

McAfee Enterccept Desktop Agent

Intrusion Prevention for Notebooks and Desktops

The Challenge

Traditional anti-virus products alone cannot ensure the availability, integrity, and confidentiality of mobile and desktop systems. These systems contain the same proprietary or regulated data found on enterprise servers, yet are often outside the protection of corporate security tools like firewalls and network intrusion prevention systems, inviting security breaches.

Enterprises need to defend their most vulnerable systems with advanced, proactive protection against vulnerability-based threats and attacks. Traditional anti-virus products are reactive and do nothing to block *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.

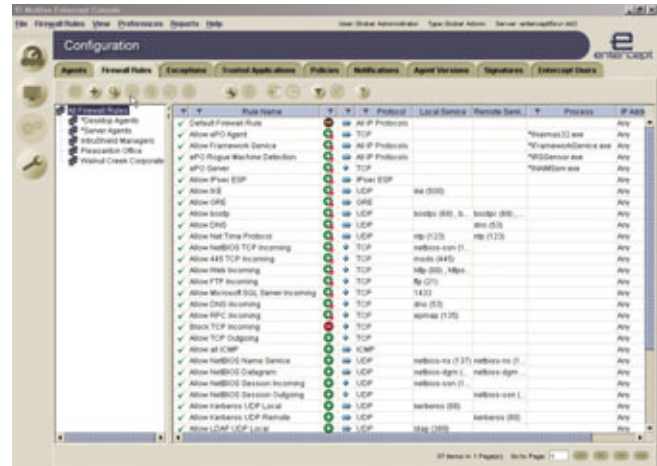
For comprehensive, proactive protection for mobile and desktop systems, organizations need to deploy enterprise-class intrusion prevention. McAfee® Enterccept® delivers the most accurate and scalable host intrusion prevention solution for desktops and mobile systems on the market, enabling enterprises to mitigate risk, ensure business availability, and lower total cost of ownership.

The McAfee Enterccept Solution for Notebooks and Desktops

McAfee Enterccept Desktop Agents protect mobile systems and desktops against zero-day and known attacks with the same patented, award-winning technology found in the Enterccept Server Agents. Enterccept Desktop Agents contain behavioral rules written specifically to protect commonly exploited desktop applications such as Microsoft® Internet Explorer and Outlook from zero-day exploits, without any update.

Each centrally managed agent utilizes a unique combination of three intrusion prevention technologies to block attacks against desktop applications and services with unmatched accuracy:

- **Behavioral Rules** protect against zero-day attacks that target new vulnerabilities or exploits for which there is no patch, reducing the urgency of patch deployment
- **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
- **System Firewall** protects applications and data by blocking traffic into or out of the system based on IP address, protocol, or port



Enterccept is completely invisible to the end user, with granular, customizable policies controlled by administrators.

Benefits

Comprehensive

- Blocks zero-day attacks without updates
- Significantly reduces criticality of patch deployment for new threats
- Protects availability, integrity, and confidentiality of data and systems
- Intrusion prevention plus firewall protection shields mobile and desktop systems from attack

Accurate

- *Trusted Applications* allow enterprises to eliminate false positives for critical applications
- Signatures significantly reduce false positives and provide exact, detailed descriptions of events
- Customizable policies match any environment

Scalable

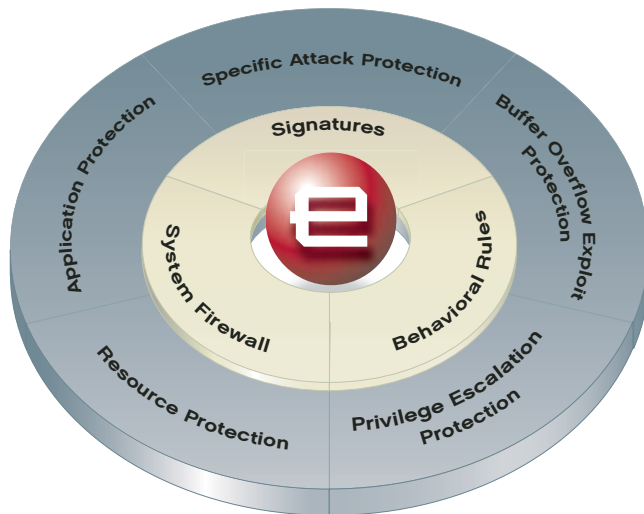
- Manage up to 10,000 agents with a single manager
- Optional management via McAfee ePolicy Orchestrator® 3.5
- Silent install and updates with no reboot or end-user intervention eliminate potential for policy violations
- Automatic response to security events and no local user interface prevent end users from accidentally permitting breaches

How McAfee Enterecept Works

Each Enterecept agent ships with fully configured default policy templates for protection *out of the box*. Agents also contain powerful customization features that allow security professionals to create and tune policies for their unique environments to reduce false positives.

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.

Agents automatically retrieve encrypted and authenticated updates from the management system, ensuring that each agent has the latest policies and new attack signatures.



Enterecept ensures the availability, integrity, and confidentiality of mobile and desktop systems.

Features

Zero-Day Attack Prevention—Enterecept prevents new, previously unknown attacks via its powerful behavioral rules that do not require updates to block unknown attacks. 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, which is the largest source of system security vulnerabilities.

Known Attack Prevention—Detects and blocks known exploits and prevents damage to systems by matching activity to its extensive, automatically updated database of known attacks and provides detailed forensics.

System Firewall—Blocks 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.

Resource Protection—Protects systems from compromise by locking down the critical system resources (files, settings, registry keys, services, etc.) and prevents even users with administrative privileges from bypassing security policies.

Invisible to End-Users—Agents are completely invisible to end users, requiring no interaction during installation, updates, or in response to security events.

Local Access Control—Block access to USB memory drives, floppy drives, etc.

Application Shielding/Enveloping—*Shielding* prevents outside penetration and misuse of Internet Explorer and Microsoft Outlook resources (files, users, registry, etc.). *Enveloping* prevents those applications from performing malicious activities outside their normal behavior (such as accessing other applications' data).

Fast Path to Prevention Policies Out of the Box—Intuitive management console enables organizations to move agents through increasing levels of sensitivity, thus changing their security posture incrementally. The result is near-zero false positives and minimal long-term tuning.

Centralized Management—Management system enables enterprises to enforce security configurations and policies across applications, user groups, and agents to decrease the cost of installation and maintenance.

System Requirements

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

- Windows XP SP2, Windows 2000 Workstation, or Windows NT 4 Workstation

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

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, 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-ent-dta-001-1204