

# McAfee Enterccept Web Server Edition

## Intrusion Prevention für Webserver

### Die Herausforderung

Die Anzahl neuer Sicherheitslücken und die Geschwindigkeit und Raffinesse, mit der diese Sicherheitslücken angegriffen und ausgenutzt werden, wächst jedes Jahr und erhöht die Risiken für die Sicherheit von Unternehmen. Neuartige komplexe Angriffe, die mithilfe zahlreicher Vektoren in die Sicherheitsinfrastruktur von Unternehmen eindringen, müssen abgewehrt werden.

Webserver abzusichern, ist eine schwierige Aufgabe. Sie müssen von außen zugänglich sein, doch damit sind sie auch für Angreifer auf der ganzen Welt leicht erreichbar.

Leider arbeiten herkömmliche IDS-Tools reaktiv, die Angreifer sind also immer einen Schritt voraus. Zur Gewährleistung umfassender, proaktiver Sicherheit benötigen Unternehmen ein mehrstufiges Sicherheitskonzept mit ineinandergreifenden und sich ergänzenden Technologien, die Netzwerke und Systeme von der Peripherie bis zum Kern schützen. McAfee® 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 McAfee Enterccept-Lösung

Der McAfee Enterccept® Web Server Edition identifiziert Angriffe, wehrt unautorisierte Zugriffe auf Webserver-Ressourcen ab und verhindert dadurch bösartige Transaktionen. Auf der Basis der patentierten Schutzfunktionen der Enterccept Standard Edition schützt die Web Server Edition den Host proaktiv. Dazu werden HTTP-Aufrufe an den Webserver, die Anwendungsprogrammchnittstelle (API) und das Betriebssystem zunächst evaluiert und erst dann verarbeitet. Enterccept ist die einzige Intrusion Prevention-Lösung, die anwendungsspezifische Programme und Regeln zur Inhaltsüberwachung erstellt. Die Web Server Edition kombiniert die mehrfach ausgezeichneten Schutzfunktionen für Betriebssystem und Anwendungen und schafft dadurch eine exzellente Sicherheitsstufe gegen bekannte und unbekannte Angreifer.

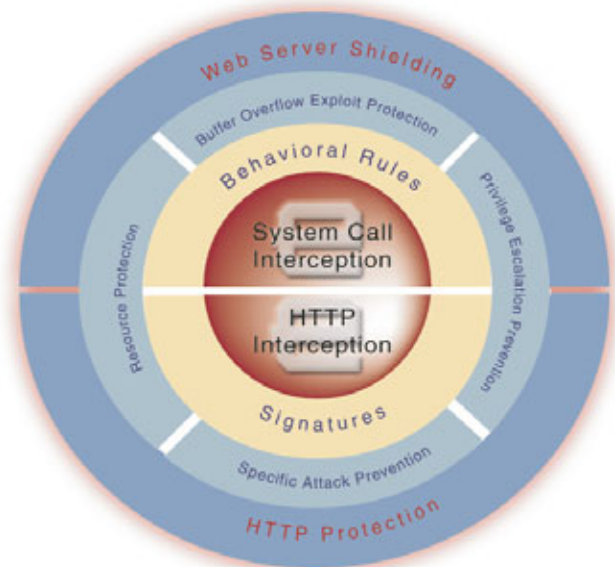
### Vorteile

#### Umfassend

- Reduziert bei neuen Sicherheitslücken und Gefahren die Dringlichkeit der Patch-Implementierung
- Schützt IIS-, Apache- und iPlanet-Webserver
- Verhindert die Zerstörung oder Löschung geschäftskritischer Dateien und Verzeichnisse
- Aktive, automatische Richtliniendurchsetzung ohne Eingreifen des Endbenutzers
- Sichert die Verfügbarkeit der Website

#### Genau

- Verhaltensregeln in Verbindung mit Signaturen bieten einen sicheren Schutz vor sogenannten *Zero-Day* Angriffen (Angriffe auf eine neue, bisher unbekannt



*Durch HTTP- und Webserver-Schutz von McAfee Enterccept werden Angriffe auf geschäftskritische Webserver erfolgreich abgewehrt.*

Sicherheitslücke) wie z. B. Angriffe, die einen Buffer Overflow erzeugen und reduzieren das Auftreten von falschen Alarmmeldungen

- Prozessbasierte Firewall setzt Richtlinien über einen granularen Paketfilter und eine Firewall auf der Anwendungsebene durch
- Vorkonfigurierte, individuell anpassbare Regeln und Signaturen verringern das Auftreten von Fehlalarmen und die Sicherheitsspezialisten können sich wieder auf ihre eigentlichen Aufgaben konzentrieren

#### Skalierbar

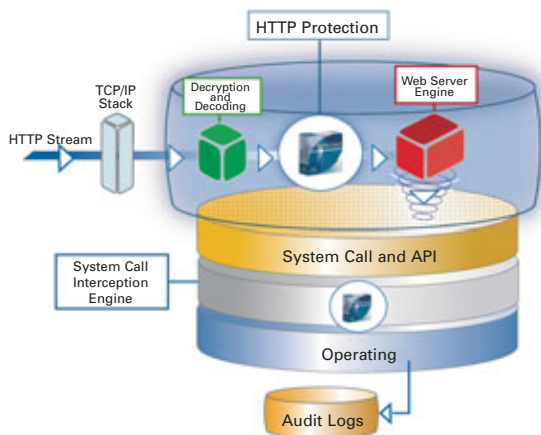
- Konfigurieren und Verwalten von mehreren Tausend Agenten mit einem einzigen Management-Server
- Optionale Implementierung und Überwachung von Agenten mit McAfee ePolicy Orchestrator® 3.5 (3. Quartal 2004)
- Installation bzw. Update im Hintergrund, kein Neustart erforderlich
- Schützt Webserver unter Windows® und Solaris
- Individuell anpassbare Schutzebenen, von Protokollierung bis Blockierung

### Funktionsweise der Enterccept Web Server Edition

Jeder zentral verwaltete Web Server-Agent wird mit vollständig konfigurierten Standard-Sicherheitsrichtlinien geliefert, die als Vorlage dienen und ohne weitere Konfigurationseinstellungen verwendet werden können. Der Agent stellt auch leistungsfähige Anpassungsfunktionen zur Erstellung eigener Sicherheitsrichtlinien bereit, die ganz auf die spezifischen Anforderungen einer Umgebung zugeschnitten werden können. Auf diese Weise lassen sich die falschen Einstufungen weiter verringern. Agenten rufen automatisch

verschlüsselte und authentifizierte Updates aus dem Management-System ab.

Der Agent überprüft bestimmte System- und API-Aufrufe (diese werden von allen Anwendungen zur Anforderung von Diensten des Betriebssystems verwendet). Er gleicht dann schnell und effizient seine Verhaltensregeln und bekannten Angriffssignaturen mit den verfügbaren Informationen zu jedem Aufruf ab (z. B. aufrufender Prozess, Sicherheitskontext des Prozesses, aufgerufene Ressource usw.) und blockiert dann alle Anfragen, die schädigendes Verhalten auslösen würden.



**Die McAfee Enterecept Web Server Edition-Agenten befinden sich auf dem Server und schützen dort Betriebssystem und Anwendungen.**

## Features

**Webserver-Abschirmung** — Bei der Abschirmung des Webserver wird ein Schutzschild um Apache-, iPlanet- und Microsoft® IIS-Webserver errichtet. Er schützt die Webserver-Anwendung und die zugehörigen Ressourcen, einschließlich der Daten. Enterecept installiert den Schutzschild, nachdem ein adaptiver Auditing-Prozess automatisch die Konfiguration des Servers ermittelt hat. Anschließend wird ein Schutzschild erzeugt, das ein Eindringen von außen und den Missbrauch des Datenbankservers unmöglich macht. Eindringlinge können selbst dann keine Webseiten manipulieren oder Betriebsparameter ändern, wenn sie sich die erforderlichen Berechtigungen für den Zugriff auf den Server verschaffen.

**HTTP-Schutz** — Dieser Mechanismus blockiert Angriffe, die mittels HTTP-Anfragen auf Apache-, iPlanet- oder Microsoft IIS-Webservern gestartet werden. Ein Parsing-Prozess überprüft den HTTP-Datenstrom, identifiziert böswillige Anfragen und verhindert, dass sie den Webserver erreichen und dort Schaden anrichten. Auf diese Weise lassen sich gängige Attacken auf Webserver abwehren, z. B. Ausführung von externem Code, Verzeichniswechsel und Preisgabe von Dateiinhalten. Dieser Schutz greift auch dann, wenn Eindringlinge versuchen, mithilfe einer Verschlüsselung auf Anwendungsebene z. B. SSL, eine Entdeckung zu verhindern.

## 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](http://www.mcafee.de)

**Die Enterecept Web Server Edition umfasst alle Funktionen der Enterecept Standard Edition** — Wie z. B. Abwehr bekannter und unbekannter Angriffe, Schutz vor Buffer Overflows, Ressourcenschutz und Verhinderung einer Berechtigungseskalation.

**Prozess-Firewall (nur Windows-Version)** — Der Web Server-Agent regelt den Netzwerkverkehr zum und vom System über einen hochgranularen Paketfilter und eine Firewall auf der Anwendungsebene. Er analysiert mehr als 120 IP-Protokolle und kann Netzwerkangriffe wie z. B. WinNuke und Ausspähungstechniken wie z. B. Port-Scanning in Echtzeit blockieren.

**Schnellster Weg um Abwehrrichtlinien ohne weitere Anpassung zu Erstellen** — Über eine intuitive und systematische grafische Benutzeroberfläche (GUI) können Richtlinien durch Ausnahmen erstellt und geschäftskritische Systeme problemlos auf eine höhere Sicherheitsstufe gehoben werden. Unternehmen können für Agenten immer höhere Sensitivitätsstufen festlegen, um so ihr Schutz- und Abwehrverhalten schrittweise zu ändern. Auf diese Weise lassen sich Fehlalarme nahezu eliminieren und langfristige Anpassungen auf ein Minimum beschränken.

**Implementierung und Überwachung mit dem McAfee ePO™ 3.5** — Optionen zur Installation, Aktualisierung und Überwachung von Agenten.

**Ereignisaggregation** — Das Enterecept Management-System fasst ähnliche Ereignisse zu einem einzigen Eintrag zusammen, um die Analyse zu vereinfachen.

**Ereignisüberwachung durch Integration von HIPS und NIPS** — Der IntruShield® 2.1 Manager importiert und korreliert die Alarme der Enterecept-Agenten mit den Alarmen der IntruShield-Sensoren, um die Anzeige des Sicherheitsstatus für das gesamte System zu vereinheitlichen.

## Installationsvoraussetzungen

### Windows Webserver

- Windows 2000 Server, Windows 2000 Advanced Server, Windows 2003 Server
- Windows NT 4 Server oder Enterprise Server, Service Pack 6a oder höher
- IIS 4
- IIS 5
- IIS 6

### Solaris Webserver

- Solaris 7 (32-Bit und 64-Bit Kernel)
- Solaris 8 (32-Bit und 64-Bit Kernel)
- Solaris 9 (32-Bit und 64-Bit Kernel)
- Apache 1.3.6 und höher
- Apache 2.0.42 und höher

### iPlanet Web Server

- 3.6 (alle Versionen)
- 4.0
- 4.1
- 6.0

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 Sicherheitsforschung, führt die bahnbrechenden Innovationen bei der Entwicklung und Verbesserung unserer Technologien fort.

McAfee, Enterecept, ePolicy Orchestrator, ePO, IntruShield, 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-wse-gr-001-0704