

McAfee Enterccept Management System

Enterprise-Class Management for McAfee Enterccept Intrusion Prevention

The Challenge

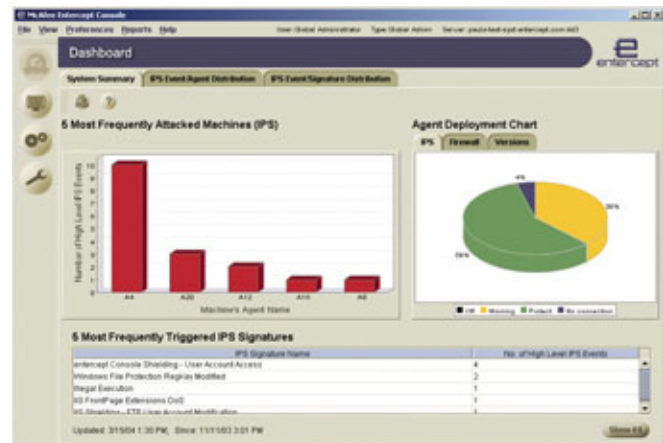
Enterprises face the daunting task of protecting today's geographically dispersed, heterogeneous networks. They must deal with sophisticated new hybrid attacks that use multiple vectors to breach the security infrastructure. They must also adhere to regulatory requirements to protect the integrity and confidentiality of the data within their critical systems and applications. And, they must document the value of their security investment to upper management.

Organizations need to deploy a security management system that can powerfully manage thousands of agents, provide unmatched threat protection, and minimize the time required to administer the system. McAfee® Enterccept® 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 Enterccept Solution

The Enterccept Management System delivers comprehensive, enterprise-class management for Enterccept's intrusion prevention agents. The Management System provides a scalable, robust, and easy-to-use management infrastructure, able to control up to 10,000 agents per management server.

All Enterccept agents (Desktop and Server) share the common management infrastructure provided by the Management System. Enterprises can easily leverage security configurations and policies across applications, user groups, and agents to decrease the cost of installation and maintenance. Security administrators can also import and export configurations across multiple management servers, ensuring consistent policy enforcement. Enterccept enables cross platform protection of Windows®, Solaris, and HP-UX platforms, delivering consistent, reliable, host intrusion prevention security for today's heterogeneous server environments.



The McAfee Enterccept Management System provides a summary dashboard to display an overall view of system status.

How Enterccept Management System Works

The Enterccept Management System consists of the highly scalable management server and console. The management server acts as the intermediate layer between the Enterccept agents and the console, coordinating communications and housing the event and configuration database. Multiple consoles in geographically distributed locations can simultaneously connect to the management server to administer and monitor the agents.

As agents detect and block attacks, they send relevant information to the Enterccept management server. The server forwards relevant data to consoles as well as storing it in the central SQL database. The console aggregates similar events to minimize the amount of raw data displayed and provide a summary view of the overall system status in a unique dashboard view.

The Management System provides a broad set of response and notification options, including e-mail alerts, pager alerts, SNMP traps, and spawning a process. The console communicates with the agents using encrypted and authenticated channels. The Enterccept Management System actively enforces enterprise security policies with its award-winning intrusion prevention technology, blocking attacks while providing unmatched reporting and data analysis features.

Benefits

Comprehensive

- Reduces criticality of patch deployment for new threats
- Blocks known and *zero-day* attacks
- Protects integrity and privacy of confidential data
- Active, automatic policy enforcement that requires no end-user intervention
- Protects Windows, Solaris, and HP-UX systems with patented, award-winning technology
- Application Shielding/Enveloping—*Shielding* prevents outside penetration and misuse of Web servers, database servers, and desktop application resources (files, data, users, registry, etc.). *Enveloping* prevents those applications from performing malicious activities outside their normal behavior (such as accessing other applications' data)

Accurate

- Powerful combination of behavioral rules, signatures, and system firewall protects against zero-day attacks like buffer overflow exploits and reduces false positives
- Wizards create custom rules and signatures to match any environment
- No end-user interaction eliminates calls to IT help desk
- Searching, filtering, and grouping allows administrators to identify trends and uncover potential threats

Scalable

- Manage thousands of agents with a single manager
- Optional agent deployment and monitoring via McAfee ePolicy Orchestrator® 3.5
- Leverage configurations across applications, user groups, or agents
- Silent install/update with no reboot required
- Event aggregation consolidates repeated events in a single console entry
- Console audit trail records all configuration changes made by administrators
- Customizable levels of protection, from logging to blocking

System Requirements

Recommended Configuration

Management Server

- 1.5GHz Pentium IV or better
- 1GB RAM
- 20GB hard disk space
- Windows 2003 Server
- Windows 2000 Server or Advanced Server (SP 2 or later)
- SQL Server 2000 (SP 2 or later)
- Static IP Address
- No other applications installed
- TCP Ports 443 and 5005 available (443 used by default but can be changed)

Console

- 800MHz Pentium III or better
- 256MB RAM
- 100MB free hard disk space
- Windows XP SP 2
- Windows 2000 Professional, Server or Advanced Server
- Windows NT 4 Server or Workstation, SP 6a

McAfee PrimeSupport

McAfee has pursued a strategy of providing best-of-breed technology for each type of security and performance management application—but the Protection-in-Depth™ Strategy is more than just deploying and implementing best-of-breed solutions today. Prevention is certainly our first priority, but inevitably, you will have to react to a problem.

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 Right Reserved. 1-sps-ent-mgt-003-1204