

www.securecomputing.com

Secure Computing® is a global leader in Enterprise Gateway Security solutions. Powered by our TrustedSource™ technology, our award-winning portfolio of solutions help our customers create trusted environments inside and outside their organization.



SafeWord Solutions Provide Easy, Cost-Effective Strong Authentication to Manage Remote Users

Table of Contents

Access Begins with Identity	2
Memorized Passwords Are Becoming Obsolete	2
The Answer is Strong Authentication	2
Introducing SafeWord Two-Factor Authentication	3
Why SafeWord?	4
Conclusion	5

Secure Computing Corporation

Corporate Headquarters

4810 Harwood Road
San Jose, CA 95124 USA
Tel +1.800.379.4944
Tel +1.408.979.6100
Fax +1.408.979.6501

European Headquarters

Berkshire, UK
Tel +44.(0).870.460.4766

Asia/Pac Headquarters

Wan Chai, Hong Kong
Tel +852.2598.9280

Japan Headquarters

Tokyo, Japan
Tel +81.3.5339.6310

For a complete listing of all our global offices, see www.securecomputing.com/goto/globaloffices

Access Begins with Identity

Remote access to your network has become mission-critical. As IT administrators increasingly provide more access to more resources from more remote locations, they are charged with ensuring a secure remote access connection that proves user identity before authorizing access. Employees working remotely need access to email, files and other applications in order to perform their duties productively. Similarly, partners and even customers may need to have access to certain applications and data residing on an enterprise network. The growing number of users that need access to the network is matched only by the growing amounts of data that is available in the corporate datacenters. A user's identity is the key to managing access to this data.

Ensuring that data is accessible only to the intended recipients is good business. Data in the wrong hands may result in severe business and legal liabilities (e.g. proprietary business information in the hands of competitors may diminish a competitive advantage). Similarly, customers' private data (credit card information, health records, Social Security numbers, etc.) must be protected from unauthorized access to ward off potential legal liabilities. In fact, stricter compliance requirements in many cases require that enterprises ascertain identities of the users before providing them access to sensitive data.

User authentication with passwords has served as a means of establishing user identities since the earliest days of network security. The system worked fine when the user community requiring access was small and data stored on the systems was not very sensitive. Thus, hackers had little incentive to gain unauthorized access to networks. Over the years, increasingly sensitive data on the networks has attracted more hackers to break into enterprise networks. Simultaneously, access by a large user community leaves enterprises even more vulnerable to hacker access since security of the system is now dependent on the strength of the weakest password in a large group of passwords.

Access in critical network environments begins with proof of identity. Only properly authenticated, properly authorized individuals should be allowed access to the network. Two-factor authentication is a de facto requirement for remote access and very often a requirement for internal access as well.

Memorized Passwords Are Becoming Obsolete

Remote access gateways such as VPNs, Citrix, and Outlook Web Access all create secure tunnels over the Internet. These gateways provide a convenient and secure remote link to network resources. However, relying on simple usernames and passwords to access the entrances to these secure gateways is similar to leaving the front door to your house unlocked, or using a lock that can be easily picked. Static passwords are an unreliable mechanism for guarding the entrance to your trusted systems, applications, and networks. Passwords can be easily guessed, hacked, or compromised by brute force attacks.

Even complex password policies present problems for end users and IT departments. Changing passwords every 30 days, not allowing users to repeat a password over a given time period and requiring multiple special characters in passwords adds significant complexity. Users may simply forget their password, requiring a call to the help desk to reset the password and driving up the overall cost of IT support and lost productivity, to say nothing of diminished user convenience.

Most industry analysts agree that passwords are rapidly becoming obsolete, and companies that rely on them are exposing themselves to significant risk of security breach.

The vulnerabilities of static passwords as an identity mechanism have been well-documented, raising the need for stronger methods of user authentication. Companies need strong authentication solutions that not only provide reliable security, but that are also easy to install and deploy, simple to manage, and able to grow with their needs.

The Answer Is Strong Authentication

Clearly, organizations with valuable information must choose something stronger than passwords to protect their resources. Strong authentication refers to systems that require multiple factors for authentication and use advanced technology, such as secret keys and encryption, to verify a user's identity. The simplest example of strong authentication is your ATM card. This requires something

you have (your card), and something you know (your PIN). Most people wouldn't want their bank to allow access to their checking account with just one factor. Yet many organizations allow entrance to their valuable VPN, Citrix, and Outlook Web Access resources (often much more valuable than a single personal checking account) with only one factor—a weak static password.

Typical two-factor authentication systems use a shared secret (e.g. one-time password and one additional factor) to determine the identity of the user accurately. Even today, hardware token-based authentication remains the most reliable and trusted form of strong authentication. Token-based authentication distinguishes itself in terms of security, cost of ownership and ease of use. Secure Computing's SafeWord® strong authentication is a leading two-factor authentication solution preferred by some of the most discerning and security-conscious enterprises.

Introducing SafeWord Two-Factor Authentication

SafeWord products positively identify users through strong authentication to assure that only the right people can access your trusted applications and networks. SafeWord offers unparalleled flexibility, scalability, and ease of use, and is used by thousands of organizations and millions of end users worldwide every day.

SafeWord solutions deliver security through one-time passcode-generating hardware tokens combined with the user's PIN.



Figure 1: SafeWord hardware tokens

When a user pushes the button on the SafeWord token, it immediately generates and displays a single-use passcode (via a unique secret key and an advanced encryption algorithm that is contained inside). The user enters the passcode, followed by the user's unique PIN, to gain access. After one use, the passcode is thrown away by the system. If someone attempts to re-use a passcode, access is denied by the authentication server.

Each remote user must have the SafeWord token in their possession (much like the ATM card) and know the PIN. This is true two-factor authentication, and it eliminates the risks of stolen or compromised passwords.

SafeWord also offers a solution for users of mobile devices who prefer not to carry a token. SafeWord MobilePass combines the security of proven two-factor authentication with the convenience of one-time passcodes delivered right on your personal mobile device or laptop PC. MobilePass is a software-based authentication solution that delivers one-time passcodes for a variety of mobile phone platforms, including Palm, Blackberry, Windows Mobile, and J2ME-enabled devices. MobilePass is also available for SMS messaging delivery and Windows Desktop, where one-time passcodes are generated on your laptop or desktop PC.

Why SafeWord?

1. SafeWord tokens never expire

SafeWord provides the lowest total cost of ownership with tokens that never expire. Competing authentication solutions require you to repurchase tokens every two or three years—their tokens are programmed to expire at the end of that period. Additional costs are incurred not only purchasing replacement tokens, but also re-deploying those tokens to the user base. SafeWord tokens never expire, giving you compelling cost-of-ownership value.

2. Easy to install, easy to use, perfect for Windows environments with Active Directory

SafeWord products are designed to be easily and cost-effectively managed by administrators of remote access solutions. Independent industry product audits have confirmed that SafeWord is one of the easiest products to implement and administer, especially for Microsoft environments.

Installation is lightning-fast. Competing solutions can take hours or days to install and configure properly. Often, systems engineers must be scheduled from the vendor to install the software correctly. Security policies must be mapped out. Ports must be opened, or closed, or both. But with SafeWord, the wizard-driven installation leads you through the process in as little as 15 minutes.

In many cases, a separate server is not even needed. SafeWord solutions can install easily on your Active Directory domain controller.



Figure 3: The SafeWord plug-in to Active Directory

Administrators can manage all user information from the Microsoft tools they already know and use with Active Directory. Other solutions use a proprietary user database which must be managed separately. SafeWord offers true Active Directory integration. The Microsoft Management Console in Active Directory ties the SafeWord tokens directly to your Active Directory users, so there's just one place to manage users and tokens.

SafeWord also includes a convenient, Web-based user self-enrollment capability. With user self-enrollment, administrators don't have to match each user to their correct token or assign tokens—users can simply enroll themselves online.

3. Powerful Remote Access Authentication for VPNs, Citrix, Outlook Web Access (OWA)

SafeWord adds critical strong authentication to positively identify a user before an encrypted VPN gateway is established—an essential component of any secure VPN solution. SafeWord offers robust and scalable solutions that work with all major VPN vendors including Alcatel, Cisco, Check Point, Microsoft, Nortel Networks, Juniper, Aventail, and F5, in addition to the SafeWord SecureWire® Access Gateway.

SafeWord also ships with software agents that enhance security for Citrix®—and requires no additional software on the client's workstation. Users can take advantage of a single login screen for ease of authentication. PremierAccess protects Citrix applications including Citrix Access Gateway, Citrix Presentation Server, Citrix GoToMyPC Corporate, and Citrix Access Essentials.

SafeWord even provides strong authentication and a single-screen user login experience to Microsoft Outlook Web Access, protecting valuable corporate e-mail from password attacks.

4. SafeWord Solutions to fit your requirements

SafeWord fits the needs of both large and mid-size organizations. SafeWord is designed to protect VPN, RADIUS, Citrix, and Outlook Web Access connections and offers tailored solutions specifically designed for Citrix, Cisco, Check Point, and Nortel remote access environments.

SafeWord also provides advanced features and functionality and extends authentication for Windows Domain and Terminal Services logins as well. SafeWord offers powerful management tools with the Enterprise Solution Pack (ESP), an add-on package that provides advanced user management, support for a wide range of authentication form factors, advanced reporting capabilities, rich access control functionality, a Universal Web Agent to protect Windows and Solaris servers, and support for UNIX logins and custom applications.

Conclusion

SafeWord solutions offer powerful and scalable strong authentication that is also easy to administer and easy to use. With tight integration to Microsoft Active Directory, administrators can leverage their existing user infrastructure and the tools they already use and know. And with Web-based user self-enrollment, deploying tokens to end users is quick and cost-effective. Finally, SafeWord tokens never expire, providing you with a much lower total cost of ownership and compelling overall authentication value.