

# AppSense®

## Application Manager

### Automatische Eliminierung sämtlicher nicht autorisierter Anwendungen und Steuerung des Anwendungszugriffs

AppSense Application Manager bietet funktionsfähigen, sofort einsatzbereiten Schutz vor allen Anwendungen, die durch Benutzer eingeschleust werden.

AppSense Application Manager blockiert die Ausführung sämtlicher nicht autorisierter Software unabhängig davon, ob sie aus dem Internet heruntergeladen wurde, als E-Mail-Anhang eingegangen ist oder von einem Wechseldatenträger, wie z. B. einem USB-Stick stammt, einschließlich Spyware, Peer-to-Peer- und Hacker-Tools.

### Security from within™

AppSense Application Manager ist ein wichtiges Werkzeug zur Gewährleistung der Sicherheit und Zuverlässigkeit Ihres Systems. AppSense Application Manager eliminiert durch unerwünschte Programme hervorgerufene Systemverschlechterungen, beseitigt die Bedrohung durch Viren und Trojaner und hilft dabei, die Bereitstellung von Produktionsanwendungen effektiv zu verwalten. Dies führt zu einer Reduzierung der Verwaltungs- und Managementkosten.

AppSense Application Manager verwendet sichere Abfangmechanismen auf Kernel-Ebene und ist mit dem NTFS-Sicherheitssystem integriert. Es fängt alle Ausführungsanfragen ab und blockiert unerwünschte Anwendungen automatisch. Nachdem Sie einen Satz von Benutzer-, Gruppen- und Client-Regeln definiert haben, sucht AppSense Application Manager für jeden angemeldeten Benutzer nach dem am besten geeigneten Regelsatz und wendet diesen an. Wenn keine passenden Regeln gefunden werden, wird ein standardmäßiger Schutzgrad angewendet, der lediglich die Ausführung von Anwendungen erlaubt, die vom Administrator installiert wurden.

### Proaktiver Schutz

AppSense Application Manager bietet 100-prozentigen proaktiven Schutz gegen skriptbasierte und ausführbare Viren, Trojaner und Spyware. AppSense Application Manager ermöglicht zudem die Kontrolle über Anwendungsinhalte, wie ActiveX, Bildschirmschoner, VBScripts, Batchdateien, Windows Installer-Pakete und Konfigurationsdateien für die Registrierung.

Ein weiterer gängiger Problembereich für Administratoren ist die Lizenzverteilung, d. h. die Kontrolle darüber, welche Benutzer Zugriff auf welche Anwendungen haben. Mit AppSense Application Manager können Sie die Anzahl Benutzer bzw. Benutzergruppen beschränken, die zur Ausführung bestimmter Anwendungen berechtigt sind. Die Beschränkung kann anhand der Anzahl ausgeführter Anwendungsinstanzen bzw. des Zeitpunkts oder der Dauer der Programmausführung erfolgen.

### Wichtige Funktionen

- Filterung von Ausführungsanfragen auf Kernel-Ebene
- Regelbasierte Konfiguration (Benutzer, Gruppe, Client)
- Vertrauenswürdige Besitzer
- Digitale Signaturen
- Software Lizenzkontrolle
- Passive Monitoring
- Automatische Aufzeichnung und Benachrichtigung
- Archivierung geblockter Dateien
- Weiße und schwarze Listen von Konfigurationen
- Zeitbasierte Anwendungseinschränkungen

### Die wichtigsten Vorteile

- Entscheidende Verbesserung der Systemsicherheit durch Verhinderung der Ausführung von Spyware, Peer-to-Peer- und Hacker-Tools
- Proaktiver Schutz vor ausführbaren und skriptbasierten Viren
- Optimale Systemstabilität und -integrität für alle Server und Desktopcomputer
- Einfaches Konfigurations- und Bereitstellungsverfahren mit umfassenden Prüfungsfunktionen
- Gesteigerte Rendite und reduzierte IT-Verwaltungskosten

*„Mit AppSense Application Manager haben wir den großen Vorteil zu wissen, dass Anwendungen, die die Stabilität und Sicherheit gefährden, nicht auf unseren Systemen ausgeführt werden. Wir haben kein Produkt gefunden, das mit dem Ausmaß der Kontrolle und der Benutzerfreundlichkeit dieser Lösung auch nur vergleichbar gewesen wäre.“*

*Die umfangreichen Kontroll- und Steuerungsmöglichkeiten, die wir uns für unsere Umgebung wünschten, standen bei Standardtools einfach nicht zur Verfügung.“*

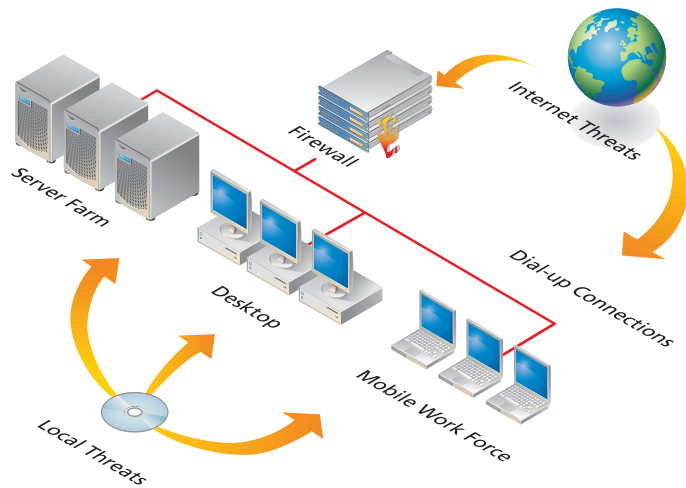
Chris Ransdell, Project Manager, Motorola

### Bereitstellung und Auditing



Die Bereitstellungsarchitektur von AppSense ermöglicht eine Softwarelösung, die an einem zentralen Ort verwaltet und von dort aus auf alle physischen und virtuellen Desktop- und Serverumgebungen verteilt werden kann.

Die Mitarbeiter können dabei während Konfigurationsänderungen weiterarbeiten, da die neuen Einstellungen dynamisch angewendet werden. Das integrierte Auditing-System zeichnet wichtige Ereignisse bezüglich Sicherheit und Leistung in Standardformaten auf, beispielsweise in einem Systemereignisprotokoll, einer E-Mail oder SNMP.



### Vertrauenswürdige Besitzer

Durch die Integration mit dem NTFS-Sicherheitssystem schützt AppSense Application Manager das System automatisch, ohne dass dazu komplexe Konfigurationen oder konstante Überwachung notwendig sind.

Anhand einer vordefinierten Liste von "vertrauenswürdigen Besitzern" lassen sich unerwünschte Anwendungen schnell identifizieren. Standardmäßig gelten nur Administratoren als vertrauenswürdig. Dadurch wird sichergestellt, dass nur von einem Administrator installierte Anwendungen ausgeführt werden können.

### Passive Überwachung

Überwachung unberechtigter Ausführungsversuche, ohne dass die Benutzer an der Ausführung der Anwendungen gehindert werden. Die passive Überwachung kann auf Benutzer-, Gruppen- oder Computerebene aktiviert bzw. deaktiviert werden. Sie stellt ein extrem hilfreiches Tool dar, mit dem sich das Verhalten der Benutzer vor einer vollständigen Implementierung akkurat nachverfolgen lässt.

### Anwendungseinschränkungen und Zeitlimits

Mit Anwendungseinschränkungen lassen sich die Lizenzrichtlinien des Unternehmens durchsetzen, indem sichergestellt wird, dass nur berechtigte Benutzer Geschäftsanwendungen ausführen. Eine weitere Kontrollmöglichkeit in Bezug auf den Anwendungszugriff besteht in der Anwendung von Zeitlimits, d. h., Benutzer können ein Programm nur in einem bestimmten Zeitraum oder für eine bestimmte Dauer verwenden.

### ZIP-Dateien und Windows Installer-Pakete

Sicheres Öffnen selbstextrahierender ZIP-Dateien mithilfe des eingebauten Zip Extractor. Zugriffsberechtigungen auf Windows Installer-Pakete durch Festlegen von Regeln, die angeben, welche Pakete ausgeführt werden dürfen.

### MMC-Schnittstelle

Mit der Microsoft Management Console können Regeln zentral verwaltet werden. Konfigurationen können automatisch für die Weitergabe verpackt werden. Die Weitergabe erfolgt mittels Windows Installer unter Verwendung des AppSense Enterprise Deployment-Systems oder eines alternativen Bereitstellungsmechanismus Ihrer Wahl.

### Regelbasierte Konfiguration

Richtlinien der Anwendungsausführung können für einzelne Benutzer, Gruppen oder Clients durch Hinzufügen von Regeln hinzugenommen werden. Jede Regel umfasst eine weiße Liste mit Elementen, auf die zugegriffen werden darf, und eine schwarze Liste mit verbotenen Elementen.

### Digitale Signaturen

Erhöhte Sicherheit durch Hinzufügen digitaler Signaturen zu Ihrer Konfiguration. Durch die Überprüfung digitaler Signaturen kann der Administrator sicher sein, dass die auf einem System installierten Anwendungen und Dateien unverändert bleiben. Dadurch bleibt die Systemintegrität erhalten, und die Wartungskosten werden reduziert. Durch die Erstellung von Gruppen digitaler Signaturen lässt sich die Verwaltung großer, komplexer Konfigurationen vereinfachen.

### Weißer und schwarzer Listen von Konfigurationen

Problemloses Verarbeiten großer Mengen von Dateien und Ordnern mit weißen und schwarzen Listen von Konfigurationen. Schutz vor bekannten Bedrohungen und Problemanwendungen durch die Definition schwarzer Listen sowie garantierte, systemweite Ausführungsbeschränkung auf bekannte, vertrauenswürdige Anwendungen durch weiße Listen.

### VBSkripts & Batchdateien

Dadurch dass Benutzer nur Skripte ausführen können, die vom Administrator autorisiert wurden, werden Angriffe durch schädlichen Code und Viren verhindert. Skripte, wie z. B. Windows Script Host-Dateien und DOS Batch-Skripte werden anhand der bestehenden Regeln überprüft. Auf diese Weise wird festgestellt, ob sie ausgeführt werden dürfen. Die Überprüfung digitaler Signaturen sorgt für zusätzliche Sicherheit. Sie gewährleistet, dass der Inhalt von Skripten unverändert bleibt.

### Konsole für die Regelanalyse

Mit der Konsole für die Regelanalyse können Administratoren Probleme mit einer angewendeten Konfiguration beheben. Mit XML-basierten Protokolldateien lässt sich leicht auf die Gründe zugreifen, aus denen eine Anwendung ausgeführt oder nicht ausgeführt werden konnte.

## Risiken innerhalb des Unternehmens

Die derzeit gängigen Maßnahmen zum Schutz von Unternehmensnetzwerken vor externen Angriffen bieten eine nur unzureichende Lösung. Systeme und Daten werden oft nicht ausreichend geschützt. Das FBI in den USA bestätigt, dass 80% der gesamten Computerkriminalität ihren Ursprung innerhalb der Organisationen hat.

Sicherheitsmethoden, wie etwa Firewalls, blockieren nicht immer Anwendungen, die über E-Mail, Webbrowser oder Wechseldatenträger eingeschleust werden. Benutzer von laptops arbeiten außerhalb Ihres geschützten Netzwerks und können so nicht autorisierte Anwendungen auf ihrem Mobilcomputer installieren.

## Systemanforderungen

- Windows Server 2003
- Windows XP
- Windows 2000
- Windows NT 4.0 (SP 6 or greater)
- Mit Terminaldiensten kompatibel (Alle Versionen)
- Mit Citrix MetaFrame kompatibel (Alle Versionen)

## Unsere Lösungen

### Sicherheit

Automatische Eliminierung sämtlicher nicht autorisierter Anwendungen und Steuerung des Anwendungszugriffs

### Management

Zentrale Konfiguration und Überwachung von selbstheilenden Benutzerumgebungen

### Performance

Dynamische Optimierung der Systemleistung, -verfügbarkeit und -kapazität

## Web links

- Informationen über unsere Produkte <http://www.appsense.de/products>
- Informationen über unsere Lösungen <http://www.appsense.de/solutions>
- Laden Sie Ihre kostenlose Testversion herunter <http://www.appsense.de/downloads>

### German Office

AppSense GmbH  
Am Söldnermoos 17  
85399 Hallbergmoos  
Deutschland

Tel +49 89 607 68530  
Fax +49 89 607 68540  
Email [de-info@appsense.com](mailto:de-info@appsense.com)



© AppSense 2005 v1.1DE