Secure your e-business

IBM eNetwork Software solution for security and directory integration

June 1998

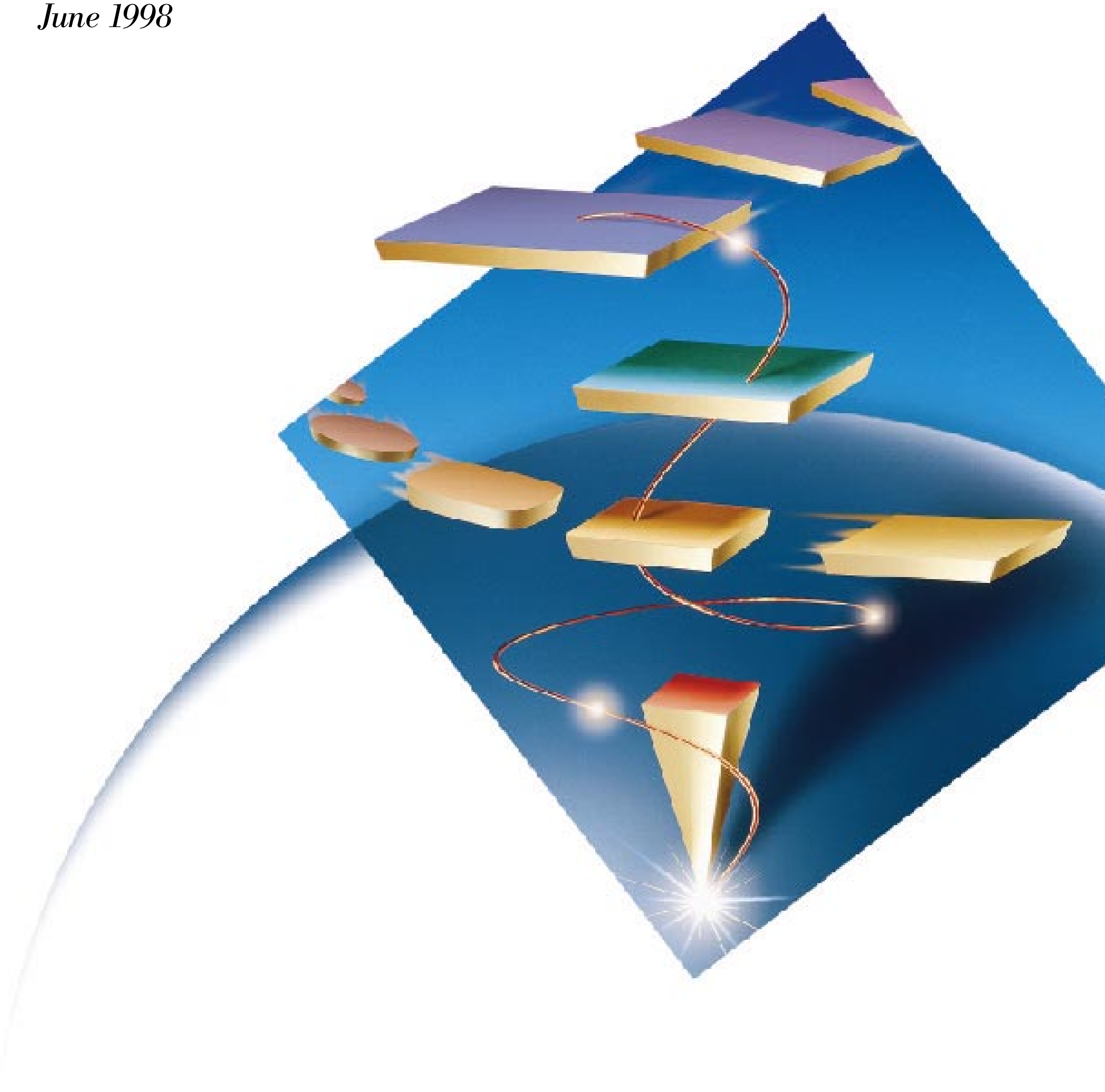


Table of contents

Introduction

This paper discusses strategy and plans which are subject to change due to IBM business and technical judgments. IBM eNetwork solution for security and directory integration:

- Is a comprehensive, integrated security solution
- Enables networks, systems, and applications with a cross-platform LDAP directory
- Extends your enterprise to the Internet with IBM security

The rise of the Internet and e-business

Nearly 30 years ago in the Fall of 1969, the Internet began by connecting two computers at UCLA and Stanford. A handful of University and business computer researchers were exploring "strategies for using the network and initial experiments with the network."[1] Efforts were documented using a curious strategy—Requests for Comments, or RFCs. Anyone could create notes for inclusion in the RFC series, because people involved with the Internet wanted to learn and experiment, not create tested, error-free networks for use by businesses. Indeed, their original philosophy was just the opposite! "These standards (or lack of them) are stated explicitly. We hope to promote the exchange and discussion of considerably less than authoritative ideas."[2]

This original philosophy continues and is partly responsible for the huge growth and success of the Internet, now connecting thousands of networks and millions of computers. The Internet grew by sharing information and techniques, with people enhancing and improving each others' work. New things were tried without worrying about marketplace success. Unfortunately, this sometimes delivered incomplete software, leading to exposures, such as the Morris Worm that brought down the Internet and SMTP e-mail software, which hackers use to penetrate systems.

Whether the Internet is designed for business or not, millions of e-businesses use it daily to extend the reach of their business and increase profits. In fact, some e-businesses exist only in cyberspace with dramatic online sales growth. According to Datamonitor, a London-based research firm, "Online purchases will soar to $16 billion in the United States and Europe in 2002, fueled by Internet-based card transactions. Last year's total was between $300 million and $500 million."[3]

[1] *Network Working Group RFC-3 April 1969, by Steve Crocker, UCLA*

[2] *ibid.*

[3] *American Banker Vol. 163, #27, February 10, 1998 Page 10*

eNetwork Software: The foundation for e-business

IBM® eNetwork™ Software helps many e-businesses, allowing any client and any user to securely access any data on any server. eNetwork Software delivers this capability through four solutions:

- Security and directory integration—providing a comprehensive integrated security solution and cross-platform Lightweight Directory Access Protocol (LDAP) directory
- Mobile enablement—providing more cost-effective wireline and wireless application access
- Server-managed client enablement—providing more cost-effective network communication and services for network-driven Java™ applications
- Host integration—providing more cost-effective host and LAN universal connectivity, information access, and network asset utilization

The remainder of this paper focuses on the security and directory integration solution, which addresses customers' universal need to protect assets from unauthorized access from both internal and external sources. This solution provides a scalable, manageable, and comprehensive security solution, based on a common directory service, addressing core security requirements for single sign-on, firewalls, virtual private networks (VPNs), authentication, encryption, AntiVirus services, and management. This is implemented through an integrated set of offerings, such as IBM Global Sign-On, eNetwork Firewall, KeyWorks security framework, and AntiVirus.

The what, why and how of directory

A directory service is just an information repository, an access method and related services. It stores detailed information about resources, such as users, printers, and file and application servers.

Although directory services have been used for decades, the explosion of distributed and Internet-based computing has resulted in multiple directory services throughout an organization. Resources are often defined in several directories—for e-mail systems, networks, systems, and applications. With a different repository, access protocol, and management interface for each directory, a maintenance nightmare exists in these organizations.

Despite obvious benefits of using a single, integrated directory, vendors have been reluctant to use such a service natively. Existing directories usually feature tight linkages to an application or operating system, so vendors prefer that customers build their computing environments around the vendor's directory service—the so-called center-of-the-universe mentality. This theoretically generates incremental revenues and locks the customer into using the vendor's directory service.

As a result, customers have a wide variety of directory services implemented in their businesses. This leads to wasted effort to define and consistently manage and maintain multiple definitions of resources—hence the strong demand for integrated management tools to synchronize resource definitions across directories, and to provide a single sign-on to the multiple directories.

Because customers demand flexibility due to today's fast-changing business climate, it is widely expected, even among proprietary Network Operating System (NOS) vendors, that heterogeneous networks will continue to be the rule for the foreseeable future. However, given the extensive pressure that customers are putting on vendors to solve the problems of incompatible directories within these heterogeneous networks, it is likely that most vendors will support a common access method, LDAP.

The what, why and how of security

Webster's New Collegiate Dictionary defines security as "measures taken to guard against espionage or sabotage, crime, attack or escape."[4] For information technology, a broader definition also includes measures to recover from security breaches. These methods include:

Authorization

Only fully identified and authenticated clients should be able to access enterprise networks, systems, and applications. Access control lists and data protection methods, such as encryption, maintain confidentiality and protect information technology.

Accountability

Users should be fully accountable for and unable to deny their actions. It should be possible to determine, through the system's accountability features, who performed any given action and which actions have taken place in a specified interval.

Availability

Networks, systems, and applications should be available for use when required, protected from breaches, but also discovering breaches and recovering from those breaches. This includes functions, such as antivirus mechanisms, and the ability to recover data and keys used for encryption in case of accidental loss or warranted legal request for inspection.

These security measures are designed to stop three kinds of threats: vandalism, espionage, and theft. Vandalism includes Web graffiti (rewriting Web pages), stopping others from using systems (service denial), flooding with spurious information (spamming), and spreading viruses across multiple resources. Espionage includes gathering information and close monitoring of activities to gain business intelligence. Theft is accomplished by many techniques, including social hacking (stealing passwords left on terminals or other social impersonations), brute force attacks to discover information or passwords, and pretending to be another system (spoofing).

While popular opinion attributes these security breaches to young hackers roaming the Internet, in reality, most security breaches come from within an organization. According to a survey conducted by the Computer Security Institute (an association of corporate data security officers) for the United States Federal Bureau of Investigation's International Computer Crime Squad, computer attacks by insiders were more common last year than external Internet-based attacks. More than 87 percent of the corporate, financial, government, and university information security managers polled said disgruntled employees were the most likely cause of data security incidents, ranging from sabotage, fraud, and theft of proprietary information to unauthorized snooping in a colleague's e-mail or the storing of digital pornography on a company computer.[5]

With attacks like these, it is not surprising that most organizations are spending more on security this year. To spend that money wisely, it is important to implement a security policy which starts with an organization's information technology assets and the risks and exposures for those assets. After assessing the risk, organizations must define, implement, and administer this policy. It is then important to audit security success against the policy. As situations change, this process of assessing risk, defining policy, implementing policy, administering policy, and auditing security must be updated to reflect the new environment.

Policies can include items, such as encrypting all communication among executive staff to prevent inadvertent eavesdropping. At one company, a technician diagnosing network problems read e-mail the CEO had sent to his vice presidents. As the word of the e-mail contents spread, corporate business plans had to be changed because of the lack of confidentiality. Other policies can include how often passwords are changed, or whether stronger forms of identification, such as token cards or fingerprint readings, are required to access especially sensitive systems.

[4] *Webster's New Collegiate Dictionary, page 1045, A Merriam-Webster, copyright 1975*

The paradox of the four I's

Research shows that organizations want security to be invincible, invisible, inexpensive, and integrated—attributes that at times represent conflicting capabilities. Invincible means that no one should be able to breach the security precautions that are in place. Invisible means that users should not know security is in place, unless they try to breach security, at which time it is not at all invisible! Inexpensive means that the organizational cost for implementing security should be low. Integrated means that systems work together and share information.

With multiple networks, systems, and applications deployed, organizations use many different security and directory mechanisms. This adds administrative cost and also makes it more visible to users. Achieving invincibility requires multiple security measures, and thus making it inexpensive represents a significant challenge. Integrating security and directory mechanisms will make them less visible and less expensive.

The challenge for vendors and for customers purchasing security and directory offerings is to select the right balance of the four I's to achieve the desired levels of cost and security.

IBM eNetwork Software security and directory integration

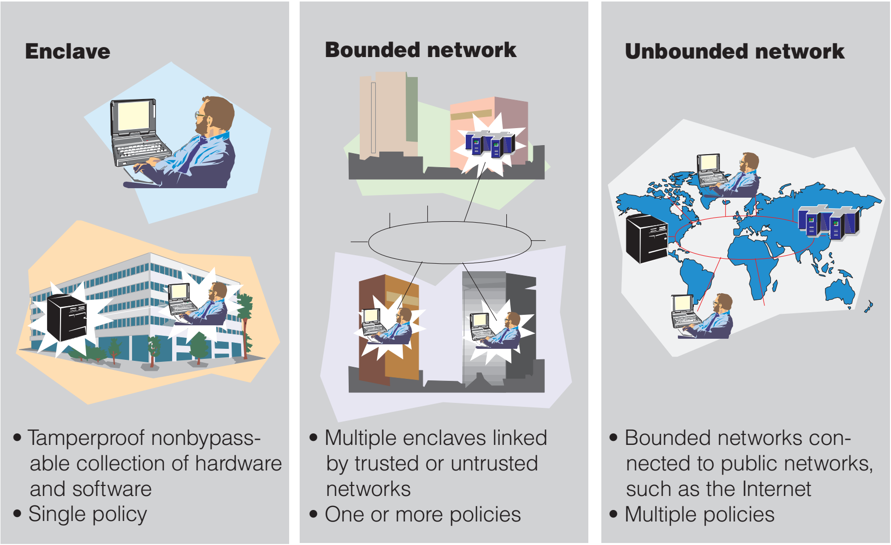
As the world's leading supplier of advanced information technologies, including computer systems, software, networking systems, storage devices, and microelectronics, IBM is uniquely positioned to offer a comprehensive security solution. IBM is linking together separate elements to create eNetwork Software solution for security and directory integration, allowing organizations to implement policies to secure information technology resources in even the most complex environments.

This solution allows customers to secure networks, systems, and applications by delivering effective authorization, accountability, and availability functions. To help customers understand how best to deploy this offering, IBM has leveraged years of security experience to develop a comprehensive security architecture.

[5] *Reported in The New York Times, Monday March 2, 1998 Section D; Pg. 1, Col. 2, Business/Financial Desk*

IBM security architecture

Over the last decade, information technology (IT) has evolved into a complex security environment, which is best understood by breaking it into smaller pieces. There are three different security domains: enclaves, bounded networks, and unbounded networks. Enclaves have a single security policy with invincible security. Put another way, an enclave is a tamperproof collection of hardware and software with a single security policy, which might be a single personal computer (PC). Bounded networks are multiple enclaves with one or more policies which are connected by trusted or untrusted networks. Unbounded networks have multiple policies and are connected to untrusted networks, such as the Internet.



Enclave

- Tamperproof nonbypassable collection of hardware and software
- Single policy

Bounded network

- Multiple enclaves linked by trusted or untrusted networks
- One or more policies

Unbounded network

- Bounded networks connected to public networks, such as the Internet
- Multiple policies

Security domains

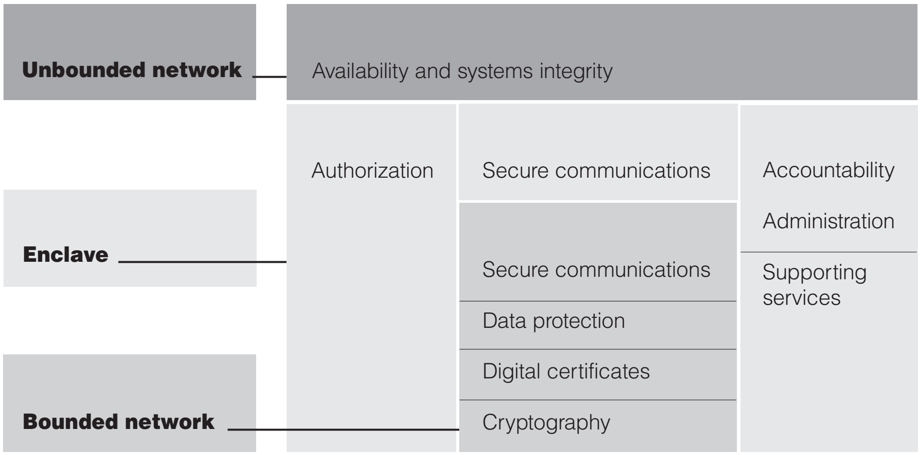
In simpler terms, consider an enclave as a single person, or a group of people that embodies the values of Robert Fulghum—"Share everything, Play fair, Don't take things that aren't yours."[6] A bounded network is like one or more groups of people who learned that "When you go out into the world, watch out for traffic, hold hands and stick together."[7] Finally, an unbounded network is more like groups of grown-ups who have decided to "trust, but cut the cards."

Different security products are required, depending on what type of security domain you are protecting. Enclaves require functions like the ability to log onto systems, administer policy, and securely communicate within the enclave. Encryption and public-key infrastructures are required for bounded networks. Unbounded networks require security functions to maintain availability and integrity of the systems to detect intrusion attempts and recover from security breaches.

[6] *All I really needed to know I learned in Kindergarten, Ballantine Books, 1986, by Robert Fulghum*

[7] *ibid.*

IBM security architecture



Unbounded network

Availability and systems integrity

Enclave

Authorization

Secure communications

Accountability

Administration

Secure communications

Supporting services

Data protection

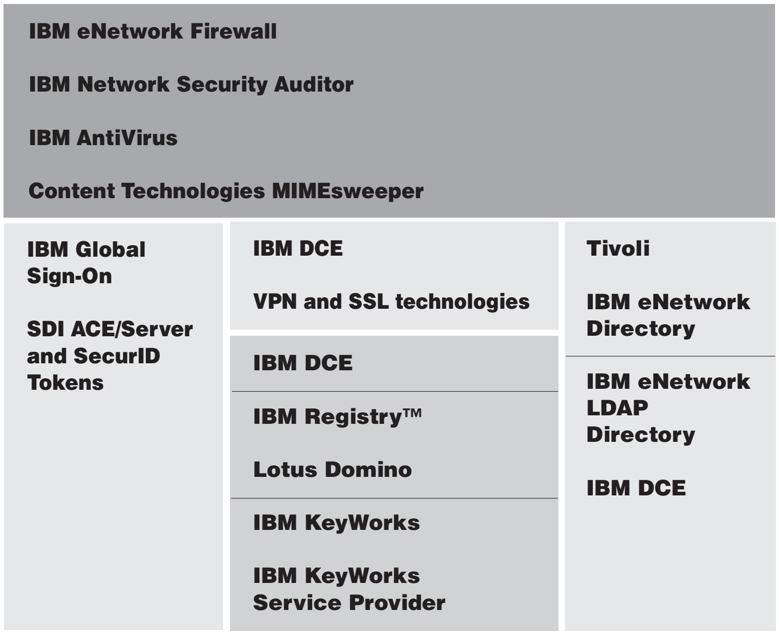
Digital certificates

Bounded network

Cryptography

IBM security architecture

IBM eNetwork Software security and directory integration solution offers complete security and directory functions covering all these security domains. IBM Global Sign-On and Security Dynamics SecurID enhance logon capabilities; IBM LDAP Directory, Tivoli®, and IBM DCE enable policy administration; and IBM DCE, VPN, and SSL capabilities allow the secure communication required in bounded networks. IBM eNetwork Firewall, IBM AntiVirus, Content Technologies MIMEsweeper, and IBM Network Security Auditor maintain availability for unbounded networks.



IBM eNetwork Firewall

IBM Network Security Auditor

IBM AntiVirus

Content Technologies MIMEsweeper

IBM Global Sign-On

SDI ACE/Server and SecurID Tokens

IBM DCE

VPN and SSL technologies

IBM DCE

IBM Registry™

Lotus Domino

IBM KeyWorks

IBM KeyWorks Service Provider

Tivoli

IBM eNetwork Directory

IBM eNetwork LDAP Directory

IBM DCE

IBM eNetwork Software security and directory integration

IBM directory strategy and offerings

The overall integration point of the IBM security architecture, and hence of security and directory integration, is the directory, because only through a common directory can customers address the proliferation of application-specific directory services, a major driver of high-cost security. IBM's strategy is to consolidate our directory offerings onto a standards-based LDAP directory service. In addition, IBM will directory-enable its offerings, reducing the administrative effort for maintenance and improving the data consistency across these offerings.

IBM's directory strategy has four principles:

1 *Directory enable IBM and ISV offerings*
Several IBM divisions and selected independent software vendors (ISVs) are exploiting the eNetwork LDAP Directory, because the customer benefits are multiplied as a common directory is exploited across operating systems, networks, and applications. IBM offerings will be able to use this LDAP directory to store user, configuration, and security information, reducing administrative costs and improving users' access to information.

For example, eNetwork Software offerings will store configuration information in the directory so each device can load information from a central directory service. Firewall will be able to store policy information in the directory, allowing rapid policy updates throughout the organization. As more offerings are directory-enabled, users can be given a high priority on both the transaction server and the network, improving response time. This is enabled by providing a common directory service leveraged by multiple components. As more products become directory-enabled, the possibilities for cross-product synergy become limitless.

2 *Provide a highly scalable cross-platform LDAP directory*
IBM will include the eNetwork LDAP Directory in operating systems and selected applications so directory users will have an LDAP directory available, helping drive the requisite LDAP exploitation. The directory repository is based on DATABASE 2™ (DB2®), IBM's industry-leading relational database, and provides a very scalable, high-performance directory service. The choice of a relational database-backing store provides unmatched levels of scalability and reliability for an LDAP directory, with current scalability for the eNetwork LDAP Directory at over four million entries.

3 *Provide LDAP support across our existing directories*
To provide consistent access for application developers and clients, IBM will support LDAP as the interoperability protocol across our existing directory servers, including the Domino™ Directory, DCE and X.500. This will provide organizations with a single API and protocol for IBM and Lotus®-based networks. Our direction is to allow the convergence of the DCE Cell Directory Service and application-specific information stored in unique side files into the eNetwork LDAP Directory. We are also working to further improve the operational characteristics of our LDAP support by providing a common schema across the IBM, Lotus, and Tivoli directories. We are working with the Desktop Management Taskforce (DMTF) so our schema will be consistent with their emerging standard networking-oriented schema that is part of the Directory Enabled Networks (DEN) initiative.

4 *Provide directory management tools*
IBM, with its Tivoli and Lotus subsidiaries, will provide management tools making our directories easy to administer. To meet the critical requirement of management and synchronization of multiple directory services, IBM is enhancing Tivoli User Administration to provide directory management services. IBM and Lotus will deliver directory synchronization function based on their Notespump™ technology.

IBM security strategy and offerings

eNetwork Software security and directory integration delivers an excellent balance of the requirements for security that is invincible, invisible, inexpensive, and integrated. Offerings from IBM and other vendors have been incorporated to provide this balance. Some examples include:

- IBM Global Sign-On provides secure logon to multiple systems after a single, secure logon (invincible, invisible)

- eNetwork Firewall protects networks from hackers, providing access control transparently to users through filters, network address translation, proxies, and socks servers. (invincible, invisible)

- eNetwork Firewall, Content Technologies MIMEsweeper, and IBM AntiVirus work together to search e-mail, e-mail attachments, and files as they enter your network to stop viruses. (invincible, integrated)

- Virtual private networks (VPNs) let users traverse the Internet transparently with complete security allowing customers to replace expensive dedicated lines with low-cost Internet connections; VPNs from IBM use capabilities in eNetwork Firewall, clients (Windows 95, AIX®, OS/2®), servers (AIX, OS/390®), and IBM Nways® routers and controllers and also interoperate with other vendors' products that support the IPSec standards. (invisible, inexpensive, invincible, integrated)

- Security Dynamics SecurID Tokens create one-time passwords to strongly authenticate users and is supported today with eNetwork Firewall and eNetwork VPNs. (invincible, integrated)

- IBM eNetwork LDAP Directory will be imbedded in IBM systems and applications at no additional charge. (inexpensive, integrated)

- IBM Distributed Computing Environment (DCE) is the most integrated infrastructure offering available today. Running on many platforms, this interoperable offering has been updated to take advantage of the latest Internet-based technologies, including LDAP Directory and public-key encryption in addition to its existing directory and Kerberos-based private-key encryption capabilities. (integrated, inexpensive)

Even though IBM offers the most comprehensive security solution today, we will continue to enhance it to meet customer requirements, delivering the optimal balance of invisibility, invincibility, inexpensiveness, and integration. IBM's security strategy has three principles:

1 Integrate using LDAP Directory, KeyWorks, and a public-key infrastructure
IBM will further integrate our security solutions by delivering offerings that further leverage our common eNetwork LDAP Directory, KeyWorks cryptographic toolkit and key recovery mechanisms along with a robust public-key infrastructure (PKI).

2 *Provide a highly scalable cross-platform security offering*
IBM will continue to provide the most scalable solutions in the industry, with functions, such as VPN and Firewall running on the most popular large servers, such as AS/400®, AIX, and Windows NT®. These solutions will also scale down to small, less expensive platforms, such as IBM Nways routers and controllers.

3 *Provide security management tools*
IBM, with its Tivoli subsidiary, will provide management tools making security easy to administer. IBM is enhancing Tivoli User Administration to integrate Global Sign-On and will offer Tivoli Plus Modules for additional security capabilities, such as IBM Firewall.

For more information

For more information about the security and directory integration solution, contact your IBM representative or IBM Business Partner. Or visit our Web pages at:

www.software.ibm.com/enetwork/securitysolution/

IBM Corporation
Research Triangle Park, NC
USA

Printed in the United States of America
6-98

* This paper discusses strategy and plans, which are subject to change because of IBM business and technical judgments.

♻

Printed in the United States of America on recycled paper containing 10% recovered post-consumer fiber

For Position Only