

# AppSense®

## Application Manager

### Elimineer automatisch alle ongeautoriseerde applicaties en controleer applicatietoegang

AppSense Application Manager biedt 'out-of-the-box' beveiliging tegen alle applicaties die uw medewerkers proberen te installeren.

Het doet er niet toe of software gedownload is van het internet, ontvangen als e-mailbijlage of afkomstig is van opslagmedia als USB Flash-drives of CD-ROM; AppSense Application Manager voorkomt de installatie van alle ongeautoriseerde software. Dus ook spyware-, peer-to-peer- en hacking-tools.

### Beveiliging van binnenuit

AppSense Application Manager is een integraal hulpmiddel voor het onderhouden van systeembeveiliging en -betrouwbaarheid. Door te voorkomen dat ongewenste programma's het systeem bevuilden, en door aanvalsdreigingen van virussen en trojans weg te nemen en de distributie van productieapplicaties te beheren, verbetert de oplossing de ROI en worden beheerkosten en -overhead verlaagd.

Op basis van veilige interceptie op kernel niveau en integratie met NTFS-beveiliging blokkeert AppSense Application Manager alle opstart verzoeken van ongewenste applicaties. Als u een reeks gebruikers-, groep- of client-regels heeft gedefinieerd, kent de oplossing de best passende regels voor iedere ingelogde gebruiker toe. Als AppSense Application Manager geen specifieke regels vindt, wordt een standaard beveiligingsniveau toegepast. In dat geval kan alleen de beheerder applicaties installeren.

### Proactieve bescherming

AppSense Application Manager biedt 100% proactieve bescherming tegen scriptgebaseerde en uitvoerbare virussen, trojans en spyware.

Daarnaast biedt de oplossing controle over veel andere type applicaties, waaronder ActiveX, screensavers, VBScripts, batchbestanden, Windows Installer-pakketten en Register-configuratiebestanden. Door gebruik te maken van de geïntegreerde Zip Functionaliteit worden Zip-bestanden veilig uitgepakt.

Licentiebeheer is een andere bron van zorg voor beheerders, oftewel welke gebruiker toegang heeft tot welke applicatie. Met AppSense Application Manager kunt u het aantal gebruikers of groepen gebruikers van applicaties beperken. Deze limieten zijn in te stellen wat betreft aantal applicatiegebruikers, gebruikstijd of wanneer een applicatie is te gebruiken.

### Belangrijkste functionaliteit

- Filteren van installatiepogingen op kernel niveau
- Op regels gebaseerde configuratie (gebruiker, groep, client)
- Betrouwbare eigenaar
- Digitale handtekeningen
- Tijdsgebaseerde applicatiebeperkingen
- Limiet aan gelijktijdig gebruik van applicaties
- Configuratiemogelijkheden voor een zwarte en een geautoriseerde lijst
- Controle op softwarelicenties
- Passieve monitoring
- Geïntegreerde event controle en directe notificatie
- Archivering van verbannen bestanden (gebruikersspecifiek, anoniem)
- Naadloos uitpakken van Zip-bestanden

### Belangrijkste voordelen

- Sterk verbeterde systeembeveiliging. Voorkomt dat gebruikers spyware-, peer-to-peer en hacking-tools installeren
- Proactieve virusbescherming tegen uitvoerbare en scriptgebaseerde virussen
- Optimale systeemstabiliteit en -integriteit voor alle servers en desktops
- Eenvoudig te configureren en in te zetten met uitgebreide analysemogelijkheden
- Snellere ROI en lagere IT-beheerkosten

*“Met AppSense Application Manager weten we dat applicaties die de stabiliteit of veiligheid van ons systeem in gevaar kunnen brengen, niet op onze systemen draaien. We hebben geen andere oplossing kunnen vinden die het controleniveau of de eenvoud van deze oplossing benadert. Standaard-tools leveren eenvoudigweg niet de controlemogelijkheden waar wij behoefte aan hebben.”*

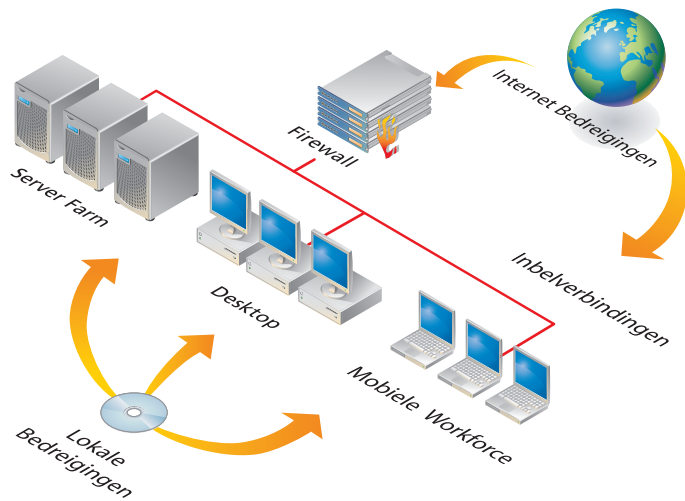
Chris Ransdell, Project Manager, Motorola

### Deployment & Auditing



De deployment architectuur van AppSense biedt één softwareoplossing die u centraal kunt beheren en distribueren naar al uw fysieke en virtuele desktop- en serveromgevingen.

Aangezien nieuwe instellingen dynamisch worden doorgevoerd, kunnen gebruikers tijdens configuratiewijzigingen gewoon doorwerken. Het geïntegreerde auditing-raamwerk slaat belangrijke beveiligings- en prestatie-gebeurtenissen op in standaardformaten zoals system event log, e-mail en SNMP.



### Betrouwbare Eigenaar

Door de naadloze integratie met NTFS-beveiliging beschermt AppSense Application Manager het systeem automatisch, zonder complexe configuraties en intensieve beheerspanningen. Een vooraf opgestelde lijst met 'betrouwbare eigenaars' zorgt ervoor dat u snel vaststelt welke applicaties onbetrouwbaar zijn. In de standaardinstellingen worden alleen beheerders als betrouwbaar beschouwd, waardoor alleen door hen geïnstalleerde applicaties kunnen draaien. U kunt deze lijst naar eigen keuze uitbreiden.

### Passieve monitoring

U kunt ongeautoriseerde startpogingen monitoren zonder het gebruik van applicaties tegen te houden. Deze passieve monitoring is per gebruiker, groep of computer in of uit te schakelen. Met deze tool kunt u gebruikersgedrag zeer nauwkeurig traceren voordat u applicaties in hun geheel implementeert.

### Applicatielimiten en tijdsbeperkingen

Om te voldoen aan het licentiebeleid van uw bedrijf kunt u gebruikmaken van de functionaliteit voor applicatielimiten. Hiermee bent u ervan verzekerd dat alleen geautoriseerde gebruikers bedrijfsapplicaties kunnen draaien. Nog grotere controle over applicatietoegang is te realiseren door de toepassing van tijdsbeperkingen. Dit houdt in dat gebruikers alleen tijdens bepaalde uren of voor een beperkte tijd applicaties kunnen gebruiken.

### Zip-bestanden & Windows Installer Packages

Maak gebruik van de geïntegreerde Zip Extractor om Self-Extracting Zip-bestanden veilig te openen. Daarnaast kunt u de toegang tot Windows Installer-pakketten beperken door regels op te stellen welke pakketten mogen draaien.

### MMC-interface

De Microsoft Management Console biedt mogelijkheden voor een centraal beheer van regels. Configuraties zijn automatisch in te pakken voor distributie door Windows Installer in het Deployment-systeem van AppSense of door een systeem naar keuze.

### Op regels gebaseerde configuratie

U kunt beleid voor applicatie-uitvoering per individuele gebruiker, groep of client opstellen door regels toe te voegen. Elke regel omvat een lijst met te benaderen items en een zwarte lijst met verboden items. De configuratie van uitvoeringsbeleid is ook regel voor regel toe te passen.

### Digitale handtekeningen

Voor geavanceerde beveiliging kunt u digitale handtekeningen toevoegen aan uw configuratie. Het controleren van deze handtekeningen biedt gemoedsrust voor de beheerder. Diegene weet dat de op een systeem geïnstalleerde applicaties en bestanden ongewijzigd blijven. Dit zorgt voor systeemintegriteit en verlaagt beheerkosten. De opzet van groepen digitale handtekeningen vereenvoudigt het beheer van grotere en complexere configuraties.

### Configuratiemogelijkheden voor een zwarte en een geautoriseerde lijst

Verwerk grote hoeveelheden bestanden en folders naadloos met configuratiemogelijkheden voor een zwarte en een geautoriseerde lijst. Door zwarte lijsten op te stellen beschermt u zich tegen bekende bedreigingen en probleemapplicaties. Met geautoriseerde lijsten garandeert u zich ervan dat alleen bekende en betrouwbare applicaties op uw systeem draaien.

### VBScripts & batchbestanden

U voorkomt aanvallen van schadelijke code en virussen door ervoor te zorgen dat gebruikers alleen door de beheerder goedgekeurde scripts kunnen oproepen. Scripts als Windows Script Host files en Dos Batch worden tegen de beleidsregels afgezet om te bepalen of ze mogen draaien. U bereikt extra veiligheid met de controle van digitale handtekeningen. Hierdoor weet u zeker dat script-content onveranderd blijft.

### Rules Analyzer-console

Beheerders kunnen met de Rules Analyzer configuratieproblemen oplossen. XML-gebaseerde logbestanden bieden vereenvoudigde toegang tot informatie over waarom een applicatie wel of niet mag draaien.

## Bedreigingen van binnenuit

De huidige beveiligingsaanpak tegen externe aanvallen biedt slechts een gedeeltelijke oplossing. Deze laat openingen over in systemen en data die zijn te misbruiken. De FBI bevestigt deze stelling en verklaart dat 80 procent van de computercriminaliteit van binnen de organisatie komt.

Beveiligingsmethodes op de netwerkgrens, zoals firewalls, blokkeren niet per definitie applicaties die via e-mail, webbrowsers en verwijderbare media binnenkomen. Mobile medewerkers opereren buiten de netwerkgrens en kunnen thuis of onderweg ongeautoriseerde applicaties installeren.

## Systeemvereisten

- Windows Server 2003
- Windows XP
- Windows 2000
- Windows NT 4.0 (SP 6 of hoger)
- Uitwisselbaar met Terminal Services (Alle versies)
- Uitwisselbaar met Citrix MetaFrame (Alle versies)

## Onze oplossingen

### Beveiliging

Elimineer automatisch alle ongeautoriseerde applicaties en controleer applicatietoegang

### Beheer

Zet centraal gebruikersomgevingen op, blokkeer deze en zorg voor mogelijkheden voor zelfreparatie

### Prestaties

Dynamisch beheer van systeemprestaties, -beschikbaarheid en -capaciteit.

## Weblinks

- Meer informatie over onze producten <http://www.appsense.com/products>
- Meer over onze oplossingen <http://www.appsense.com/solutions>
- Download een gratis evaluatieversie <http://www.appsense.com/downloads>

#### Benelux Office

AppSense  
3200 Daresbury Park  
Daresbury Warrington  
WA4 4BU United Kingdom

Tel +44 (0)161 216 3200  
Fax +44 (0)161 216 3232  
Email [info@appsense.com](mailto:info@appsense.com)

#### European Office

AppSense  
3200 Daresbury Park  
Daresbury Warrington  
WA4 4BU United Kingdom

Tel +44 (0)161 216 3200  
Fax +44 (0)161 216 3232  
Email [info@appsense.com](mailto:info@appsense.com)

#### North American Office

AppSense  
3333 West Commercial Blvd  
Suite 105 Fort Lauderdale  
FL 33309 USA

Tel +1 954 730 7400  
Fax +1 954 730 7380  
Email [us-info@appsense.com](mailto:us-info@appsense.com)

#### 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)

#### Australian Office

AppSense  
69/283 Glenhuntsly Road  
Elsternwick Melbourne  
Victoria 3185 Australia

Tel +61 (0) 1300 767 550  
Fax +61 (0) 3 9525 7091  
Email [australia-info@appsense.com](mailto:australia-info@appsense.com)

**Microsoft**  
CERTIFIED  
Partner

**citrix** **access** PARTNER

PREMIER  
Alliance Partner

© AppSense 2005 v1.NL