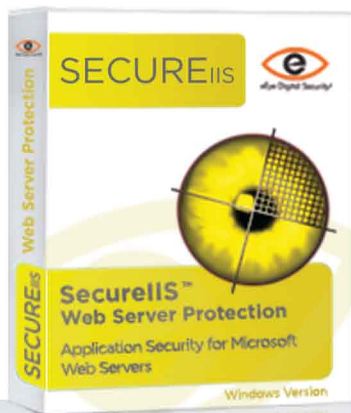




# SECURE IIS™ Web Server Protection

## Proactive Web Server Security.



### Fast Facts

- Runs on Windows NT 4 (IIS 4), Windows 2000 (IIS 5), or Windows 2003 (IIS 6, 32 bit)
- Integrated technology does not affect server performance
- Compatible with common web-based applications such as Flash, Cold Fusion, FrontPage, Outlook Web Access and more
- Protects against the following classes of attacks: buffer overflow, parser evasion, directory traversal, general exploitation, high-bit shellcode protection, cross site scripting, and SQL injection and more

**Secure Your Business.**  
[www.eEye.com](http://www.eEye.com)  
866-282-8276

Vulnerabilities in software applications are responsible for the vast majority of network security breaches and data loss today. Specifically, web server applications like Microsoft's IIS are consistently targeted because of the ease of application deployment and potential flaws inherent with coding and configuration mistakes. Because web servers often provide a portal to the internal network, they require a more formidable and customized level of protection above and beyond what network firewalls or intrusion detection systems can provide. Developed by eEye Digital Security as the most comprehensive IIS application firewall, SecureIIS™ operates within IIS to actively inspect all incoming requests at each stage of data processing. In this way, SecureIIS prevents potentially damaging network traffic, whether encrypted or unencrypted from penetrating your servers and compromising your web based applications.

### Application Layer Protection

eEye Digital Security pioneered the concept of application-layer protection, which has revolutionized proactive security. Unlike network-layer protection products, an application-layer solution works within the application that it is protecting. SecureIIS inspects requests as they come in from the network layer, as they are passed up to the kernel, and at every level of processing in between. If at any point SecureIIS detects a possible attack, it can take over and prevent unauthorized access and/or damage to the web server and host applications.

### IIS ISAPI Integration

SecureIIS was developed as an ISAPI filter, which allows for a tighter integration with the web server as compared to other application firewalls. SecureIIS monitors data as it is processed by IIS and can block a request at any point if it resembles one of many classes of attack patterns; including SQL injection and cross site scripting. Because of eEye's extensive knowledge of the various ways in which IIS servers and web applications can be attacked, as well as the nature of an application firewall, even undiscovered vulnerabilities are secured and thwarted.

### Zero Day Protection

Unlike network firewalls and intrusion detection systems, SecureIIS does not rely upon a database of attack signatures that require regular updating. Instead, it uses multiple security filters to inspect web server traffic that could cause buffer overflows, parser evasions, directory traversal, or other attacks. Therefore, SecureIIS is able to block entire classes of attacks, including those attacks that have not yet been discovered. SecureIIS provides true zero day protection for entire classes of attacks whether known or unknown.

### Compatibility and Key Features

SecureIIS works with and protects all common web-based applications such as Flash, Cold Fusion, FrontPage, Outlook Web Access, and many third party and custom applications. Configurations can be modified without having to restart the web server, thus preventing disruption of the active website. SecureIIS runtime logs provide detailed explanations as to why requests were denied and allow for data to be exported in any number of different formats including tab delimited, text, and Excel. This activity can also be graphed in real-time based on class of attack. Regardless of the communications protocol, SecureIIS offers protection without affecting service levels on your web server, and even stops attacks on encrypted sessions based on the ability to analyze the content of HTTPS sessions before and after SSL encryption.

### Designed by Security Research Experts

eEye is recognized as one of the most trusted and respected sources dedicated to improving IIS security. eEye's research team is credited with having discovered several high-severity IIS vulnerabilities that would have allowed an attacker to gain complete remote control over a susceptible server.

# SECURE IIS®

## Additional Features and Benefits

SecureIIS protects against the following attack types:

### SQL Injection

SecureIIS is designed to filter the most common commands and characters used in SQL injection attacks. This stops SQL injection attempts dead in their tracks and can be verified with Retina® Web Security Scanner.

### Buffer Overflow Attacks

SecureIIS checks the lengths of all client-supplied buffers. If the data is larger than the maximum size allowed, SecureIIS will drop the connection, thereby avoiding a buffer overflow.

### Parser Evasion Attacks and High-Bit Shellcode Protection

Insecure string parsing can allow attackers to remotely execute commands on the machine running the web server. SecureIIS checks for various characters in a string that would allow an attacker to add on commands to a normal value. If these characters are found, SecureIIS will drop the connection. In addition, normal English-language web traffic does not contain high bit characters. SecureIIS will drop all requests containing high bit characters, which often signal a potential buffer overflow attack.

### 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. SecureIIS checks for these characters and also blocks access to specific directories and can even alert when specified files or directories are accessed or modified or even deleted.

### RFC Compliancy and Other Attack

SecureIIS prevents attackers from manipulating the HTTP protocol in attempts to bypass security systems and exploit security holes. SecureIIS has additional checks in place to identify and drop requests that contain recognized patterns. Limitations are also placed on the size of uniform resource locators (URL/URI), HTTP variables, request methods, request header size and other HTTP-related content and payloads that try to use common commands like cmd.exe.

## About eEye Digital Security

eEye® Digital Security is pioneering a new class of security products: integrated threat management. This next-generation of security detects vulnerabilities and threats, prevents intrusions, protects all of an enterprise's key computing resources, from endpoints to network assets to web sites and web applications, all while providing a centralized point of security management and network visibility. eEye's research team is consistently the first to identify new threats in the wild, and our products leverage that research to deliver on the goal of making network security as easy to use and reliable as networking itself. Founded in 1998 and headquartered in Orange County, California, eEye Digital Security protects more than 9,000 corporate and government organizations worldwide, including half of the Fortune 100. **For more information, please visit [www.eEye.com](http://www.eEye.com).**

U.S. Tel: 1.866.282.8276

N. America: 1.949.333.1900

Germany: +49 (0) 8031 2227 432

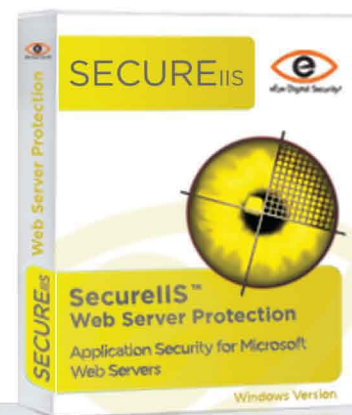
U.K.: +44 (0) 20 8144 1102

Asia Pacific: +603 79581575

N. America Sales: [sales@eEye.com](mailto:sales@eEye.com)

International Sales: [sales.eu@eEye.com](mailto:sales.eu@eEye.com)

Asia Pacific Sales: [apacsales@eEye.com](mailto:apacsales@eEye.com)



## System Requirements

- Windows NT 4.0, IIS 4.0 and Service Pack 6
- Windows 2000, IIS 5.0 and Service Pack 1 or greater
- Windows 2003, IIS 6.0 (32 bit only)