

McAfee Enterccept Web Server Edition

Intrusion Prevention for Web Servers

The Challenge

The number of new vulnerabilities and the speed and sophistication of attacks seeking to exploit those vulnerabilities increase every year, intensifying the risks to enterprise security. Enterprises must defend themselves against new hybrid attacks using multiple vectors to breach the security infrastructure.

Web servers present unique security challenges. They must be externally accessible, yet such accessibility places them within easy reach of attackers anywhere in the world.

Unfortunately, traditional host IDS tools are reactive and always one step behind an attack. To ensure comprehensive, proactive security, enterprises need to adopt a layered approach to security that delivers overlapping and complementary technologies that protect networks and systems from the edge to the core. McAfee® Intrusion Prevention delivers the most comprehensive, accurate, and scalable threat protection solutions available, helping enterprises mitigate risk, ensure business availability, and reduce total cost of ownership.

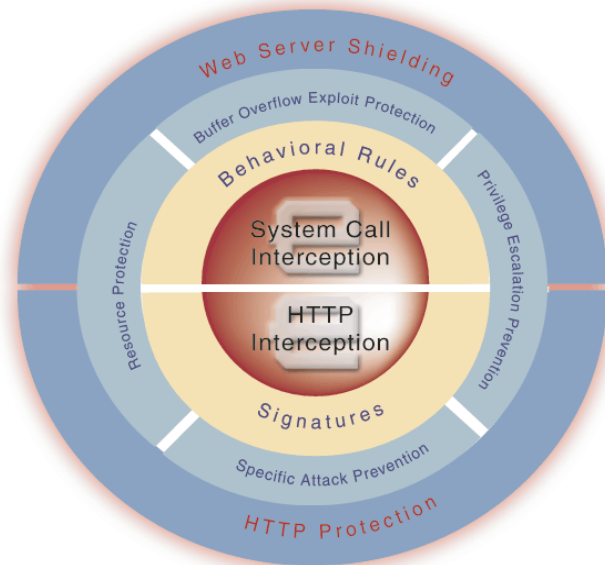
The McAfee Enterccept Solution

McAfee Enterccept® Web Server Edition identifies attacks and prevents unauthorized access to Web server resources before any malicious transactions occur. Building on the patented protection of the Enterccept Standard Edition, the Web Server Edition proactively defends the host by evaluating HTTP requests to the Web server, the application programming interface (API), and the operating system before being processed. Enterccept is the only intrusion prevention solution to create application-specific content interception engines and rules. The Web Server Edition combines award-winning operating system and application protection to deliver an unmatched level of security against known and unknown attacks.

Benefits

Comprehensive

- Reduces criticality of patch deployment for new vulnerabilities and exploits
- Protects IIS, Apache, and iPlanet Web server
- Prevents the corruption or deletion of critical files and directories
- Active, automatic policy enforcement that requires no end-user intervention
- Preserves Web site availability



McAfee Enterccept's HTTP protection, plus Web Server Shielding, delivers defense in depth for critical Web servers.

Accurate

- Powerful combination of behavioral rules and signatures protects against *zero-day* attacks like buffer overflow exploits and reduces false positives
- Process firewall enforces policies with granular packet filter and application layer firewall
- Preconfigured, customizable rules and signatures reduce false positives thus freeing up valuable security staff

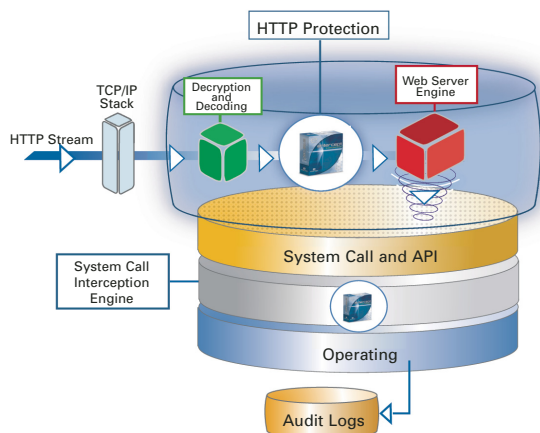
Scalable

- Configure and manage thousands of agents with a single management server
- Optional agent deployment and monitoring via McAfee ePolicy Orchestrator® 3.5 (Q3 2004)
- Silent install/update with no reboot required
- Protects Web servers running on Windows® and Solaris
- Customizable levels of protection, from logging to blocking

How Enterccept Web Server Edition Works

Each centrally managed Web Server agent ships with fully configured default policy templates for protection out of the box. The agent also contains powerful customization features, which allow organizations to create custom policies and tune them for their unique environments to further reduce false positives. Agents automatically retrieve encrypted and authenticated updates from the management system.

The agent examines specific system calls and API calls (both of which are used to by all applications to request services from the operating system). It quickly and efficiently compares its behavioral rules and known attack signatures against a range of information about each call (e.g., the process making the call, the security context in which the process runs, the resource being accessed by the call, etc.) The agent then blocks all calls that would result in malicious behavior.



McAfee Enterecept Web Server Edition agents reside on the server, protecting the operating system and applications.

Features

Web Server Shielding—Web Server Shielding creates a protective shield around Apache, iPlanet, and Microsoft® IIS Web servers. It protects the Web server application and its resources, including data. Enterecept installs the shield after an adaptive auditing process automatically determines the configuration of the server. The shield then provides a protective envelope of operation that prevents both outside penetration and malicious use of the Web server. Intruders cannot deface Web pages or modify operational parameters—even if they manage to gain privileged access to the server.

HTTP Protection—HTTP Protection blocks attacks directed against Apache, iPlanet, or Microsoft IIS Web servers via HTTP requests. A parsing process checks the HTTP stream, identifies malicious requests, and blocks them from reaching the Web server before they can cause damage. This technology prevents popular Web server attacks such as remote code execution, directory traversal, and file disclosure from succeeding even if intruders try to evade detection with application-level encryption such as SSL.

All Features of Enterecept Standard Edition—Including known and unknown attack prevention, buffer overflow

exploit prevention, resource protection, and prevention of privilege escalation.

Process Firewall (Windows Version Only)—The Web Server agent controls network traffic to and from the system through a highly granular packet filter and application layer firewall. It analyzes over 120 IP protocols and can block network attacks like WinNuke and reconnaissance techniques like port scanning in real time.

Fast Path to Prevention Policies Out of the Box—Enterecept easily shifts critical systems into a high level of protection quickly through an intuitive and systematic GUI, which builds *policies through exceptions*. Organizations can switch agents through increasing levels of sensitivity, allowing them to change their security posture incrementally. The result is near-zero false positives and minimal long-term tuning.

McAfee ePO™ 3.5 Deployment and Monitoring—Options for installing, updating, and monitoring agents

Event Aggregation—The Enterecept Management System aggregates similar events and displays as a single line for ease of analysis

Integrated HIPS and NIPS Event Monitoring—IntruShield 2.1 Manager imports and correlates Enterecept agent alerts with IntruShield sensor alerts for a consolidated, system-wide view of security status

Installation Requirements

Windows Web Server

- Windows 2000 Server, Windows 2000 Advanced Server, Windows 2003 Server
- Windows NT 4 Server or Enterprise Server, Service Pack 6a or later
- IIS 4
- IIS 5
- IIS 6

Solaris Web Server

- Solaris 7 (32-bit and 64-bit kernel)
- Solaris 8 (32-bit and 64-bit kernel)
- Solaris 9 (32-bit and 64-bit kernel)
- Apache 1.3.6 and later
- Apache 2.0.42 and later

IPlanet Web Server

- 3.6 (all revisions)
- 4.0
- 4.1
- 6.0

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766 , www.mcafee.com

McAfee® products denote years of experience and commitment to customer satisfaction. The McAfee PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission-critical projects—all with service levels to meet the needs of every customer organization. McAfee Research, a world leader in information systems and security research, continues to spearhead innovation in the development and refinement of all our technologies.

McAfee, Enterecept, ePolicy Orchestrator, ePO, and PrimeSupport are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. Red in connection with security is distinctive of McAfee® brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2004 Networks Associates Technology, Inc. All Rights Reserved. 1-sps-ent-wse-004-0704