

# McAfee Host Intrusion Prevention for Desktop

Präventiver Schutz für Endgeräte, Daten und Anwendungen

## Hauptvorteile

### Besserer Schutz

- Durchsetzung des breitesten Spektrums an IPS- und Zero-Day-Schutzmaßnahmen auf allen Ebenen: Netzwerk, Anwendung und Ausführung

### Geringere Kosten

- Verringerung des Zeit- und Kostenaufwands mit einer leistungsstarken, zentralen Konsole für Ausbringung, Verwaltung, Reporting und Audits von Vorfällen, Richtlinien und Agenten
- Weniger häufige und dringliche Endgeräte-Patches

### Einfachere Einhaltung

- Verwaltung der Einhaltung mit leicht verständlichen, umsetzbaren Ansichten, Workflows, Event-Monitoring und Reporting für prompte und gründliche Untersuchungen und Analysen

## Die Herausforderung

Die Verwaltung der Sicherheit und die Steuerung der Internetverbindung für Desktops und Laptops in Ihrem Unternehmen kann große Probleme bereiten. Aufgrund der wachsenden Anzahl von aktiven profitorientierten Internetkriminellen gab es in der ersten Hälfte des Monats Januar 2008 mehr neue Bedrohungen als im ganzen Jahr 2007.<sup>1</sup> IT-Sicherheitsteams stehen unter immensem Druck, alle Endgeräte vor der schnell zunehmenden Anzahl komplexer Bedrohungen zu schützen. Und da mehr als 32 % der Angriffe innerhalb von drei Tagen nach Entdeckung der betreffenden Schwachstelle erfolgen<sup>2</sup>, sind Unternehmen gefährdet, denn bis zur Implementierung der Endgeräte-Patches können 30 oder mehr Tage vergehen. Unternehmen benötigen Schutz vor Zero-Day-Bedrohungen, um die Sicherheit und Zeit für die ordnungsgemäße Priorisierung, Planung, Erprobung und Implementierung von Patches zu erhalten.

Eine der größten Herausforderungen für IT-Manager besteht darin, unternehmenskritische Endgeräte erfolgreich vor bekannten und unbekanntem Angriffen zu schützen, bevor diese Schaden anrichten. Virenschutz allein reicht nicht aus, da Angriffe auf Schwachstellen schneller erfolgen und immer komplexer werden. Die Lösung besteht darin, eine präventive Sicherheitsstrategie zu implementieren, die verhindert, dass Angriffe überhaupt stattfinden. Mit einem präventiven Sicherheitsansatz für Endgeräte können IT-Manager sicherstellen, dass alle Endgeräte und vertraulichen Daten geschützt sind und die Geschäftskontinuität aufrechterhalten wird.

## McAfee Host Intrusion Prevention for Desktop

Als integraler Bestandteil von McAfee® Total Protection (ToPS) for Endpoint schützt McAfee Host Intrusion Prevention (Host IPS) for Desktop Endgeräte vor bekannten und Zero-Day-Bedrohungen durch die Kombination von signatur- und verhaltensorientiertem Intrusion Prevention-Schutz mit einer zustandsgesteuerten Desktop Firewall und Anwendungskontrolle. McAfee Host IPS reduziert die Häufigkeit und Dringlichkeit von Patches, erhält die Geschäftstätigkeit und Mitarbeiterproduktivität, schützt die Vertraulichkeit von Daten und vereinfacht die Einhaltung von gesetzlichen Bestimmungen.

## Verwaltbarkeit für Unternehmen

McAfee ePolicy Orchestrator® (ePO™) ist die branchenführende Plattform für die Verwaltung der Systemsicherheit, die Unternehmen einen koordinierten, präventiven Schutz vor Bedrohungen und Angriffen bietet. Mit ePO als Kern der McAfee-Lösungen für das Sicherheitsrisiko-Management (SRM) können Administratoren von einer zentralen, webbasierten Konsole aus rund um die Uhr das Risiko unberechtigter, regelwidriger Systeme mindern, den Schutz aktuell halten, Sicherheitsrichtlinien einrichten und durchsetzen sowie den Schutzstatus überwachen. Implementieren Sie ePO und verwalten Sie Ihre gesamten neuen Sicherheitslösungen oder erweitern Sie Ihre Investitionen in unternehmensorientierte Lösungen für Sicherheitsmanagement und integrieren Sie Host IPS in Ihre bestehende ePO-Infrastruktur. Mit einem einzigen Agenten lässt sich die Endgerätesicherheit leicht bereitstellen, konfigurieren und verwalten. Die Konsolidierung des Sicherheitsmanagements bedeutet nicht nur weniger Probleme, sondern ebenfalls erhebliche IT-Kosteneinsparungen.

1 McAfee Labs™  
2 McAfee Labs™

**Spezifikationen**

Microsoft Windows  
(Englisch, Französisch, Deutsch, Spanisch, Japanisch, Koreanisch, traditionelles Chinesisch)

- Windows XP Home mit Service Pack 2 oder 3
- Windows XP Professional mit Service Pack 2 oder 3
- Windows XP Tablet PC
- Windows Vista, 32-Bit und 64-Bit

**Funktionen und Vorteile**

**Mehrstufiger Schutz bietet eine breite, umfassende Abdeckung**

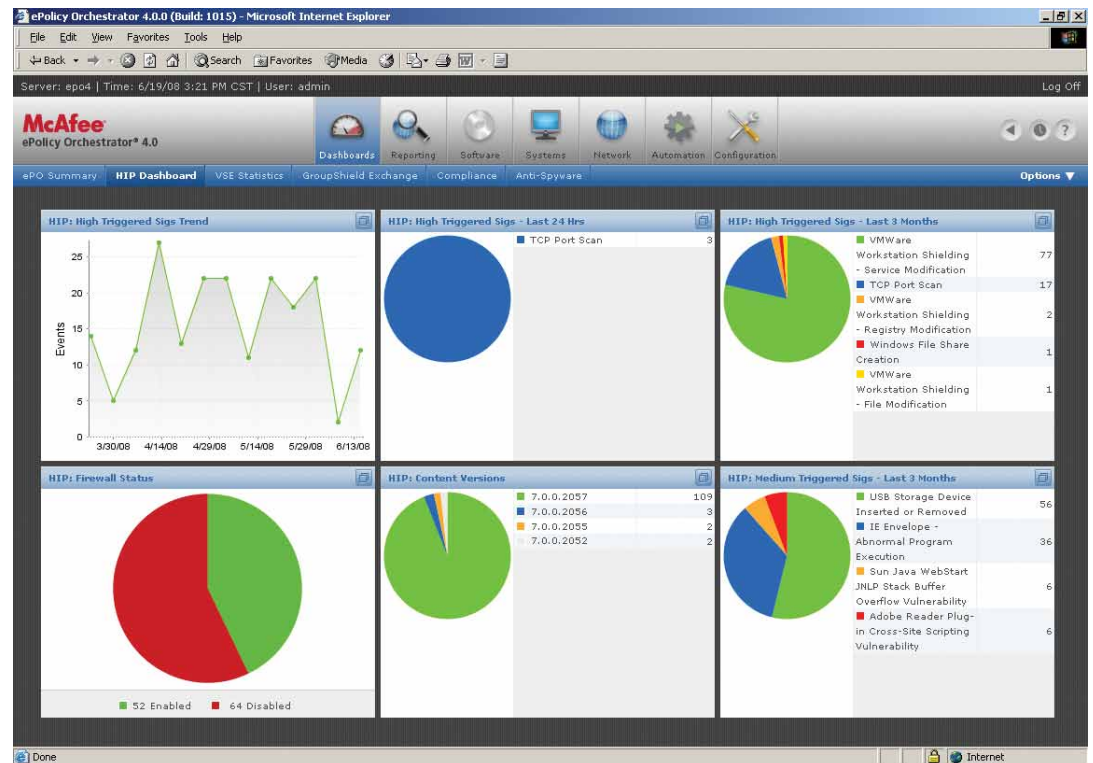
Angesichts der schnellen Zunahme der profitorientierten Internetkriminalität benötigen Unternehmen einen mehrstufigen Schutz, um ihre Endgeräte vor bekannten und Zero-Day-Bedrohungen zu schützen und den Verlust vertraulicher Daten zu verhindern.

- **Der signaturbasierte Schutz** identifiziert und blockiert bekannte Angriffe präzise
- **Der verhaltensbasierte Schutz** schützt Endgeräte vor neuen, Zero-Day-Bedrohungen wie z.B. Buffer Overflow-Angriffen
- **Die zustandsgesteuerte Firewall** blockiert unerwünschten eingehenden Datenverkehr, kontrolliert den ausgehenden Datenverkehr und wendet Richtlinien nach Datenverkehr, Ports, Anwendungen und Standorten an
- **Die Anwendungskontrolle** hilft Ihnen bei der Erstellung von Weiß- und Schwarzslisten, um festzulegen, welche Anwendungen ausgeführt werden dürfen und welche nicht

**Schutz für mobile Laptops und Verhinderung von Infektionen des Netzwerks durch regelwidrige Systeme**

Immer mehr Mitarbeiter - und ihre PCs - sind mobil und machen Unternehmen so anfälliger für neue Bedrohungen. Host IPS schützt Laptops, wenn sie nicht mit dem Firmennetzwerk verbunden sind und verhindert, dass regelwidrige Systeme das Netzwerk infizieren.

- **Schutz für Laptops**, auch wenn sie nicht mit dem Firmennetzwerk verbunden sind, um sicherzustellen, dass Angriffsversuche nicht das Netzwerk bedrohen
- **Der verbindungsbewusste Schutz** verwendet verschiedene Stufen von Schutzregeln, je nach Verbindung des Endgeräts - im Firmennetzwerk, über VPN oder ein öffentliches Netzwerk
- **Der Quarantänemodus** blockiert den Zugriff von Remote-Anwendern, die die Sicherheitsprüfungen nicht bestehen, auf Netzwerkressourcen



ePO-Dashboards erleichtern die Einsicht von Host IPS-Daten.



### Ihr IT-Team kann Patches seltener, weniger dringlich und nach eigenem Zeitplan durchführen

Ein großer Teil der Angriffe erfolgt innerhalb von drei Tagen nach Entdeckung einer Schwachstelle. Aber viele Unternehmen benötigen bis zu 30 Tage, um Patches auf allen Endgeräten zu implementieren. Host IPS schließt diese Sicherheitslücke und macht den Patch-Prozess einfacher und effizienter.

- **Der Schwachstellenschutz** aktualisiert Signaturen automatisch, um Endgeräte vor Angriffen auf Schwachstellen zu schützen
- **Der sofort aktive Schutz** kann eine überlegene Leistung aufweisen: Host IPS schützte 97 % aller im Jahr 2007 bekannt gewordenen Microsoft-Schwachstellen<sup>3</sup>
- **Die Signatur-Updates** werden regelmäßig automatisch heruntergeladen, ähnlich wie .DAT-Datei-Updates, um den Schutz zu gewährleisten

### ePO konsolidiert und zentralisiert die Verwaltung aller McAfee-Produkte

Unternehmen tun sich schwer mit den Kosten und dem Aufwand für die Verwaltung separater Sicherheitstechnologien auf ihren Endgeräten und in ihren Netzwerken. Durch die Verwendung einer einzigen, integrierten Sicherheitskonsole reduzieren Unternehmen die Anzahl der benötigten IT-Manager für die Verwaltung der Endgerätesicherheit um 44 %.<sup>4</sup>

- Zugriff auf zentrales Event-Monitoring, Berichte, Dashboards und Arbeitsabläufe mithilfe einer einzigen, Web-basierten Management-Konsole
- Bereitstellung, Verwaltung und Aktualisierung von Agenten und Richtlinien von einer Verwaltungsplattform aus

### Geringerer Zeitaufwand für die Erfassung der Daten, die für Archivierung, Reporting und den Nachweis der Einhaltung benötigt werden

Die Einhaltung aufrechtzuerhalten und nachzuweisen kann eine Unmenge von IT-Ressourcen in Anspruch nehmen. Host IPS hilft Unternehmen dabei, mehr Transparenz und Kontrolle zu erhalten sowie die Einhaltung zu vereinfachen und den Aufwand für Reporting und Audits zu verringern.

- Erfassung von Angriffsdetails wie Art, Vektor, Quelle, Schwere, Zeitstempel usw., die in verständlicher Form dargestellt werden, für prompte Berichte, Audits, Untersuchungen und Gegenmaßnahmen
- Erstellung von Compliance-Berichten für Auditoren und andere Interessengruppen
- Anpassung von Dashboards für einen Compliance-Status in Echtzeit

McAfee Host IPS ist ein integraler Bestandteil von McAfee ToPS for Endpoint, McAfees umfassender Sicherheitslösung für Endgeräte. ToPS for Endpoint ist vollständig in McAfee ePO, die zentrale SRM-Plattform, integriert, die Unternehmen durch unerreichte betriebliche Effizienz Zeit und Geld spart. Weitere Informationen zu ToPS for Endpoint finden Sie unter: [www.mcafee.com/de](http://www.mcafee.com/de).

<sup>3</sup> McAfee Labs™

<sup>4</sup> Insight Express, 2007

