks framework.

The IBM Key Recovery Service Provider plug-in enables the recovery of encrypted information. It utilizes the standard functions provided by the IBM KeyWorks Toolkit. Consequently, the key recovery function can be used with different cryptographic suppliers, standard certificates from various Certificate Authorities, trust policies from Verisign and Entrust, and directories that can be accessed by LDAP.

The IBM Key Recovery Service Provider creates key recovery information based upon the session key associated with the communication between correspondents. It does not cause the escrow of private keys avoiding the implementation of single points of security failure.

**IBM Key Recovery Server:** The Key Recovery Server is a Microsoft Windows NT based application that consists of the KeyWorks framework with altered user and communications interfaces, and allows recovery of corporate data using the IBM Key Recovery process. This application is required for developing and testing application runtimes using KeyWorks framework and Key Recovery Service Provider.

**Secure Sockets Layer Toolkit:** The Secure Sockets Layer Toolkit is a pure Java implementation of a toolkit designed to support secure TCP/IP applications. SSL APIs provide basic SSL protocol and utilities services in the Java programming language. The SSL APIs are a few simple programming objects designed to quickly add the SSL protocol to any Java application. Advanced programmers will find the SSL APIs have the in-depth functionality to write robust PKI based products.

The SSL APIs provide an implementation of SSL Version 3 as specified by Netscape and published at:


SSL APIs support the industry standard RSA ciphersuites.

**SecureWay Public Key Infrastructure for X.509 (PKIX) toolkit:** This PKIX toolkit (equivalent to Trust Authority Version 3.1) is an entry level offering of a Certificate Authority toolkit. The toolkit is a cross-platform, easy-to-use offering with registration and installation capabilities targeted at medium and large enterprises, OEMs, and ISVs with less sophisticated operational requirements who want to facilitate interoperability with FirstSecure components. Customers may integrate it with their applications to provide the ability to enroll for PKIX certificates via a PKIX End Entity client, and request other certificate types such as S/MIME and VPNs through browser-based enrollment. It supports the certificate lifecycle including certificate registration, enrollment, generation, revocation, and renewal.

The PKIX toolkit uses a PKIX-based certificate authority (CA) based on the IBM PKIX reference implementation. The CA includes features such as cross-certification, certificate hierarchies and user-defined certificate extensions. The CA requires IBM KeyWorks for cryptographic and key store function.

**SecureWay Directory Client Toolkit and Security Enabler:** This LDAP toolkit provides expanded capability to customize access to LDAP servers while providing cryptographic and security application support.

**SecureWay Policy Director Authorization API:** The Authorization API (aznAPI) is provided as a means of accessing Policy Director without having to incur full integration. Applications can then access the Policy Director in its environment and obtain services. This is a C level interface.

The aznAPI allows a user to build Policy Director security and authorization directly into customer corporate applications, helping reduce application development time and cost. By taking advantage of this, a network can be managed centrally by Policy Director, significantly reducing total cost of ownership and the likelihood of security breaches. The aznAPI gives access to an application-independent security and authorization framework avoiding having to write authorization code for each application.

**Year 2000**

These products are Year 2000 ready. When used in accordance with their associated documentation, they are capable of correctly processing, providing, and/or receiving date data within and between the twentieth and twenty-first centuries, provided that all products (for example, hardware, software, and firmware) used with the products properly exchange accurate date data with them. These solutions include third-party products. These third-parties have represented to IBM that their products are Year 2000 ready. However, IBM does not itself make any representations nor give any warranty as to the Year 2000 readiness of these product. Contact the appropriate third-party with any questions regarding the Year 2000 readiness of their product.

Information regarding non-IBM products and services are replications under the Information and Readiness Disclosure Act based on information supplied by other companies about the products and services they offer. IBM has not independently verified the contents of these replications and takes no responsibility for the accuracy of completeness of information contained in such replications.

The service end date for these Year 2000 ready products is November 30, 2001.

**Offering Information**

Product Information will be available on day of announcement through Offering Information (OITOOL) at:

http://www.ibm.com/wwoi

**Publications**

Hardcopy publications are available through Lotus Passport Advantage documentation packs. Visit the following URL to obtain the order number:

http://www.Lotus.com/passportadvantage

**Displayable Softcopy Publications:** Displayable publications are offered in softcopy form on the program CDs provided in the media package. Terms and conditions for use of the machine-readable files are shipped with the files.
Technical Information

Specified Operating Environment

Hardware Requirements: Products in the offerings are installed and tested on RISC System/6000® machines capable of running AIX® Version 4.3.2, Sun SPARC systems running Solaris 2.6, and/or Intel-based systems capable of running Microsoft® Windows NT™ 4.0. Review the README information provided with each component for the most current information.

Following are product specific requirements.

SecureWay Policy Director

System Requirements

- Platforms supported:
  - RISC System 6000
  - Sun SPARC
  - Intel x86 or Pentium™
- Operating systems:
  - AIX 4.3.2 and later
  - Solaris 2.6
  - Windows NT 4.0
- Client platforms:
  - Windows™ 95/98
  - Windows NT
- Disk Space: 50 MB
- Memory: 64 MB

SecureWay Boundary Server

SecureWay Firewall Version 4.1

System Requirements

AIX

- A RS/6000® including SMP models
- 128 MB memory on AIX

Microsoft Windows NT

- A single, dual, or four-processor Intel Pentium 266 MHz, or faster, system
- Minimum 64 MB memory

For either operating system, approximately 180 MB of free disk space is required for the following:

- 90 MB for the base Firewall, Netscape Communicator, Report Utilities, and operating system patches
- 50 MB for log files

Depending on how you configure your Firewall, your storage needs for logs will vary. For example, if you record little data in the log file, you might need as little as 1 MB of log storage per day. If you implement a full Socks Firewall, you could need as much as 30 MB per day for log files. Assuming you want to keep seven days worth of logs, this would require 210 MB of disk space for logs.

- A CD-ROM drive for product installation.
- Peripheral devices:
  - Mouse, trackball, trackpoint, or pen. Not all GUI functions can be performed with the keyboard; a pointing device is required.

- At least two network adapters
  - One Adapter connects the secure, internal network that the firewall protects.
  - The other network adapter connects the non-secure, outside network or Internet
- Adapters
  - All adapters supported by NDIS, including Token Ring and Ethernet (NT only)
  - X.25, ATM, FDDI, Token Ring, and Ethernet or S/390 (AIX Only)
  - These adapters must be supported by the TCP/IP protocol stack.
- IBM modem or Hayes compatible for pager support
  - Supported pager (TAP protocol)

Security Dynamics ACE_Server

System Requirements

- Platforms: Intel, Windows NT, Sun Solaris, IBM AIX, HP-UX
- Agents: IBM AIX, Windows NT, Digital UNIX®, Netscape servers, Apple ARA, Novell Netware Connect, Open VMS, SCO, SGI IRIX, SunSO/Solaris TCACS4, UNIX
- Disk requirements: 50 MB for primary server software 22 MB for backup server 4 MB for initial user database 240 MB for installation actual storage requirements based on user population

MIMEsweeper for IBM SecureWay FirstSecure Release 2

System Requirements

WEBsweeper

- Windows NT 4.0
- Pentium 400 processor and above
- 128 MB RAM + 1 MB for each concurrent web connection
- 1 GB of free disk space
- 1 NIC

MAILsweeper

- Windows NT 4.0
- Pentium 400 processor and above
- 128 MB RAM
- 1 GB of free disk space
- 1 NIC

SurfinGate 4.05

System Requirements

SurfinGate Server

- Pentium 233 processor and above
- 256 MB RAM
- 20 MB of free disk space
- Windows network client for Microsoft Windows

SurfinConsole

- Pentium 233 processor and above
- 64 MB RAM
- Windows NT 4.x
- 15 MB of free disk space
- Windows network client for Microsoft Windows
Intrusion Immunity

Tivoli Cross-Site for Security Version 1.1: Software requirements: AIX 4.3.2 or Solaris 2.7 or Windows NT 4.0

System Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Memory in MB</th>
<th>Recommended Memory in MB</th>
<th>DASD in MB</th>
<th>Windows NT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum</td>
<td>AIX</td>
<td>Solaris</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Agent</td>
<td>64</td>
<td>128</td>
<td>10</td>
<td>12</td>
</tr>
<tr>
<td>Server</td>
<td>128</td>
<td>256</td>
<td>275</td>
<td>305</td>
</tr>
<tr>
<td>Console</td>
<td>64</td>
<td>128</td>
<td>20</td>
<td>27</td>
</tr>
</tbody>
</table>

Public Key Infrastructure

SecureWay Trust Authority Version 3.1: SecureWay Trust Authority Version 3.1 can be installed on:

- RS/6000 systems (minimum 233 MHz, 256 MB RAM, 9.1 GB disk space) with AIX Version 4.3.2, or later
- Intel-based systems (minimum 450 MHz, 256 MB RAM, 9.1 GB disk space) with Microsoft Windows NT 4.0 (with Service Pack 5)

SecureWay Trust Authority Version 3.1 also requires the following products which are included in the Trust Authority media pack:

- DB2® Version 5.2 Fix Pack 10 (Enterprise Edition)
- WebSphere™ Application Server Version 2.03 Standard Edition including IBM HTTP Web Server Version 1.3.3. and JDK Version 1.1.6

Compatibility: Security authentication Devices — You can use IBM Firewall V4.1 with the following security devices to provide remote authentication of your users:

- Security Dynamics SecurID card
  - Model SD200
  - PINPAD

Limitations: The SecureWay Trust Authority Version 3.1 is included in the FirstSecure offering and is also offered as a separately orderable product.

The Trust Authority Version 3.1 product is a new entry level PKI Offering, and not the next release of the IBM Vault Registry product available as an option with FirstSecure Release 1.

IBM Vault Registry will interoperate with FirstSecure Release 2 in the same manner as it did in Release 1.

Customers who purchased the IBM Vault Registry as offered in SecureWay FirstSecure Version 1 should refer to Software Announcement 299-317, dated October 26, 1999, for additional information about IBM Vault Registry.

Planning Information

Packaging

SecureWay FirstSecure Media Pack
- International Program License Agreement
- License Information book

SecureWay FirstSecure Planning and Integration
- International Program License Agreement
- License Information book
- Program CDs
- Year 2000 flyer

SecureWay FirstSecure Documentation Pack
- International Program License Agreement
- License Information book
- Program CDs
- Year 2000 flyer

Ordering Information

The SecureWay offerings in this announcement are available only through Lotus® Passport Advantage.

The 128-bit DES encryption library and key recovery function for SecureWay Firewall Version 4.1 included in the FirstSecure and Boundary Server are not included in the SecureWay FirstSecure or SecureWay Boundary Server media package. Instructions to obtain these functions via download from a secured Web site are provided in the FirstSecure or Boundary Server media package.

The SecureWay Toolbox software is not included in the FirstSecure Media Package. The FirstSecure Media Package includes a card with instructions to obtain the Toolbox via download from a secured Web site.

The charge structure for the SecureWay FirstSecure, Policy Director, Boundary Server, and Trust Authority is Registered User based.

A Registered User is a person. Each person (Registered User) who accesses or uses any
The combination of clients or servers that are part of the offering, is counted as a Registered User.

- The Registered User authorization is offering specific. If you purchase more than one offering, you must purchase a Registered User authorization for each offering a Registered User (person) will use.
- The deliverables associated with the order for each offering are Proofs of Entitlement (POEs) only.
- The media and documentation must be acquired by ordering the media and documentation packs for each offering and are available through Lotus Passport Advantage.
- Each Registered User PoE acquired entitles the user to access a combination of servers and clients within and between any of the products included in the offering for which the proof of entitlement is acquired, as specifically stated in the License Information book included in the media package.

**Passport Advantage**

<table>
<thead>
<tr>
<th>Description</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Volume Purchase Option</strong></td>
<td></td>
</tr>
<tr>
<td>Instl IBM SecureWay FirstSecure</td>
<td>D26IHLML</td>
</tr>
<tr>
<td>Instl IBM SecureWay FirstSecure</td>
<td>1 ins</td>
</tr>
<tr>
<td>Instl SW Sub IBM SecureWay FirstSecure</td>
<td>D26ILML</td>
</tr>
<tr>
<td>Instl SW Sub IBM SecureWay FirstSecure</td>
<td>1 ins 1 Year</td>
</tr>
<tr>
<td>Instl SW Sub IBM SecureWay FirstSecure</td>
<td>D26IRML</td>
</tr>
<tr>
<td>Instl SW Sub IBM SecureWay FirstSecure</td>
<td>1 ins 2 Years</td>
</tr>
<tr>
<td>SW Sub Rnwl IBM SecureWay FirstSecure</td>
<td>E16J3ML</td>
</tr>
<tr>
<td>SW Sub IBM SecureWay FirstSecure</td>
<td>1 ins</td>
</tr>
<tr>
<td>SW Sub IBM SecureWay FirstSecure</td>
<td>D26J1ML</td>
</tr>
<tr>
<td>SW Sub IBM SecureWay FirstSecure</td>
<td>1 ins 1 Year</td>
</tr>
<tr>
<td>SW Sub IBM SecureWay FirstSecure</td>
<td>D26J2ML</td>
</tr>
<tr>
<td>SW Sub IBM SecureWay FirstSecure</td>
<td>1 ins 2 Years</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contract Option</strong></td>
</tr>
<tr>
<td>Instl/SW Sub IBM SecureWay FirstSecure</td>
</tr>
<tr>
<td>Instl/SW Sub IBM SecureWay FirstSecure</td>
</tr>
<tr>
<td>Instl/SW Sub IBM SecureWay FirstSecure</td>
</tr>
<tr>
<td>Instl/SW Sub IBM SecureWay FirstSecure</td>
</tr>
<tr>
<td>SW Sub Rnwl IBM SecureWay FirstSecure</td>
</tr>
<tr>
<td>SW Sub IBM SecureWay FirstSecure</td>
</tr>
<tr>
<td>SW Sub IBM SecureWay FirstSecure</td>
</tr>
<tr>
<td>SW Sub IBM SecureWay FirstSecure</td>
</tr>
<tr>
<td>SW Sub IBM SecureWay FirstSecure</td>
</tr>
<tr>
<td>SW Sub IBM SecureWay FirstSecure</td>
</tr>
<tr>
<td>Supt IBM SecureWay FirstSecure Flat</td>
</tr>
<tr>
<td>Supt IBM SecureWay FirstSecure Flat</td>
</tr>
<tr>
<td>Supt IBM SecureWay FirstSecure Flat</td>
</tr>
<tr>
<td>Supt IBM SecureWay FirstSecure Flat</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Volume Purchase Option</strong></td>
<td></td>
</tr>
<tr>
<td>Instl SecureWay Policy Director</td>
<td>D275KML</td>
</tr>
<tr>
<td>Instl SecureWay Policy Director</td>
<td>1 ins</td>
</tr>
<tr>
<td>Instl SW Sub SecureWay Policy Director</td>
<td>D275LML</td>
</tr>
<tr>
<td>Instl SW Sub SecureWay Policy Director</td>
<td>1 ins 1 Year</td>
</tr>
<tr>
<td>Instl SW Sub SecureWay Policy Director</td>
<td>D275ML</td>
</tr>
<tr>
<td>Instl SW Sub SecureWay Policy Director</td>
<td>1 ins 2 Years</td>
</tr>
<tr>
<td>SW Sub Rnwl SecureWay Policy Director</td>
<td>E176KML</td>
</tr>
<tr>
<td>SW Sub SecureWay Policy Director</td>
<td>1 ins</td>
</tr>
<tr>
<td>SW Sub SecureWay Policy Director</td>
<td>D2764ML</td>
</tr>
<tr>
<td>SW Sub SecureWay Policy Director</td>
<td>1 ins 1 Year</td>
</tr>
<tr>
<td>SW Sub SecureWay Policy Director</td>
<td>D2765ML</td>
</tr>
<tr>
<td>SW Sub SecureWay Policy Director</td>
<td>1 ins 2 Years</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contract Option</strong></td>
<td></td>
</tr>
<tr>
<td>Instl/SW Sub SecureWay Policy Director</td>
<td>D276PML</td>
</tr>
<tr>
<td>Instl/SW Sub SecureWay Policy Director</td>
<td>1 ins</td>
</tr>
<tr>
<td>Instl/SW Sub SecureWay Policy Director</td>
<td>D276RML</td>
</tr>
<tr>
<td>Instl/SW Sub SecureWay Policy Director</td>
<td>1 ins 2nd Anniv</td>
</tr>
<tr>
<td>SW Sub Rnwl SecureWay Policy Director</td>
<td>E176MUL</td>
</tr>
<tr>
<td>SW Sub SecureWay Policy Director</td>
<td>1 ins</td>
</tr>
<tr>
<td>SW Sub SecureWay Policy Director</td>
<td>D278BML</td>
</tr>
<tr>
<td>SW Sub SecureWay Policy Director</td>
<td>1 ins 1st Anniv</td>
</tr>
<tr>
<td>SW Sub SecureWay Policy Director</td>
<td>D278MML</td>
</tr>
<tr>
<td>SW Sub SecureWay Policy Director</td>
<td>1 ins 2nd Anniv</td>
</tr>
<tr>
<td>Supt SecureWay Policy Director Flat</td>
<td>AR7Y1ML</td>
</tr>
<tr>
<td>Supt SecureWay Policy Director Flat</td>
<td>1st Anniv</td>
</tr>
<tr>
<td>Supt SecureWay Policy Director Flat</td>
<td>AR63UML</td>
</tr>
<tr>
<td>Supt SecureWay Policy Director Flat</td>
<td>2nd Anniv</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Volume Purchase Option</strong></td>
<td></td>
</tr>
<tr>
<td>Instl SecureWay Boundary Server</td>
<td>D27XBML</td>
</tr>
<tr>
<td>Instl SecureWay Boundary Server</td>
<td>1 ins</td>
</tr>
<tr>
<td>Instl/SW Sub SecureWay Boundary Server</td>
<td>D27XDM</td>
</tr>
<tr>
<td>Instl/SW Sub SecureWay Boundary Server</td>
<td>1 ins 1st Anniv</td>
</tr>
<tr>
<td>Instl/SW Sub SecureWay Boundary Server</td>
<td>D27XEM</td>
</tr>
<tr>
<td>Instl/SW Sub SecureWay Boundary Server</td>
<td>1 ins 2 Years</td>
</tr>
<tr>
<td>SW Sub Rnwl SecureWay Boundary Server</td>
<td>E160NML</td>
</tr>
<tr>
<td>SW Sub SecureWay Boundary Server</td>
<td>1 ins</td>
</tr>
<tr>
<td>SW Sub SecureWay Boundary Server</td>
<td>D27Y2ML</td>
</tr>
<tr>
<td>SW Sub SecureWay Boundary Server</td>
<td>1 ins 1 Year</td>
</tr>
<tr>
<td>SW Sub SecureWay Boundary Server</td>
<td>D27Y4ML</td>
</tr>
<tr>
<td>SW Sub SecureWay Boundary Server</td>
<td>1 ins 2 Years</td>
</tr>
<tr>
<td>SW Sub SecureWay Boundary Server</td>
<td>E176FML</td>
</tr>
<tr>
<td>SW Sub SecureWay Boundary Server</td>
<td>1 ins 1st Anniv</td>
</tr>
<tr>
<td>SW Sub SecureWay Boundary Server</td>
<td>D27Y6ML</td>
</tr>
<tr>
<td>SW Sub SecureWay Boundary Server</td>
<td>1 ins 2nd Anniv</td>
</tr>
<tr>
<td>SW Sub SecureWay Boundary Server</td>
<td>D27Y7ML</td>
</tr>
<tr>
<td>Supt SecureWay Boundary Server Flat</td>
<td>AR63WML</td>
</tr>
<tr>
<td>Supt SecureWay Boundary Server Flat</td>
<td>1st Anniv</td>
</tr>
<tr>
<td>Supt SecureWay Boundary Server Flat</td>
<td>AR63MML</td>
</tr>
<tr>
<td>Supt SecureWay Boundary Server Flat</td>
<td>2nd Anniv</td>
</tr>
<tr>
<td>FirstSecure Version 2 Strong Media</td>
<td>BE68MNA</td>
</tr>
<tr>
<td>FirstSecure Version 2 Documentation</td>
<td>BE6SNA</td>
</tr>
<tr>
<td>Policy Director V2 Strong Media</td>
<td>BE607NA</td>
</tr>
<tr>
<td>Policy Director V2 Documentation</td>
<td>BE6AUNA</td>
</tr>
<tr>
<td>SecureWay Boundary Server V2 Strong Media</td>
<td>BE6T5NA</td>
</tr>
<tr>
<td>SecureWay Boundary Server V2 Documentation</td>
<td>BE6T7NA</td>
</tr>
</tbody>
</table>

-9- 299-326
The Server Components are:

- SecureWay Firewall server
- MIMEsweeper product
- SurfinGate product
- Policy Director Server. Policy Director server Components are:
  - SecureWay Authorization Server
  - SecureWay Key Work Management Console Server
  - SecureWay Key Work Authorization Server
  - SecureWay Key Work DCE Security Directory Server
- SecureWay Key Work Trust Authority
- WebSphere
- DB2 Universal Database® Enterprise Edition
- Tivoli Cross-Site for Security Server
- Tivoli Cross-Site for Security Agent

The Client Components are:

- Symantec Norton AntiVirus
- NetSeal Client
- Tivoli Cross-Site for Security agent
- DCE Client

The Toolbox Components are:

- KeyWorks Toolkit
- Key Recovery Service Provider Toolkit
- Key Recovery Server Version 1.1.3
- SecureWay Policy Director Authorization API
- Secure Sockets Layer (SSL) Toolkit
- Public Key Infrastructure for X.509 (PKIX) Toolkit
- SecureWay Directory Client and Security Enabler

Authorized Use of the Program is based on the number of Registered User Authorizations acquired. For each Registered User Authorization you acquire, you receive one Client PoE.

Server PoE are based on the number of Registered User Authorizations you acquire:

With the purchase of your initial 500 Registered User Authorizations, you receive one Server PoE for each server Component:

For each subsequent purchase of a total of 500 Registered User Authorizations, you will receive an additional one Server PoE for each server Component.

Toolbox PoE are based on the number of Registered User Authorizations you acquire:

With the purchase of your initial 500 Registered User Authorizations, you receive four Toolbox PoE.

Subsequent purchase of additional Registered User Authorization does not entitle to you install additional copies. If you require the ability to make and use additional copies, contact your IBM representative.

You may NOT combine Registered User Authorizations for Program with Registered User Authorizations for other SecureWay products.

Terms Applicable to all Program Components: This Agreement governs the use and support of the Program with the exception of Components of the Program which contain their own license agreements. The terms and conditions governing such Components are provided when installing or starting such specific Components.

The Program contains encryption technology that is subject to special export licensing requirements by the U.S. Department of Commerce. It may also be subject to export and import requirements of other countries. IF YOU DISTRIBUTE ANY COMPONENTS OF THIS PROGRAM, YOU MUST ABIDE BY ALL APPLICABLE LAWS, RULES AND REGULATIONS REGARDING THE EXPORT OF SUCH CODE. FURTHER, YOU MUST ENSURE THAT ALL USERS WHO RECEIVE THE PROGRAM FROM YOU COMPLY WITH THE TERMS OF THIS AGREEMENT

If you purchase a license or PoE for a Component of the Program separately from the Program (“Separate Product”), the use of such Separate Product is governed by the license terms associated with such Separate Product and not this Agreement. However, you may use the Program in association with such Separate Product.

Terms Applicable for each Valid Server PoE: Except as set forth below for Policy Director and Trust Authority, you may install and use one copy of your choice of the operating system version of each Server Component of the Program but, you may not install more than one copy of any Server Component. You may install the authorized number of Server Components on different machines (for example, install SecureWay Firewall for AIX on machine 1 and install SurfinGate Server on machine 2).

Terms Applicable for each Valid Client PoE: You may install and use one copy of each Client Component of the Program on a machine or machines for a single user.

You may install your choice of the operating system version of each such Component provided that you may not install more than one copy of any Client Component. While you do not have to install or use every Component, you may not install the Components on different machines for different users under a single Client PoE (for example, you may not install the IBM SecureWay Firewall client on a machine for User A but install the Norton AntiVirus client on a different machine for User B). You must acquire a separate Client PoE for each user who will use any client Component.

Terms Applicable for each Valid Toolbox PoE: Support for the Toolbox is limited solely to bug fixes. Under a separate services agreement from IBM, you can obtain:

1. Systems engineering
2. Design
3. Technical implementation and integration support
   (to include programming guidance). Determination of what constitutes a bug-fix versus other support is solely at the discretion of IBM.

You may integrate the Toolbox, or portions thereof, with applications and/or middleware and distribute the resulting server and/or client runtime products (each referred to as a “Program Derivative”) solely to your Registered Users of the Program.
You may allow only individuals for whom Registered User Authorizations have been acquired to access and use the services of these Servers.

Terms applicable to MIMEsweeper product:

- You may allow only individuals for whom Registered User Authorizations have been acquired to access and use the services of these Servers.

Terms applicable to Policy Director Server Components:

- You may allow only individuals for whom Registered User Authorizations have been acquired to access and use the services of these Servers.

For each valid Server PoE, you may install one DCE Security and Directory Server, one SecureWay Directory Server, and any six copies of the other Policy Director Server Components, in any combination. For example, in addition to the DCE Security and Directory Server and the SecureWay Directory Server, for the remaining six of the other Policy Director Server Components, you may install one copy of each Component (not including the IBM DCE Security and Directory Server or the SecureWay Directory), or two copies of the Console Server, and four copies of the WebSeal Server, or any other combination of Policy Director Server Components (not including the DCE Security and Directory Server or SecureWay Directory) adding up to six that meets your business needs.

- You may only use the DB2 UDB Component in association with your licensed use of the SecureWay Directory.

Terms applicable to the DCE Client:

- The DCE Client can only be used to access IBM Policy Director Server Components.

Terms applicable to Norton AntiVirus:

While several different antivirus clients are provided (for example, Norton AntiVirus/IBM Solution for Windows 95/NT Workstations and Norton AntiVirus/IBM Solution for Lotus Notes®), you may install one copy of your choice of only one of the Norton AntiVirus Components. SecureWay Trust Authority

Terms applicable to Tivoli Cross-Site for Security agent:

For the first 500 Registered User Authorizations you acquire, you may install five Tivoli Cross-Site for Security agents. For each subsequent 500 Registered User Authorizations you acquire, you may install ten additional Tivoli Cross-Site for Security agents.

Terms applicable to SecureWay Trust Authority:

You may issue and manage as many certificates as you require solely for individuals for whom Registered User Authorizations have been acquired. You may not issue or manage certificates for individuals other than Registered Users.

You are responsible for acquiring all of the prerequisite products required in order to use the Trust Authority. Except as otherwise set forth herein, you may make as many copies of the Trust Authority as is necessary to support the number of Registered Users Authorizations you have acquired.

You understand and agree that the Trust Authority contains data encryption functions which are subject to special export licensing restrictions by the U.S. Department of Commerce.

You understand and agree that the Trust Authority contains software from RSA Data Security, Inc. (RSA Code). You may modify or directly access the RSA Code or its functions, except through the function calls of the Program, which may not be modified. In addition, the Program contains Standard Template Library software ("STL Software") from Silicon Graphics Computer Systems, Inc. ("SG STL Software") and Hewlitt-Packard Company ("HP STL Software"). SG STL Software is copyright “1996-1999 Silicon Graphics Computer Systems, Inc. and HP STL Software is copyright” 1994 Hewlitt-Packard Company. STL Software may be found on the Web at:

http://wwwsgi.com/Technology/STL

and other places. Permission to use, copy, modify, distribute, and sell the SG STL Software and HP STL Software and their documentation for any purpose is
The Trust Authority includes portions of DB2 Universal Database software ("DB2 Components"). You are not authorized to install or use the DB2 Components other than in connection with your licensed use of the Trust Authority for the storage and management of data used or generated by the Trust Authority. For example, this license does not include inbound connections to the database or the DB2 Components from other applications for queries or report generation. The DB2 Components must reside on the same machine as the Trust Authority, and you are not authorized to install or use the DB2 Components separate from the Trust Authority.

The Trust Authority includes portions of the WebSphere Application Server and the IBM HTTP Web Server ("IBM Servers"). You are not authorized to install or use the IBM Servers other than in connection with your licensed use of the Program. The IBM Servers must reside on the same machine as the Program, and you are not authorized to install or use the IBM Servers separate from the Trust Authority.

You may not take any action, or permit any omissions, with respect to the Trust Authority that would exceed the license rights granted in the Agreement and these Program-unique Terms. Any other use of the Trust Authority is prohibited. You are responsible for maintaining the overall security of your systems, processes, and information.

The Trust Authority includes the following code modules (hereinafter referred to as “Modules”), which are installed into the customer-chosen destination path for the Trust Authority Registration Authority portion of the Trust Authority:

1. All configuration files (file extension .cfg) and letter templates (file extension .ltr) in the \etc directory
2. The policy_exit file in the \bin directory
3. All files in the \webpages directory

You may copy and modify the Modules only for the purpose of customizing hypertext markup language ("HTML") screens, Java™ Server Pages, graphics, policy exits, configuration files, and sample letters in connection with your own applications which you create for use with the Program. You may not distribute or otherwise copy or modify the Modules.

IBM shall have no liability to you or your customers or end users for your or their use of the Trust Authority, and you agree to indemnify, defend, and hold IBM and its subsidiaries and suppliers harmless from and against any claims (actual or alleged) that are based on or arise in connection with:

1. Your use of the Trust Authority
2. Any of your customers or end users use of or interaction with the Trust Authority
3. Any use of or reliance upon any digital certificates issued by you using or in connection with the Trust Authority

4. Any representations made by you about the Trust Authority, provided that IBM:
   - Promptly notifies you in writing of such claim
   - Allows you to control, and cooperates with you in the defense and any related settlement negotiations.

IBM shall have the right to participate in such claim at its own expense.

Terms applicable to Tivoli Cross-Site for Security: The following definitions apply to the Tivoli Cross-Site for Security Product and this agreement:

Channel Master: You (FirstSecure Customer)
Trading Partners: Third parties engaged in business with You Management Server
Security Server Agent: Tivoli Cross-Site for Security Agent

For the first 500 Registered User Authorizations you acquire, you may install five (5) Tivoli Cross-Site for Security Agents. For each subsequent 500 Registered User Authorizations you acquire, you may install ten (10) additional Tivoli Cross-Site for Security Agents.

Encryption and Authentication: The Management Server and Agent contain cryptographic or authentication features. Channel Master understands and agrees that Channel Master must separately obtain a signed digital certificate from a certificate authority or a certificate server in order to utilize the cryptographic or authentication features. Channel Master may be charged additional fees for certification services. Following successful installation of a digital certificate, Channel Master’s use of the Programs’ cryptographic or authentication features will be enabled. Channel Master is responsible for maintaining the security of the environment in which the Programs are used and the integrity of the private key file used with the Programs. In addition, the use of digital certificates is subject to the terms specified by the certificate provider, and there are inherent limitations in the capabilities of digital certificates. If Channel Master is sending or receiving digital certificates, Channel Master is responsible for familiarizing itself with and evaluating such terms and limitations. Subject to this Agreement, each authorized copy of the Management Server may be installed and used on one of Channel Master’s or Trading Partners’ premises to support Agents for which Channel Master has acquired an Application Client hereunder.

Agents may display an End-User license upon installation. Use of the Agents is governed by these terms and the terms in the accompanying end-user License. A copy is provided below for your review.

Subject to the following terms, Channel Master may transfer copies of the Management Server or Agent for which Channel Master has acquired the requisite authorization to Trading Partners.

Prior to any such transfer, Channel Master must execute a written license agreement with such Trading Partner which contains provisions materially equivalent to the terms contained herein. Channel Master shall be responsible for compliance by the user of the Management Server with the terms of the license. Trading Partners may not distribute either the Application Management Server to any other party. Despite any terms in this Agreement or the Agent End-User license to the contrary, a Trading Partner may utilize Agents provided to it by Channel Master solely to interface with
the Management Servers which are (1) operated by such Channel Master or (2) provided to the Trading Partners by such Channel Master.

Neither Channel Master nor Trading Partner may install or use Agents or Management Servers for which the appropriate authorization has not been acquired.

Cross-Site End User License Agreement

IMPORTANT — READ CAREFULLY.

BY CLICKING ACCEPT OR INSTALLING THE SOFTWARE, YOU ARE AGREING TO ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. LICENSOR IS WILLING TO MAKE THE SOFTWARE AVAILABLE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK DECLINE AND THE INSTALLATION PROCESS WILL NOT CONTINUE. IF YOU CLICK DECLINE, CONTACT LICENSOR FOR REFUND INFORMATION (IF APPLICABLE).

IF YOU RECEIVED THE SOFTWARE PURSUANT TO A SIGNED PRINTED LICENSE AGREEMENT AND THE TERMS OF THAT AGREEMENT VARY FROM THIS AGREEMENT, THEN THE PRINTED AGREEMENT GOVERNS YOUR USE OF THE SOFTWARE.

IF YOU RECEIVED THE SOFTWARE FOR EVALUATION PURPOSES, THEN THE STATED EVALUATION PERIOD IS 60 DAYS, AND ANY USE OF THE SOFTWARE AFTER THE END OF THE EVALUATION PERIOD WITHOUT PURCHASE OF A LICENSE IS STRICTLY PROHIBITED.

This Cross-Site End User License Agreement (Agreement) is between you (either an individual or entity) (Licensee) and Tivoli Systems, Inc. (licensor). This Agreement applies to the object code copy of the Cross-Site software which Licensee has elected to install (Software), together with any related documentation provided by Licensor (Documentation). The Software and Documentation are referred to collectively herein as Software. GRANT OF LICENSE: Licensee is permitted to use the Cross-Site Programs to deploy and manage applications or other data for use by one user on one server or endpoint computer for which the appropriate license has been purchased.

RESTRICTIONS. Unless otherwise specified in the Grant of License (Section 1), Licensee may not copy the Software except for one copy made solely for back-up purposes. To the extent copying is permitted, Licensee must include the copyright notice and any other notices that appear on the original Software on any copies and any media therefor. Licensee shall not (and shall not allow any third party to) (i) decompile, disassemble, or otherwise reverse engineer the Software (except solely to the extent that applicable law prohibits reverse engineering restrictions) or attempt to reconstruct or discover any source code, underlying ideas, algorithms, file formats or programming interfaces of the Software by any means whatsoever, (ii) remove any product identification, proprietary, copyright or other notices, (iii) provide, lease, lend, grant a security interest in, use for timesharing, hosting or service bureau purposes or otherwise transfer or use or allow others to transfer or use the Software to or for the benefit of third parties, (iv) modify, translate, incorporate into or with other software or create a derivative work of any part of the Software, or (v) disseminate performance information or analysis (including, without limitation, benchmarks) from any source relating to the Software. Licensee acknowledges that the Software is not designed or licensed for use in hazardous or high risk environments such as operation of nuclear facilities, direct life support, air or space travel or police, rescue or military operations and Licensor shall have no liability in connection with any use of the Software in such situations.

Title: Notwithstanding anything to the contrary herein, Tivoli Systems, Inc. and/or its licensors or suppliers, retains all title to, and, except as expressly and unambiguously licensed herein, all rights to the Software, all copies and derivative works thereof (by whomever produced) and all related documentation and materials.

Warranty Through Program Services: Yes, except for the Sun Solaris JRE provided from IBM as a Component of the Policy Director Server.

Limited Warranty Applies: Yes

Program Services: Available until November 30, 2001

Money-back Guarantee: Two-month, money-back guarantee

Copy and Use on Home/Portable Computer: No

Volume Orders (IVO): Yes, contact your IBM representative

Passport Advantage Applies: Yes

Passport Advantage Subscription Applies: Yes

Support Line: No

AIX/UNIX Upgrade Protection Applies: No

Entitled Upgrade for Current AIX/UNIX Upgrade Protection Licensees: No

AS/400® Software Subscription Applies: No

Variable Charges Apply: No Note to the Field Communications Editor: Do not include/publish prices on Internet

Charges

Passport Advantage

Note: For Passport Advantage and charges, contact your IBM Lotus representative or authorized IBM Lotus Business Partner. Additional information is also available on the Passport Advantage URL: http://www.lotus.com/passportadvantage

Customer Financing: IBM Global Financing offers attractive financing to credit-qualified commercial and government customers and Business Partners in more than 40 countries around the world. IBM Global Financing is provided by the IBM Credit Corporation in the United States. Offerings, rates, terms and availability may vary by country. Contact your local IBM Global Financing organization. Country organizations are listed on the Web at:

Call Now to Order

Contact the IBM Americas Call Centers (to help IBM serve you, use the Reference Code):

Phone:  800-IBM-CALL
Fax:    800-2IBM-FAX
Internet:  ibm_direct@vnet.ibm.com
Mail:  IBM Americas Call Centers
       Dept. YE001
       P.O. Box 2690
       Atlanta, GA 30301-2690
Reference Code: YE001

You can also contact your local IBM Business Partner or IBM representative. To identify them, call 800-IBM-4YOU.

Note: Shipments will begin after the planned availability date.

IBM Americas Call Centers, our national direct marketing organization, can add your name to the mailing list for catalogs of IBM products.

Trademarks

SecureWay and WebSphere are trademarks of International Business Machines Corporation in the United States or other countries or both.
RISC System/6000, AIX, RS/6000, DB2, DB2 Universal Database, and AS/400 are registered trademarks of International Business Machines Corporation in the United States or other countries or both.
Pentium is a trademark of Intel Corporation.
Microsoft, Windows NT, and Windows are trademarks of Microsoft Corporation.
Java is a trademark of Sun Microsystems, Inc.
UNIX is a registered trademark in the United States and other countries exclusively through X/Open Company Limited.
Lotus Passport is a trademark of Lotus Development Corporation.
Lotus and Lotus Notes are registered trademarks of Lotus Development Corporation.
Other company, product, and service names may be trademarks or service marks of others.

Year 2000 Readiness Disclosure