

# McAfee Enterccept Standard Multi-Platform Server Agent

## Intrusion Prevention for Critical Systems

### The Challenge

The number of new vulnerabilities and the speed with which attacks can compromise critical systems increase every year, intensifying the risks to system availability, integrity, and confidentiality. Unfortunately, traditional anti-virus and host IDS products are reactive and do nothing to protect against *zero-day* attacks based on newly discovered vulnerabilities. Furthermore, companies of every size are under intense regulatory pressure to ensure the privacy of confidential data and control system and application access.

To ensure proactive system security against today's sophisticated attacks, enterprises need to deploy intrusion prevention that provides multiple layers of protection. McAfee® Enterccept® delivers the most comprehensive, accurate, and scalable host intrusion prevention solution on the market, enabling enterprises to mitigate risk, ensure business availability, and lower total cost of ownership.

### The McAfee Enterccept Solution

Enterccept Standard Multi-Platform Agents protect systems against zero-day and known attacks with patented, award-winning technology. Each centrally managed agent utilizes a powerful combination of intrusion prevention technologies to block attacks with unmatched accuracy:

- Behavioral rules protect against zero-day attacks that target new vulnerabilities—without requiring updates
- Signatures protect the host by accurately identifying known hostile traffic, significantly reducing false positives
- System firewall (Windows® versions only) controls system and application access by blocking traffic into or out of the system based on IP address, protocol, or port

### Benefits

#### Comprehensive

- Blocks zero-day attacks with no updates, significantly reduces criticality of patch deployment for new threats
- Complementary technologies protect availability, integrity, and confidentiality of servers and data
- Intrusion prevention plus system firewall shields critical applications from attack



*McAfee Enterccept utilizes behavioral rules, signatures, and a system firewall to prevent zero-day and known attacks.*

#### Accurate

- *Trusted Applications* allow enterprises to eliminate risk of false positives for critical applications
- Signatures provide specific detailed descriptions of events
- Preconfigured, customizable policies reduce false positives and free up valuable security staff

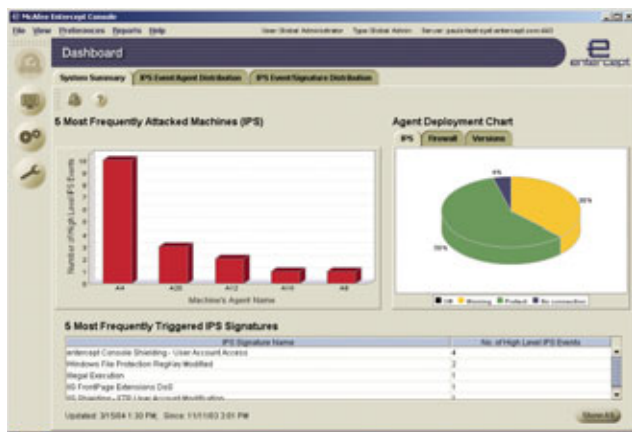
#### Scalable

- Manage up to 10,000 agents with a single manager
- Optional management via McAfee ePolicy Orchestrator® 3.5
- Silent install and updates with no reboot ensure continuous protection
- Customizable levels of protection, from logging to blocking

### How McAfee Enterccept Works

Each agent ships with a fully configured default policy template for protection out of the box. Agents also contain powerful customization features, which allow security professionals to create and tune custom policies for their unique environments to reduce false positives.

The agent examines specific system calls and API calls used by all applications to request services from the OS. 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, etc.) The agent then blocks all calls from malicious behavior or malware.



*Enterecept's management console provides an at-a-glance summary of threats and system status.*

## Features

**Zero-Day Attack Prevention**—Prevents new, previously unknown attacks via powerful behavioral rules. Behavioral rules enforce proper OS and application behavior and block new attacks that violate policies without any updates.

**Buffer Overflow Exploit Prevention**—Patented technology prevents code execution as a result of a buffer overflow. Agents protect critical servers from these dangerous exploits, which account for the largest source of server security vulnerabilities.

**Known Attack Prevention**—Blocks known exploits and prevents damage to servers by matching activity to its extensive database of known attacks. Agents automatically retrieve updates of new attack signatures.

**Resource Protection**—Protects system availability, integrity, and confidentiality by locking down the critical system resources (critical files, settings, registry keys, services, etc.).

**System Firewall (Windows Version Only)**—Blocks network traffic to and from the system through a highly granular packet filter and firewall. It can block traffic into or out of the system based on port, protocol, and IP address.

**Web and Database Server Shielding/Enveloping**—*Shielding* prevents outside penetration and misuse of critical application resources (files, users, registry, etc.). *Enveloping* prevents the protected application from performing malicious activities outside its normal behavior (such as accessing other applications' data).

**HTTP and SQL Protection**—HTTP protection blocks attacks directed against Apache, Sun, or Microsoft® Web servers via unique HTTP parsing engine. SQL protection protects SQL 2000 servers from SQL injection techniques via unique SQL query engine.

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

## System Requirements

### Windows (English, French, and German OS Versions Only)

- Windows 2003 Server
- Windows XP SP2
- Windows 2000 Server and Advanced Server
- Windows NT 4 Server or Enterprise Server, SP 6a
- Microsoft SQL Server 2000
- Microsoft IIS 4, 5, and 6

### Sun

- Solaris 7, 8, and 9 (32-bit and 64-bit kernel)
- Sun ONE/iPlanet 3.6, 4.0, 4.1, and 6.0

### HP-UX

- HP-UX II.0, Ili (64-bit PA-RISC)

### Apache

- Apache 1.3.6 and later, 2.0.42 and later

## McAfee PrimeSupport

The McAfee PrimeSupport® program is essential for making the most of your investment in McAfee System and Network Protection Solutions. McAfee's PrimeSupport team has all the right resources and is ready to deliver your needed service solution. PrimeSupport resources include: delivering authorization to access all available maintenance releases and product upgrades, access to a comprehensive suite of additional online self-support capabilities, live telephone support accessible 24/7/365, available assigned support account managers, and a range of software and hardware support solutions that can be tailored to meet your needs.

**McAfee, Inc.** 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, [www.mcafee.com](http://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, IntruShield, and PrimeSupport are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. The color 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 McAfee, Inc. All Rights Reserved. 1-sps-ese-005-1204