

McAfee Enterccept Standard Edition for Servers

System Intrusion Prevention for Enterprise Servers

The Challenge

Enterprise security becomes harder every day. CERT (Computer Emergency Response Team) reports that the number of reported security incidents is doubling each year. Nearly twice as many vulnerabilities were discovered this year as in the previous year. Attackers are becoming harder to stop with each new exploit technique. Firewalls and perimeter security are no longer enough to protect today's enterprise. Increasingly knowledgeable hackers have discovered ways around firewalls and existing detection systems to launch attacks, such as buffer overflows and worms, directly against servers and applications. The Code Red worm bypassed firewalls and network-based IDS to cause enormous damage. Computer Economics estimates the worldwide economic impact of the Code Red worm to be \$2.62 billion. Multiple forces combine to create a need for a better solution, such as:

- Rapidly increasing number of vulnerabilities
- Advancement of attack techniques
- Inability of yesterday's security solutions to deal with today's new security threats

The McAfee Enterccept Solution

McAfee® Enterccept® meets the enterprise server security needs of today as well as tomorrow, by providing organizations with protection against today's known attacks and possible attacks in the future. Based on patented technology, McAfee Enterccept safeguards the entire server by preventing known and unknown malicious attacks. By blocking these attacks, McAfee Enterccept significantly decreases downtime, reduces security-related costs, and protects critical assets. McAfee Enterccept proactively protects the host by evaluating requests to the operating system before they are processed. Unlike other security solutions, McAfee Enterccept uses a combination of both behavioral rules and signatures to prevent both known and unknown attacks, rather than merely detecting and reporting them after they occur. McAfee Enterccept is the proven leader in intrusion prevention software.

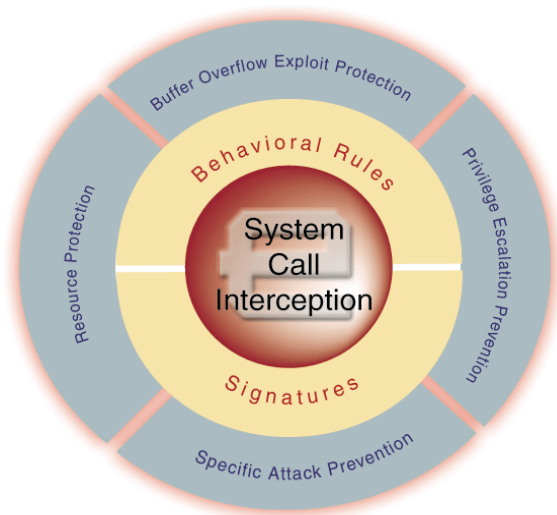
Benefits

Decreases Downtime

- Prevents attacks, rather than simply detect them
- Protects against buffer overflow exploits

Reduces Security-Related Costs

- Minimizes recovery costs associated with downtime
- Reduces need for specialized personnel



McAfee Enterccept's system call interception capability utilizes both signatures and behavioral rules to prevent buffer overflows, privilege escalation, and other known and unknown attacks.

Protects Assets

- Protects customer data
- Shields applications
- Safeguards reputation

How McAfee Enterccept Works

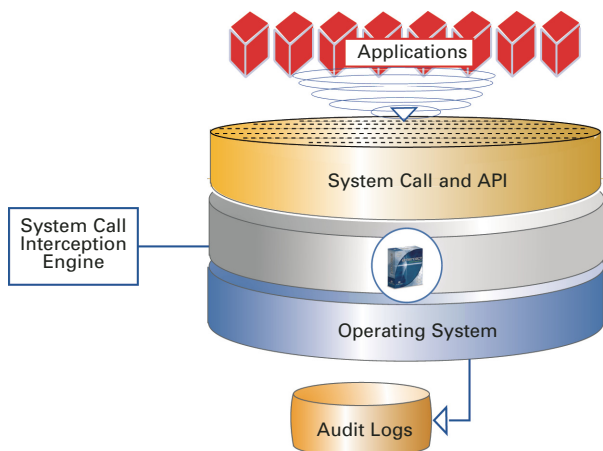
McAfee Enterccept combines several core technologies to protect enterprise servers. Using a distributed architecture, McAfee Enterccept Agents are installed on each server in an enterprise. These agents intercept specific system calls and API calls (both are used by all applications to request services from the operating system) and block calls that would result in malicious behavior. McAfee Enterccept determines, among other things, the process making the call, the user making the call, the resource accessed by the call, and the user permissions related to the call. Using this information, calls are matched against the appropriate behavioral rules and known attack signatures.

McAfee Enterccept then blocks calls that attempt malicious behavior or match any specific attack signature. All preventive activity is logged to the McAfee Enterccept Management System for review and reporting.

The policy database ships with a fully configured default template incorporating powerful customization features, allowing false-positives to be virtually eliminated. The default policy ensures rapid deployment.

Agents are deployed on a per-server basis and are controlled and updated via the McAfee Enterecept Management System. Agents are completely self-contained, protective units and not reliant on the management system to function. This approach improves both reliability and security.

Agents retrieve updates from the management system, including code updates and new attack definitions. RC4 encryption and Diffie-Hellman key exchange agreements are used for all communications.



McAfee Enterecept resides on the server, protecting the operating system and applications.

Known Attack Prevention—Using its extensive database of known attacks, McAfee Enterecept can block known exploits and prevent damage to servers. New attacks are constantly added to the database, allowing McAfee Enterecept to specifically identify attacks by name.

Unknown Attack Prevention—McAfee Enterecept detects and prevents new, previously unknown attacks via its powerful behavioral rules. This behavior-based approach enforces proper OS and application behavior and blocks new attacks, since attacks violate the pre-defined appropriate behaviors. By combining this behavioral protection with McAfee Enterecept's specific attack prevention, servers are protected against both known and unknown threats.

Buffer Overflow Exploit Prevention—McAfee Enterecept's patented technology prevents code execution as a result of a buffer overflow. Buffer overflows account for over 60 percent of CERT advisories and are the largest source of server security vulnerabilities. McAfee Enterecept protects servers from these dangerous exploits.

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

Prevention of Privilege Elevation—Many attackers gain access to a non-privileged account and then use various exploits to gain root-level privileges. McAfee Enterecept blocks these exploits and ensures that attackers do not increase their privilege level.

SecureSelect—McAfee Enterecept provides three security modes: SecureSelect Warning Mode, SecureSelect Protection Mode, and SecureSelect Vault Mode. Each mode provides higher security than the previous mode. Customers begin McAfee Enterecept deployments in Warning Mode, and then progress to Protection Mode and Vault Mode as they tune and tighten their McAfee Enterecept installation.

Features

- Proactive attack response allows McAfee Enterecept to block malicious actions before any damage is done
- Secure, self-contained agents
- Pre-configured policy template, including full customization options
- Ability to prevent malicious access to system resources
- Complements existing security infrastructure

Installation Requirements

Agent—Windows® (English OS versions only)

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

Agent—Solaris

- Solaris 2.6 (32-bit kernel)
- Solaris 7 (32-bit and 64-bit kernel)
- Solaris 8
- Solaris 9

Agent—Unix

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

McAfee Security 3965 Freedom Circle, Santa Clara, CA 95054, 888.VIRUSNO (888.847.8766), www.mcafeesecurity.com

Network Associates® products denote years of experience and commitment to customer satisfaction. The 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, continues to spearhead innovation in the development and refinement of all our technologies.

Network Associates, McAfee, and Enterecept are registered trademarks or trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. Sniffer® brand products are made only by Network Associates, Inc. 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-002-0304