

McAfee Enterccept Management-System

Enterprise-Class-Management für Intrusion Prevention von McAfee Enterccept

Die Herausforderung

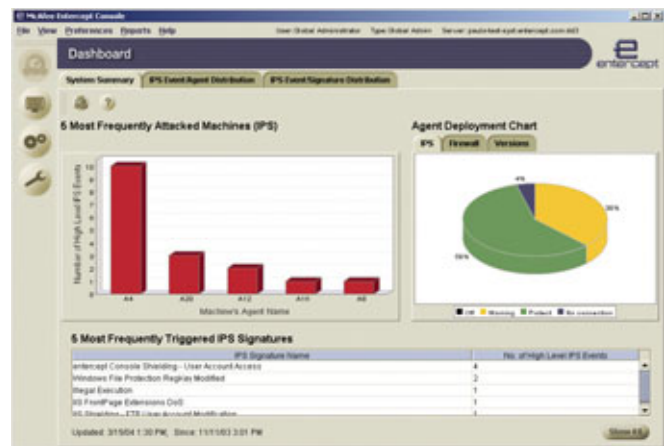
Unternehmen müssen die gewaltige Aufgabe bewältigen, geografisch verteilte, heterogene Netzwerke zu schützen. Sie müssen raffinierte neue komplexe Angriffe bewältigen, die mithilfe zahlreicher Vektoren in die Sicherheitsinfrastruktur eindringen. Sie müssen zudem die gesetzlichen Bestimmungen zum Schutz der Integrität und Vertraulichkeit der Daten in ihren geschäftskritischen Systemen und Anwendungen erfüllen. Und nicht zuletzt müssen sie der Unternehmensführung Daten liefern, um den Wert ihrer Investitionen in die Sicherheit zu belegen.

Unternehmen benötigen ein Security Management-System, das mehrere Tausend Agenten effizient verwalten, exzellenten Angriffsschutz bieten und den Verwaltungsaufwand minimieren kann. McAfee® Enterccept® Intrusion Prevention ist eine der umfassendsten, genauesten und skalierbarsten Angriffsabwehrlösungen auf dem Markt. Sie hilft Unternehmen, das Angriffsrisiko zu verringern, die Verfügbarkeit aufrechtzuerhalten und die Gesamtbetriebskosten zu reduzieren.

Die Enterccept-Lösung

Das Enterccept Management-System bietet ein umfassendes Enterprise-Class Management für Enterccept Intrusion Prevention-Agenten. Das Management-System stellt eine skalierbare, stabile und benutzerfreundliche Management-Infrastruktur zur Verfügung, in der ein Management-Server bis zu 5.000 Agenten verwalten kann.

Alle Enterccept-Agenten (Standard, Webserver und Database Edition) nutzen gemeinsam die vom Enterccept Management-System bereitgestellte Management-Infrastruktur. Unternehmen können Sicherheitskonfigurationen und -richtlinien problemlos über mehrere Anwendungen, Benutzergruppen und Agenten hinweg nutzen und dadurch die Installations- und Wartungskosten senken. Sicherheitsadministratoren können Konfigurationen über mehrere Management-Server hinweg importieren bzw. exportieren und so eine konsistente Durchsetzung der Sicherheitsrichtlinien gewährleisten. Der plattformübergreifende Schutz umfasst die Betriebssysteme Windows®, Solaris und HP-UX. Dadurch schafft Enterccept eine konsistente, zuverlässige Host-basierte Angriffsabwehr für moderne heterogene Serverumgebungen.



Das McAfee Enterccept Management-System zeigt den Systemstatus auf einem Dashboard in einer Gesamtdarstellung an.

Funktionsweise des Enterccept Management-Systems

Das Enterccept Management-System besteht aus einem hochskalierbaren Management-Server und einer Konsole. Der Management-Server dient als Zwischenschicht zwischen den Enterccept-Agenten und der Konsole. Er regelt die Kommunikation und beherbergt die Ereignis- und Konfigurationsdatenbank. Mehrere Konsolen an geografisch verteilten Standorten können sich gleichzeitig am Management-Server anmelden und die Agenten verwalten und überwachen.

Wenn Agenten Angriffe entdecken und blockieren, senden sie wichtige Informationen an den Enterccept Management-Server. Vom Server aus werden diese Informationen an Konsolen weitergeleitet und in der zentralen SQL-Datenbank gespeichert. Auf der Konsole werden ähnliche Vorfälle zusammengefasst, um die Menge der angezeigten Daten zu reduzieren und den Gesamtsystemstatus auf einem Dashboard einheitlich und zusammengefasst darzustellen.

Das Management-System bietet eine große Auswahl an Optionen zur Ergreifung von Gegenmaßnahmen und Meldung von Angriffen, z. B. Alarm mittels E-Mail oder Pager, SNMP-Traps und Erzeugen eines Prozesses. Die Konsole kommuniziert mit den Agenten über verschlüsselte und authentifizierte Kanäle. Auf der Basis der mehrfach ausgezeichneten Intrusion Prevention-Technologie setzt das Enterccept Management-System Sicherheitsrichtlinien im Unternehmen aktiv durch. Es blockiert Angriffe und stellt richtungsweisende Funktionen für Reporting und Datenanalyse bereit.

Vorteile

Umfassend

- Reduziert bei neuen Gefahren die Dringlichkeit der Patch-Implementierung
- Blockiert bekannte und sogenannte *Zero-Day* Angriffe (Angriffe auf eine neue, bisher unbekannte Sicherheitslücke)
- Gewährleistet Integrität und Datenschutz für vertrauliche Daten
- Aktive, automatische Richtliniendurchsetzung ohne Eingreifen des Endbenutzers
- Schützt die Betriebssysteme Windows, Solaris und HP-UX mit patentierter, mehrfach ausgezeichnete Technologie
- Anwendungsspezifische Funktionen schützen SQL 2000 Datenbankserver sowie IIS- und Apache-Server vor Missbrauch

Genau

- Verhaltensregeln in Verbindung mit Signaturen bieten einen sicheren Schutz vor Zero-Day Angriffen wie z. B. Angriffe, die einen Buffer Overflow erzeugen, und reduzieren das Auftreten von falschen Alarmmeldungen
- Es gibt Assistenten zur Erstellung benutzerdefinierter Regeln und Signaturen, die an die jeweilige Umgebung angepasst sind
- Es ist kein Eingreifen des Benutzers erforderlich, d. h. Anrufe beim IT-Helpdesk entfallen
- Die Optionen Suchen, Filtern und Gruppieren ermöglichen die Identifizierung von Trends und das Aufspüren potenzieller Gefahren

Skalierbar

- Verwaltung von mehreren Tausend Agenten mit einem einzigen Manager
- Optionale Implementierung und Überwachung von Agenten mit dem McAfee ePolicy Orchestrator® 3.5 (ab 3. Quartal 2004 verfügbar)

- Optimale Nutzung von Konfigurationen über Anwendungen, Benutzergruppen oder Agenten hinweg
- Installation bzw. Update im Hintergrund, kein Neustart erforderlich
- Ereignis-Aggregation fasst gleiche Ereignisse zu einem einzigen Eintrag auf der Konsole zusammen
- In einem Überwachungsprotokoll wird jede Konfigurationsänderung eines Administrators aufgezeichnet
- Individuell anpassbare Schutzebenen, von Protokollierung bis Blockierung

Systemanforderungen

Empfohlene Konfiguration

Management-Server

- 1,5GHz Pentium IV oder höher
- 1GB Arbeitsspeicher
- 20GB Festplattenspeicher
- Windows 2000 Server oder Advanced Server (SP 2 oder höher)
- SQL Server 2000 (SP 2 oder höher)
- Statische IP-Adresse
- Keine anderen Anwendungen installiert
- TCP Ports 443 und 5005 verfügbar (443 Standardport, kann aber geändert werden)

Konsole

- 800MHz Pentium III oder höher
- 256MB Arbeitsspeicher
- 100MB freier Festplattenspeicher
- Windows NT 4 Server oder Workstation, SP 6a
- Windows 2000 Professional Server oder Advanced Server
- Windows XP SP 1

McAfee GmbH

Ohmstraße 1, 85716 Unterschleißheim, Telefon: 089 – 37 07 0 | Luisenweg 40, 20537 Hamburg, Telefon: 040 – 25 31 0
Regus Center – Twin Tower, Wienerbergstraße 11/12 A, A-1100 Wien, Telefon: +43-(0)1-994 60 6202 | www.mcafee.de

Die Produkte von McAfee® zeichnen sich durch jahrelange Erfahrung und Engagement im Bereich Kundenzufriedenheit aus. Das PrimeSupport®-Team besteht aus hoch qualifizierten Support-Technikern, die Ihnen mit maßgeschneiderten Lösungen und detaillierter technischer Unterstützung bei der Verwaltung geschäftskritischer Projekte zum Erfolg verhelfen. Der Service-Level wird dabei jeweils an die Bedürfnisse des einzelnen Unternehmens angepasst. McAfee Research, marktführend in der Informationssysteme- und Sicherheits-Forschung, führt die bahnbrechenden Innovationen bei der Entwicklung und Verbesserung unserer Technologien fort.

McAfee, Enterecept, ePolicy Orchestrator, und PrimeSupport sind eingetragene Marken oder Marken von McAfee, Inc. und/oder seinen Niederlassungen in den USA und/oder anderen Ländern. Die Farbe Rot in Verbindung mit Sicherheit steht unverkennbar für alle McAfee® Markenprodukte. Alle anderen eingetragenen und nicht eingetragenen Marken in diesem Dokument sind Eigentum ihrer jeweiligen Besitzer. © 2004 Networks Associates Technology, Inc. Alle Rechte vorbehalten. 1-sps-ent-mgt-gr-001-0704