

Beim AppSense Security Audit handelt es sich um eine Consulting-Serviceleistung, bei der intelligente Software zum Einsatz kommt, durch die sich Unternehmen ein klares Bild von der tatsächlichen Sicherheit ihrer Terminal Server und Desktop PCs machen können.

## Was ist ein Security Audit?

Security Audits sind das Ergebnis einer engen Zusammenarbeit mit einem AppSense Certified Solution Partner, der von AppSense zur Durchführung des jeweiligen Audits akkreditiert wurde. Die Serviceleistung umfasst die Installation der AppSense Audit Software, das Loggen der Daten im Passiv-Modus und die entsprechende Auswertung. Die Software läuft unbemerkt im „Background“ der Systeme und zeichnet die sicherheitsrelevanten Daten auf, ohne dass dadurch Ihr Produktivsystem beeinträchtigt wird.

In der Regel werden die Daten innerhalb 2 Wochen aufgezeichnet. Nach dem Audit wird ein ausführlicher Bericht erstellt, in dem die wichtigsten Ergebnisse hervorgehoben werden. Es werden so mögliche Sicherheitslücken festgestellt, die für Ihr Unternehmen eine Bedrohung darstellen könnten. Dabei werden z.B. vom Benutzer ausgeführte Applikationen, die unwissentlich oder absichtlich die Systemintegrität gefährden, sowie ausführbare Viren und Trojaner, die bisher noch nicht von einem Antivirenprogramm oder einer Firewall entdeckt wurden, anonym angezeigt.

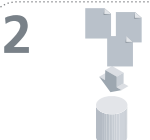
Das IT-Management erhält abschließend präzise Informationen und Empfehlungen in Form eines übersichtlichen Berichts, der mögliche Sicherheitsprobleme im Zusammenhang mit der unbefugten Nutzung von Anwendungen oder mit nicht erkannten Viren darstellt. Der Bericht ist daher für die Entscheidungsträger und die IT-Administratoren eine wichtige Entscheidungsgrundlage für mögliche Verbesserungen im Bereich IT-Sicherheit.

## Durchführung der Audits



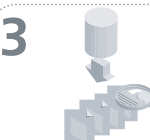
### 1 Installation

Ein AppSense Certified Auditor gewährleistet, dass sowohl die AppSense Audit Software auf jedem zu bewertenden Terminal Server/Desktop installiert ist. Die Audit Tools werden im „passiven Modus“ installiert, wodurch gewährleistet ist, dass die Leistung der Systeme nicht beeinträchtigt wird.



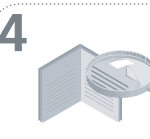
### 2 Datenerfassung

Während der folgenden zwei Wochen werden automatisch Daten über gestartete ausführbare Anwendungen erfasst. Am Ende dieses Zeitraums werden die Daten vom Auditor zu Verarbeitungs- und Analysezwecken eingesammelt.



### 3 Analyse und Berichterstellung

Der Auditor führt die Analyse Engine des Security Audits aus, um die gesammelten Daten aufzubereiten und auszuwerten. Dieser Vorgang wird extern ausgeführt und hat keine Auswirkungen auf die Systeme des Kunden. Der Auditor wertet unter Einhaltung einer strukturierten Methodik die erfassten Daten aus und erstellt einen Abschlussbericht.



### 4 Ergebnis-Präsentation

Beim Abschlussbericht handelt es sich um ein ausführliches Dokument, in dem Daten zusammengefasst, wichtige Informationen hervorgehoben und entsprechende Empfehlungen zur Verbesserung der Sicherheit gegeben werden. Der Bericht wird in elektronischer Form als PowerPoint-Präsentation und PDF-Datei bereitgestellt und bei einem Vor-Ort Termin präsentiert.

## Weitere Informationen

Weitere Informationen erhalten Sie bei Ihrem Certified Solution Partner vor Ort. Hier können Sie auch gerne ein Security Audit Ihres Systems vereinbaren.

## AppSense®

### European Office

AppSense, 3200 Daresbury Park,  
Daresbury, Warrington, WA4 4BU,  
United Kingdom

**Telephone:** +44 (0)161 216 3200  
**Facsimile:** +44 (0)161 216 3232  
**E-mail:** info@appsense.com

### North American Office

AppSense, 3333 W. Commercial Blvd,  
Suite 105, Ft.Lauderdale,  
FL33309, USA

**Telephone:** +1 954 730 7400  
**Facsimile:** +1 954 958 0321  
**E-mail:** us-info@appsense.com

### German Office

AppSense GmbH, Am Söldnermoos  
17, 85399 Hallbergmoos,  
Deutschland

**Telephone:** +49 89 607 68530  
**Facsimile:** +49 89 607 68540  
**E-mail:** de-info@appsense.com

### Benelux Office

AppSense, Postbus 54,  
6665 ZH Driel,  
The Netherlands

**Telephone:** +31 (0) 611 045 113  
**Facsimile:** +31 (0) 848 333 217  
**E-mail:** benelux-info@appsense.com

### Australian Office

AppSense, 69/283 Glenhantly Road  
Elsternwick, Melbourne. Victoria, 3185.  
Australia

**Telephone:** +61 (0) 1300 767 550  
**Facsimile:** +61 (0) 3 9525 7091  
**E-mail:** australia-info@appsense.com



PREMIER  
Alliance Partner

## Für Server und Desktops.

### Sind Sie sicher, dass Ihre IT Infrastruktur sicher ist?

Überall dort, wo Benutzer an ihrem PC-Arbeitsplatz Zugriff auf das Internet haben, E-Mails versenden und empfangen oder lokale Speichermedien (CD, DVD, Floppy, Speicher-Sticks, etc.) verwenden können, besteht das Risiko, dass nicht autorisierte Software-Programme eingeschleust werden.

Bei nicht autorisierter Software in Unternehmen kann es sich beispielsweise um Hackertools, Spiele, Animationen oder unlizenzierte Programme handeln. Eine besonders große Bedrohung stellen selbstverständlich auch die unzähligen Virentypen dar, die als ausführbare Dateien oder als Visual Basic-Skripte verbreitet werden. Aber auch wenn Benutzer unlizenzierte Software einsetzen, kann dies strafrechtliche Konsequenzen für die Verantwortlichen in der betreffenden Organisation haben.

Die durch Ausführung nicht autorisierter Anwendungen verursachte Instabilität auf den PCs der Anwender erhöht den Supportaufwand (und damit Kosten) unter Umständen ganz erheblich. Ein Virenbefall stellt eine große Gefahr für jedes Unternehmen dar und schlägt sich meistens auch sehr schnell in sehr hohen Kosten für die Beseitigung und Schadensbehebung nieder. So können in großen Unternehmen mit Hunderten oder Tausenden von PCs die Kosten schnell exponentiell eskalieren, wenn keine effektiven Kontrollmaßnahmen ergriffen werden.

Bisher standen IT-Verantwortlichen keine pro-aktiven Tools für die effektive Beseitigung dieser Sicherheits-Risiken zur Verfügung. Z.B. besteht immer eine Abhängigkeit von Anti-Viren-Patches, die möglicherweise beim Eintreffen des Virus noch nicht verfügbar oder eingerichtet sind.

### Die AppSense Lösung

Der **Application Manager Desktop** ist eine komfortable Lösung für die System- und Sicherheitsverwaltung im Unternehmen. Durch das zentralisierte Bereitstellungsverfahren der Lösung können Anwendungsserver und PCs in der gesamten Organisation ohne großen Aufwand geschützt werden. Da die hiermit verbundenen Installations- und Konfigurationsvorgänge zentral gesteuert werden können, müssen diese Arbeitsschritte nicht vor Ort an jedem einzelnen Computer durchgeführt werden.

Die einfach zu verwendenden Verwaltungskonsolen von Application Manager, basierend auf Microsoft MMC, bieten flexible Konfigurationsoptionen, mit denen die unterschiedlichsten Anforderungen an die Anwendungskontrolle in Unternehmensumgebungen jeder Art umgesetzt werden können. Die Voreinstellungen von Application Manager sorgen bereits ohne individuelle Konfiguration für einen effektiven und umfassenden Schutz vor nicht autorisierten Anwendungen und Skripten. Das einzigartige, auf dem Konzept der vertrauenswürdigen Besitzer basierende Sicherheitsmodell ist nahtlos in die von Microsoft Windows NT/2000/XP bereitgestellten Funktionen für die Sicherheit des Dateisystems integriert.

Für mehr Informationen kontaktieren Sie uns:

### Ihre Sicherheits-Vorteile mit dem AppSense Application Manager (AMD):

- » 100%iger, pro-aktiver Schutz vor allen ausführbaren Skripten
- » keine Abhängigkeit von Anti-Viren-Patches
- » sofortiger Systemschutz nach Installation
- » keine Ausführung von Hacking Tools möglich
- » effektive Lizenz-Kontrolle
- » liefert optimale System-Stabilität und -Integrität
- » zentral installier- und administrierbar
- » kompatibel ab Win NT4 bis Win XP

Kostenloser Software-Download unter :  
<http://www.appsense.com/>

