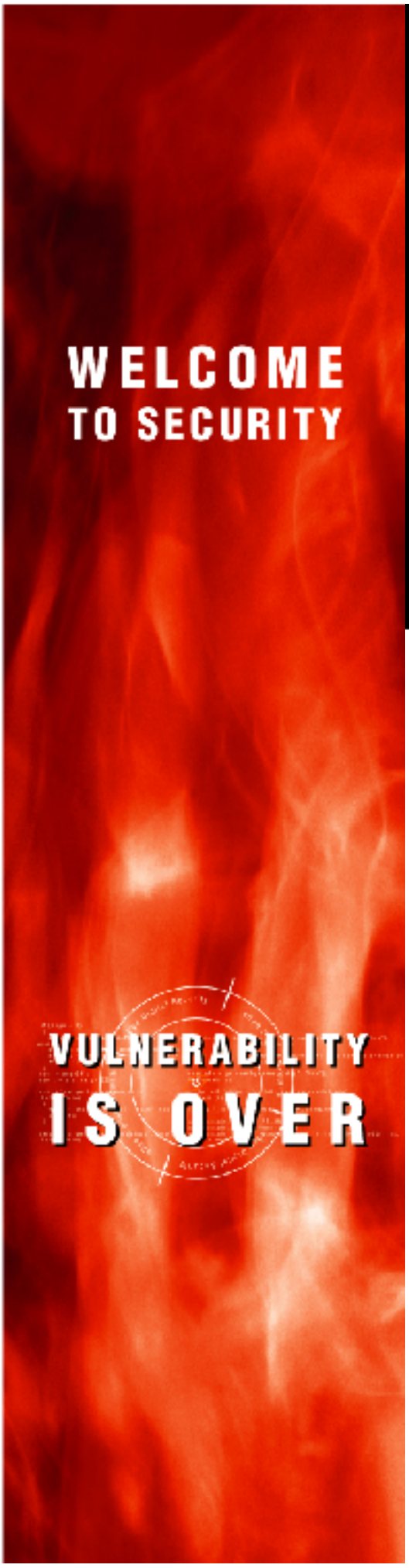


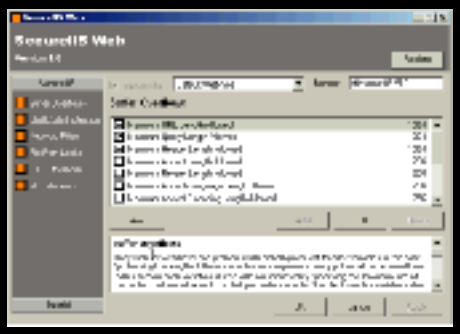
SecureIIS

SecureIIS Web™
THE APPLICATION FIREWALL

SecureIIS protects Microsoft IIS (Internet Information Services) Web servers from known and unknown attacks. SecureIIS wraps around IIS and works within it, verifying and analyzing incoming and outgoing Web server data for any possible security breaches. SecureIIS combines the best features of Intrusion Detection Systems and conventional network firewalls into one product, and it is custom tailored to your Web server.

SecureIIS Web has the ability to give your Web server security that is unmatched by any other product in the market.

With the click of a button SecureIIS protects your Web server from known and unknown attacks



SecureIIS will deny attacks on your Web server and alert administrators to any attempted break-ins

Protection Features

SecureIIS can bring never-before-seen protection to your Web sites and Intranet Web servers. This high level of protection comes from SecureIIS's ability to understand the HTTP (Web server) protocol and the classes of attacks that Web servers are vulnerable to.

SecureIIS protects against the following types of attack:

Buffer Overflow Attacks:
Buffer overflow vulnerabilities stem from problems in string handling. Whenever a computer program tries copying a string into a buffer that is smaller than the string, an overflow can be caused. If the destination buffer is overflowed sufficiently it will overwrite various crucial system data. In most situations an attacker can leverage this to takeover a specific program's process, thereby acquiring the privileges that process or program has. SecureIIS limits the size of the "strings" being copied. Doing this greatly reduces the chance of a successful buffer overflow.

Parser Evasion Attacks:
Insecure string parsing can allow attackers to remotely execute commands on the machine running the Web server. If the CGI script or Web server feature does not check for specific characters in a string, an attacker can append commands to a normal value and have the commands executed on the vulnerable server.

Directory Traversal Attacks:
In certain situations various characters and symbols can be used to break out of the Web server's root directory and access files on the rest of the file system. By checking for these characters and only allowing certain directories to be accessed, directory traversal attacks are prevented. In addition,SecureIIS only allows clients to access certain directories on the server.

General Exploitation:
Buffer overflows, format bugs, parser problems, and various other attacks all contain similar data. For example, exploits that execute a command shell will almost always have the string "cmd.exe" in the exploiting data. By checking for common attacker "payloads" involved with these exploits, an attacker can be prevented from gaining unauthorized access to your Web server and its data.

SecureIIS also has the following features:

HTTPS/SSL Protection:
SecureIIS resides inside the web server, therefore capturing HTTPS sessions before and after SSL (Secure Socket Layer) encryption. Unlike any Intrusion Detection System or Firewall currently on the market, SecureIIS has the ability to stop attacks on both encrypted and unencrypted sessions.

High Bit Shellcode Protection:
Shellcode is what is sent to a system to effectively exploit a hole called a "buffer overflow". SecureIIS's High Bit Shellcode Protection offers you a high degree of protection against this type of attack because it will drop and log all requests containing characters that contain high bits.

Third Party Application Protection:
The power of SecureIIS is not limited to IIS specific vulnerabilities. SecureIIS can also protect third party applications and custom scripts from attack. If your company has developed customized components for your Web site, components that might be vulnerable to attack, you can use SecureIIS to protect those components from both known and unknown vulnerabilities. Let SecureIIS work as your own web based “Security Quality Assurance” system.

Logging of Failed Requests:
In the installed SecureIIS directory there exists a file called SecureIIS.log. This file contains a log of all attempted attacks and events that caused SecureIIS to drop the connection. This is an effective way to monitor why requests are being stopped, and who is requesting things that they shouldn't be requesting. Since SecureIIS enforces a strong security policy for how sites are configured, an administrator can use this log to find places where the Web site may not be acting correctly due to an insecure setting.

The Ultimate Proactive Security Tool

SecureIIS protects Microsoft IIS from "typical" hacking attacks. Additional checks are in place for attacks that do not follow recognized patterns. SecureIIS monitors Web traffic before IIS receives it and after IIS has already handled it. This approach provides extra security and protects against various attacks that involve data conversion problems.

All of these additional protection features make SecureIIS the product of today that protects you from the attacks of tomorrow, making it the ultimate proactive security tool.

System Requirements

Windows NT 4.0 and
Microsoft IIS (Internet Information Services) 4.0 or

Windows 2000 and
Microsoft IIS (Internet Information Services) 5.0