

McAfee Enterccept Standard Edition for Servers and Desktops

Intrusion Prevention for Critical Systems

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.

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 that delivers overlapping and complementary technologies that protect networks and systems from the edge to the core. McAfee® Intrusion Prevention Solutions deliver the most comprehensive, accurate, and scalable threat protection solutions available, helping enterprises mitigate risk, ensure business availability, and lower total cost of ownership.

The McAfee Enterccept Solution

McAfee Enterccept® Standard Edition delivers host intrusion prevention for critical servers and desktops. It protects systems against known and unknown attacks with its patented, award-winning technology. Each centrally managed agent utilizes a powerful combination of behavioral rules and signatures to detect attacks with unmatched accuracy:

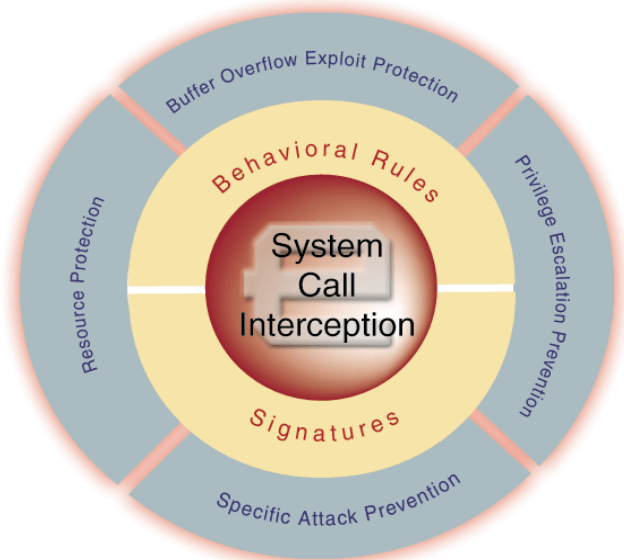
- **Behavioral Rules** protect the host by evaluating all requests to the operating system before they are processed and can protect a system against *zero-day* attacks that target new vulnerabilities for which there is no patch
- **Signatures** protect the host by accurately identifying known hostile content in the data and blocking dangerous payloads before they are processed, significantly reducing false positives

Other host IPS products that rely on just one type of detection technology create the potential for blind spots in their ability to detect attacks. Only Enterccept delivers comprehensive, accurate, and manageable intrusion protection to every server, desktop, and notebook.

Benefits

Comprehensive

- Reduces criticality of patch deployment for new threats
- Protects integrity and privacy of confidential data
- IPS, plus firewall protection, shields mission-critical applications from attack
- Blocks known and zero-day attacks



McAfee Enterccept utilizes both signatures and behavioral rules to prevent known and unknown attacks like buffer overflows and privilege escalation.

Accurate

- Signatures reduce false positives and provide exact, detailed descriptions of events
- Protects against zero-day attacks and vulnerabilities like previously unknown buffer overflow exploits
- Preconfigured, customizable policies reduce false positives thus freeing up valuable security staff

Scalable

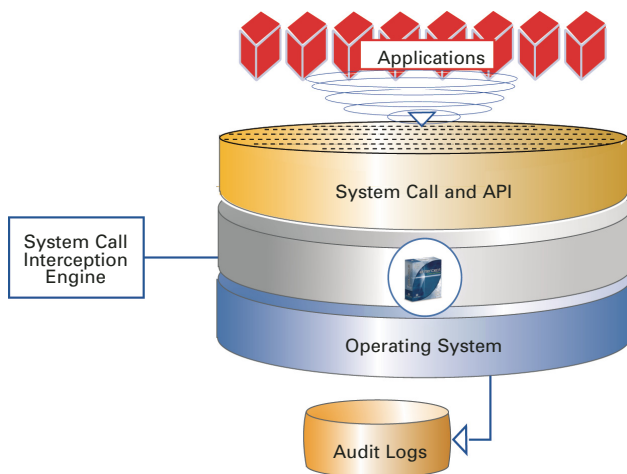
- Manage thousands of agents with a single manager
- Optional agent deployment and monitoring via McAfee ePolicy Orchestrator® 3.5 (Q3 2004)
- Protects Windows®, Solaris, and HP-UX systems with patented, award-winning technology
- No end-user interaction eliminates calls to IT help desk
- Silent install/update with no reboot required
- Customizable levels of protection, from logging to blocking

How Enterccept Standard Edition Works

Each agent ships with a fully configured default policy template for protection out of the box. The agent also contains powerful customization features, which allow

security professionals to create and tune custom policies for their unique environments to reduce false positives. Agents automatically retrieve encrypted and authenticated updates from the management system, ensuring that each agent has the latest policies and new attack signatures.

The agent examines specific system calls and API calls (both of which are used 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, etc.). The agent then blocks all calls from malicious behavior or malware.



Standard Edition agents reside on critical systems, delivering unmatched intrusion prevention for the operating system and applications.

Features

Known Attack Prevention—McAfee Enterecept blocks known exploits and prevent damage to servers by matching activity to its extensive database of known attacks. The agents automatically retrieve updates of new attack signatures.

Zero-Day Attack Prevention—Enterecept prevents new, previously unknown attacks via its powerful behavioral rules. This behavior-based approach enforces proper OS and application behavior and blocks new attacks that violate policies.

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

Resource Protection—Enterecept protects systems from compromise by locking down the critical system resources (critical files, settings, registry keys, services, etc.).

Process Firewall (Windows Version Only)—The agent blocks 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.

Prevention of Privilege Escalation—Enterecept blocks attackers who attempt to gain access to non-privileged accounts and then use various exploits to gain root-level privileges.

Fast Path to Prevention Policies Out of the Box—

Enterecept's intuitive console enables users to move critical systems into a high level of protection quickly by building *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 (English OS Versions Only)

- Windows 2000 Server, Windows Advanced Server 2000, Windows 2003 Server
- Windows NT 4 Server or Enterprise Server, Service Pack 6a
- Windows XP

Solaris

- Solaris 7 (32-bit and 64-bit kernel)
- Solaris 8 (32-bit and 64-bit kernel)
- Solaris 9 (32-bit and 64-bit kernel)

HP-UX

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

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-ese-004-0704