

**What You
Need to Know
About Secure
Information
Access:
An Overview
of Security
Dynamics
Solutions**

Today, having remote access to corporate networks is a matter of business survival. By the year 2000, 55 million people will have remote access (Gartner Group). However, as an organization increases the level of business activity over a distributed computing environment and over the public network, it is also increasing its information security risks. Without advanced network security, a company is exposing itself to millions of dollars of losses due to theft, vandalism and industrial espionage.

Securing remote access—while essential—is no longer enough. Because the corporate network is no longer defined by physical boundaries, it must be defined by business policies. These policies can be implemented through the use of enterprise-level security technology solutions which identify users and control access to network resources or applications. Security Dynamics is building next-generation technology solutions that provide secure access to information, wherever it resides in the enterprise. This white paper outlines the security challenges, discusses how Security Dynamics helps customers secure business resources and explains how organizations can implement a cost-effective migration path from Secure Remote Access to Secure Information Access.

TABLE OF CONTENTS

INTRODUCTION	1
<hr/>	
BUSINESS FACTORS DRIVING SECURITY REQUIREMENTS	3
Secure Remote Access	3
Password Protection Insufficient for Secure Remote Access	4
<hr/>	
SECURITY DYNAMICS SOLUTION	5
Global Administrative Framework	5
Laptop Data Protection	6
Secure Internet Access	6
Extranet Security	7
Moving to Secure Information Access	7
<hr/>	
SECURE INFORMATION ACCESS PROTECTS BUSINESS APPLICATIONS	7
UNIX Host Security	8
Application Security	8
Key Protection Critical	9
<hr/>	
ESS PROVIDES ARCHITECTURE FOR NEXT-GENERATION SECURITY	10
<hr/>	
SECURITY DYNAMICS PROVIDES THE FUTURE OF ENTERPRISE SECURITY	11
ABOUT SECURITY DYNAMICS TECHNOLOGIES	12

BUSINESS FACTORS DRIVING SECURITY REQUIREMENTS

Information has become a critical business asset and technology advances make it increasingly difficult to protect business applications. As users demand—and receive—more computing power and better access to critical business information, organizations realize increased productivity. Information workers increasingly view "anywhere-to-anywhere" remote access as a birthright and expect online connectivity around-the-clock, seven days a week.

Despite the obvious trends toward easy-to-use, distributed applications and universal remote access, organizations must develop appropriate security measures to protect enterprise information. The stakes have never been higher for organizations trying to protect network access and application integrity.

War Room Research, an independent market research firm based in Washington, DC, conducted a study of more than 250 large corporations that produced alarming statistics. More than 48 percent of companies have experienced break-ins within a one-year period, with 24 percent of these break-ins coming through the Internet. When company executives were asked how much money they actually lost, two thirds said they lost more than \$50,000 per year to break-ins, and twenty percent reported losses of at least \$1 million. War Room Research found that more than 208,000 laptops were reported stolen during the 12 months surveyed.

These figures reflect hard dollar losses. For most companies, a much more serious concern is the challenge of protecting intellectual capital that exists in the form of information bits. Most executives who have already adopted corporate security measures are at least as worried about protecting information capital that exists in applications and databases. Organizations must increasingly evaluate the value of securing physical assets as well as the intellectual capital stored in databases and applications.

Information Can Outweigh Dollars in Corporate Valuation

One pharmaceutical company estimates that more than half of its corporate valuation—which is considerably into the billions—exists in the form of electronic bits stored in their databases, which track everything from financial performance to the status of the new drug development. This firm's investment in security is designed to protect those intellectual assets from being stolen.

Secure Remote Access

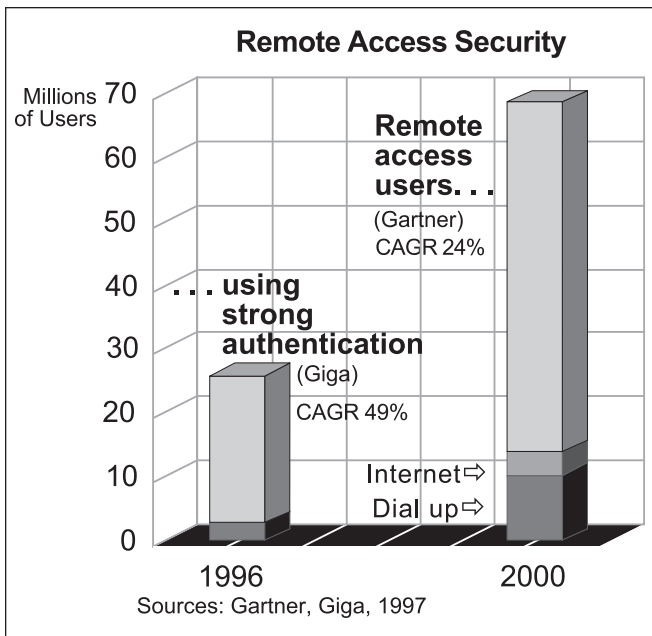
One of the clearest risks to the compromising of the corporate network is the growth of remote access. Most of this growth can be attributed to the rise in remote access users over dial-up lines, such as telecommuters, traveling executives and employees. Companies are also now turning to the Internet for remote access. Ensuring the security of these remote connections to the network is critical to the security of the enterprise network.

Securing Remote Access can be a difficult challenge, requiring both an enterprise architecture and the consistent implementation of component security technologies. Secure Remote Access is required to protect against intrusion from dial-up calls into network servers and to protect from the increasing danger of dial calls "tunneled" through the Internet to access corporate servers. Secure Remote Access technology can be implemented today to protect access to centralized network resources. For example,

organizations today implement Secure Remote Access to allow telecommuters, remote workers and traveling employees to dial into network resources over the public network.

Password Protection Insufficient for Secure Remote Access

Remote Access is one of the most significant security problems faced by customers. To date the focus has been on securing access from a user with a laptop or remote computer connecting across dial-up lines into a remote access server. In the past, security has been provided largely by a single password. This approach has left database information largely unprotected on the assumption that appropriate security has been already been implemented at the edge of the network. Once the server authorized access to a remote client via the password, the user often was free to access information located throughout the network.



Increasingly, corporations are recognizing that password protection alone is a weak form of authentication and no longer sufficient to ensure Secure Remote Access. As the remote access market experiences compound annual growth on the order of 24 percent through the year 2000, the percentage of that market using "strong authentication" is growing at 49 percent per year, according to Giga Information Group.

Corporations are turning to strong authentication because they recognize the problems with passwords. Users are forced to remember too many passwords; passwords are easily guessed or observed; and password administration, such as Help Desk calls resulting from forgotten passwords, cost the average organization more than \$150 per user each year.

When given the option, users will choose passwords that are easy to remember—and consequently easily guessed or "hacked." The most frequently used passwords are words like "secret" and "password" and the maiden name of the user's mother. In addition, with a little time, hackers can use "cracking" programs to run through every permutation of passwords to arrive at the one that unlocks the system. Conversely, better chosen, more complex passwords are difficult to remember and can create even greater security breaches as users resort to writing down their password and attaching them to the monitor. A stolen password often results in long-term damage. If a user's password is observed or hacked, security can be compromised indefinitely, since the legitimate user probably will not know that the password is being used illegitimately.

SECURITY DYNAMICS SOLUTION

The Security Dynamics solution takes the same approach that banks take in protecting automated teller machines from unauthorized users. The familiar ATM card – something we possess – is combined with a personal identification number (PIN) – something we know – to create a secure method of identifying customers. This approach is known as "two-factor authentication." Using this same approach, the Security Dynamics solution protects network access with a two-factor authentication using the SecurID token or smart card.

The SecurID token is a credit card-sized device that eliminates the constraints of simple password protection. SecurID provides an easy, one-step process to positively identify network and system users to prevent unauthorized access by using two-factor authentication. The two factors are an easy-to-remember Personal Identity Number (PIN) and the complex six-to-eight-digit passcode on the token. SecurID tokens generate a new, unpredictable passcode every 60 seconds, offering "crackproof" security for a wide range of platforms in one easy-to-use package. To gain access to a protected resource, the user simply enters the password, followed by the current code on the SecurID token. In addition, SecurID is available in a software version, known as SoftID®, and will soon be available in smart card format.

The SecurID token works in conjunction with ACE/Server® and ACE/Agents. The ACE/Server network security software operates on UNIX and Windows NT servers and utilizes patented technology that synchronizes each token and authorizes access to valid users. ACE/Agents are embedded in third-party devices, such as remote access servers, and applications, such as Netscape Web servers, and serve as access control agents directed by the ACE/Server to allow authorized users to gain access to the network.

Customers select this Security Dynamics solution safe in the knowledge that ACE/Agent technology is embedded in virtually every device that sits at the perimeter of the network. Security Dynamics works with all leading remote access technology vendors through its SecurID Ready Strategic Partner program. The company has developed more than 60 strategic partnerships with remote access server vendors, firewall providers and operating systems vendors—a Who's Who of the networking industry. No other security vendor has the market share or the extensible technology required to drive ubiquitous support of security technologies.

Global Administration Framework

Managing security can become increasingly difficult as the network scales to support tens and then hundreds of thousands of users. As remote access requirements increase, enterprise networks need to scale security solutions and expand them to provide international security. Global administration requires the ability to support multiple users, wherever they travel, wherever they log into the network. It often requires the ability to support not just tens of thousands, but hundreds of thousands of users.

Security Dynamics continues to invest heavily in global administration solutions for enterprise security that are highly scalable, easy to administer and flexible. The Security Dynamics ACE/Server solution includes the ability to administer the entire global authentication network from any location, delegate administrative roles and allocate management privileges. Security Dynamics solutions also include the ability to re-assign passwords, generate customized security reports and perform other traditional administrative tasks.

Laptop Data Protection

Horror stories abound on the dangers of lost or stolen laptops. This issue is particularly acute for companies with information workers that travel with sensitive or confidential information on their laptops. Now that users regularly carry sensitive corporate data with them, organizations must manage the risks of this information being lost or stolen.

The RSA SecurPC® product encrypts laptop data and is the first general-purpose encryption product approved for export with strong 128-bit encryption. For the first time, companies can deploy the full-strength encryption power of RSA SecurPC without the use of a trusted third party for key escrow or the need for elaborate reporting requirements or additional U.S. government approvals.

Industry analysts estimate it would take more than a billion dollars worth of computer equipment over a year to crack a single file with 128-bit encryption. RSA SecurPC encrypts each file with a different key and relies on multiple trustees to protect corporate data. It includes a key recovery feature that supports central administration of key recovery and allows companies to set up a group of trustees, a subset of whom can decrypt documents without access to the user's private key.

Secure Internet Access

As private network applications migrate to the Internet, more organizations must provide Secure Remote Access for tunneled traffic. Long-distance phone charges can be reduced dramatically by allowing remote clients—or even remote offices—to place calls to a local service provider that traverse the Internet and are terminated at the customer premises.

Virtual Private Networks (VPNs) provide the medium for using the public Internet backbone as a channel for private data communication. Mobile workers, telecommuters, contractors, traveling employees and even business partners or customers can connect to network resources over the Internet, rather than over expensive private lines. Although the session encryption technology deployed by VPNs keeps the data secure while in transit, authentication is required to validate the session. If the password of either the sender or recipient has been compromised, the entire communication is insecure. Therefore, the only way to make communication secure is to authenticate VPN users and to encrypt communications.

Leading VPN Providers Partner with Security Dynamics

Leading providers of VPN technology are participating in Security Dynamics' SecurVPN program to add two-factor SecurID authentication to their solutions. More than a dozen leading VPN vendors – including AltaVista, Ascend, Bay Networks, Checkpoint, IBM, Raptor Systems and Sun – have already joined the SecurVPN program, and are ensuring that their VPNs will support technology from Security Dynamics.

Extranet Security

Another emerging customer need is to secure access to Web pages—in particular, to support extranet applications that establish secure communications with suppliers and customers. WebID is a specialized ACE/Agent that allows customers to protect specific Web pages. ACE/Agents are embedded in both the Microsoft and Netscape Web server software to allow customers to protect specific Web pages when implemented in conjunction with SecurID.

WebID lets users secure specific pages of their Web site with authentication required only once per session. It also supports "cookie" persistence by either elapsed time or inactivity, automatic cache clean up and the optional administrative ability to require single sign-on before assigning a Web page address. Today, WebID is used by many companies to support customer service communications from their published Web sites. In addition, major banks are relying on SecurID to allow customers to engage in banking online.

Moving to Secure Information Access

Secure access directly to sensitive applications and databases is emerging as a critical concern. While in the past it may have been enough to provide security at the network periphery to authenticate each user before providing network access, it is becoming increasingly important to control user access to critical information and to support encrypted communications and secure transactions.

This shift is resulting from past perspectives of private networks as secure and public network and Internet applications as non-secure. The traditional focus has been on network periphery defense, which is becoming insufficient as organizations migrate applications to run over the Internet.

As security needs advance, access technologies also evolve. Enterprise security requires immediate focus on Secure Remote Access to ensure data privacy and network integrity, while evolving toward Secure Information Access as the technologies become available for application-layer security.

SECURE INFORMATION ACCESS PROTECTS BUSINESS APPLICATIONS

Securing Information Access is the next challenge organizations must face in protecting enterprise information. Security Dynamics is building on its market-leading product base to introduce new products and technologies that address the need for Secure Information Access and deliver secure access to applications. Customers need to implement security solutions that take into consideration the demands of securing information that travels through an Intranet or some other less secure element of the corporate network.

The company's acquisition of Sweden-based DynaSoft AB provides Security Dynamics with the tools and technologies to facilitate Secure Information Access. DynaSoft, an emerging leader in the world of application access and single sign-on solutions, added the BoKS® family of products to Security Dynamics solutions. BoKS provides UNIX host security and secure single sign-on solutions. BoKS Manager allows administrators, authenticated by SecurID tokens, to secure networked UNIX servers and workstations. Combined with new versions of BoKS Desktop and BoKS Connect, BoKS Manager also enables security managers to implement secure single sign-on for user access to a wide range of databases and applications.

UNIX Host Security

Many organizations rely on UNIX as the platform for critical corporate information and applications; however, the inherent security weaknesses of UNIX and the lack of consolidated systems audit in UNIX make the platform an easy target for users to gain unauthorized access to system resources. These weaknesses make corporate information vulnerable to threats originating from both inside or outside the corporation. BoKS Manager counters UNIX weaknesses by providing strong network-based authentication, access control, system monitoring and audit for a network of UNIX workstations and servers. In addition, BoKS Manager provides auditing features that allow administrators to monitor user activity, alerting them to possible security violations and maintaining a protected record of all access. These security features are key for certain regulated industries, such as banking and telecommunications, where UNIX host security is a key element of required security audits.

The security offered by BoKS Manager is further enhanced through the use of SecurID tokens which are deployed to authenticate administrators strongly to the system. This strong authentication combines a user's PIN with a one-time passcode generated by the token to verify that only authorized users are able to perform administrative tasks. BoKS combines this strong authentication with role-based access, ensuring that administrators perform only authorized security-related tasks. Unlike similar solutions on the market today, which authenticate administrators using easily compromised, static passwords, BoKS Manager offers administrators the ability to authenticate using SecurID, the market-leading solution for two-factor authentication.

Application Security

BoKS Manager, used in conjunction with BoKS Desktop and BoKS Connect, provides a comprehensive solution for securing access to enterprise applications while reducing the complexity of multiple passwords and credentials with which users must contend. Security Dynamics' Secure Single Sign-On (SSSO) solution goes beyond most existing single sign-on solutions by using RSA cryptography to ensure data privacy between the user desktop and the target application. The Security Dynamics' SSSO solution consists of four components:

- **BoKS Desktop.** The BoKS Desktop provides secure single sign-on capabilities from the desktop to mission-critical applications and servers. BoKS Desktop stores authentication credentials, including digital certificates, in a secured container or Personal Security Device (PSD), residing on the desktop. The BoKS PSD holds the user's credentials, including such resources as the user's private key and public-key certificates, for SSSO and other privacy and integrity applications. BoKS Desktop provides the additional option of strong authentication for accessing the PSD using smart cards.
- **BoKS Connect.** In order to create an SSSO environment, organizations deploy BoKS Connect agents for those applications and resources they want to protect. BoKS Connect provides agents that "front-end" the application server, providing security services transparently – without the need to modify applications. These agents permit access to only those users who are authorized by the BoKS Manager. BoKS Connect agents are currently available for Oracle, Sybase and Informix applications as well as Telnet and HTTP for Internet applications.
- **ToolBoKS.** Customers and ISV's can deploy SSSO agents for other third-party or internally developed applications and for other security domains using the ToolBoKS toolkit. By deploying solutions with ToolBoKS, the detail associated with coding and maintaining application logon-related security is significantly reduced for the application programmer. It enables implementation of numerous applications such as secure email, secure remote access, secure Internet services and secure electronic commerce.
- **BoKS Manager.** With BoKS Manager 4.4, access rights for individuals or groups are managed from a single point. In addition to managing clients using BoKS Desktop, BoKS Manager also manages users' single sign-on rights to applications using BoKS Connect. Along with controlling which applications a user can access, BoKS Manager administrators can also control single sign-on access to the system for each user to include time of day, access method and location of access.

BoKS Manager also acts as a Certificate Authority. Using an embedded CA, administrators can issue user and host certificates, as well as revoke such certificates. BoKS Manager also administers users' credentials including certificates, which are stored in the user's PSD, to provide or deny access to system resources from the user's desktop. The BoKS PSD Administration system can also create a soft PSD, software-based personal security devices used to authenticate users and hosts. To simplify the PSD distribution, a BoKS Directory Service is provided, making it possible to automatically download user PSDs and Certificate Revocation Lists to a BoKS Desktop.

Key Protection Critical

Public key technology is emerging as an important way of providing securing access to information. However, Secure Information Access can only be provided when the security keys are protected. Today, the most common

solution used is software protection, where the key is locked in a file in the laptop and is accessible via the static password. A stronger solution for protection of the private key is possible by using the SecurID token for authentication, and then having the network automatically send back a one-time code that unlocks the private key in the laptop. This approach allows centralized management of the authentication process and supports auditing. Smartcards are another alternative, but require each laptop to have a smart card reader. Using the technology delivered by its subsidiary, RSA Data Security, Security Dynamics is developing a smart card that actually carries the private key and allows the user access using two-factor authentication. The smart card will play an increasingly important role in delivering this technology as the readers for these cards become more ubiquitous and customers roll out Public Key Infrastructure (PKI).

As should be obvious with this approach, a customer can have strong PKI technology protected by a weak static password access. Once an unauthorized user guesses, hacks or observes a password the information is exposed. Current tokens will play a continuing and important role even as Security Dynamics expands on the technology to include the smart card in its family of soft and hard token options. According to a June 1997 report from Forrester Group on the topic of remote access over the Internet, Forrester's first conclusion and recommendation to their client base was to continue to use current token technology. Essentially, strong authentication is important, and token technology provides the ideal solution today for corporations' existing infrastructures. Tokens represent the most mature and easy-to-implement solution for the immediate future.

ESS PROVIDES ARCHITECTURE FOR NEXT-GENERATION SECURITY

Security Dynamics' Enterprise Security Services (ESS) architecture helps companies in developing a long-term security roadmap. The ESS architecture provides customers a framework to understand the strategic direction of Security Dynamics and to plan for migration of existing security solutions to new technologies.

With ESS, Security Dynamics is building from its traditional strength in securing the edge of the network and evolving from Secure Remote Access to Secure Information Access. Security Dynamics is building from the market dominance of SecurID and SoftID, and broad acceptance of the company's technology through partnerships with leading firewall, routing and server vendors.

Security Dynamics will continue to be the leader in Identification and Authentication, and is evolving its product set toward an enterprise-wide administration architecture based on distributed Windows NT and UNIX server platforms.

WHAT YOU NEED TO KNOW ABOUT SECURE INFORMATION ACCESS

Security Dynamics will continue to provide PC-level security for both desktop and laptop computers. Over time, the company will deliver a unified desktop approach allows the user to hold the credentials on the desktop and use a smart card to unlock them. The solution consists of RSA SecurPC for encrypting laptop data, SecurID for identifying and authenticating users for access to network resources, and digital signatures through the VeriSign partnership.

Managing secure single sign-on will be enabled by the integration of ACE/Server and BoKS technology to provide an enterprise security engine for administering and managing security policies worldwide. ACE/Server provides the leading authentication technology and BoKS provides privilege management. These technologies are being combined to provide a single platform for enterprise security, including management of third-party technologies. Users benefit from global, secure access to information under a common architecture and the enterprise is able to design, administer and enforce global security policies. Toolkits, such as ToolBoKS, will continue to provide users the flexibility to extend Secure Information Access to third-party application environments, such as those offered by SAP and PeopleSoft.

Key to the deployment of ESS is the expansion of Security Dynamics' agent technology to the application layer. ACE/Agent technology is already embedded in more than 60 network devices, operating systems and application environments. BoKS brings Oracle and Sybase agents and the ToolBoKS kit for building agents to interface with different environments. Security Dynamics will continue to build partnerships to ensure that application layer security is provided throughout the enterprise so that enterprise IT departments can invest in Security Dynamics' technology safe in the knowledge that Security Dynamics products are compatible with products from other leading vendors.

SECURITY DYNAMICS PROVIDES THE FUTURE OF ENTERPRISE SECURITY

Through internal development, acquisitions and partnerships, Security Dynamics will continue to expand its portfolio under the ESS architecture, providing a complete, global, enterprise security solution. ESS will protect investments in security by migrating existing technologies under a common umbrella.

As computing and communications resources continue to become more distributed, control over enterprise information will become an even greater asset. Customers can evolve from Secure Remote Access to Secure Information Access while protecting investments in security technology by relying on Security Dynamics for enterprise security requirements.

ABOUT SECURITY DYNAMICS TECHNOLOGIES

Security Dynamics is the leading provider of enterprise and network data security solutions. Security Dynamics' solutions help companies conduct business securely, protect corporate information assets and facilitate business-to-business electronic commerce. Security Dynamics' products employ patent-protected SecurID token technology and ACE/Server® software or hardware access control products to authenticate the identity of users accessing networked or standalone computing resources. With 2 million users in 2,000 companies, Security Dynamics is the world leader in two-factor user identification and authentication. RSA Data Security Inc., a wholly owned subsidiary of Security Dynamics, is the world's brand name for cryptography, with more than 80 million copies of RSA encryption and authentication technologies installed and in use worldwide. Security Dynamics and RSA can be found on the World Wide Web at <http://www.securitydynamics.com/> and <http://www.rsa.com/>, respectively.

Security Dynamics and the Security Dynamics logo are trademarks of Security Dynamics Technologies, Inc. All other trademarks are the property of their respective owners.

©1998 Security Dynamics Technologies, Inc. All rights reserved.

Printed on recycled paper.

CWP01

SecurityDynamics®

Corporate Headquarters: 20 Crosby Drive, Bedford, MA 01730 USA, Tel 800 SECURID or 781 687 7000 Fax 781 687 7010

European Headquarters: United Kingdom, Tel 44 118 9036 2600 Fax 44 118 979 5833

Asia/Pacific Headquarters: Singapore, Tel 65 733 5400 Fax 65 733 2400 | **Japan:** TEL. 81 3 35639 7511 FAX 81 3 3539 7518

Email: info@securitydynamics.com **Internet:** www.securitydynamics.com