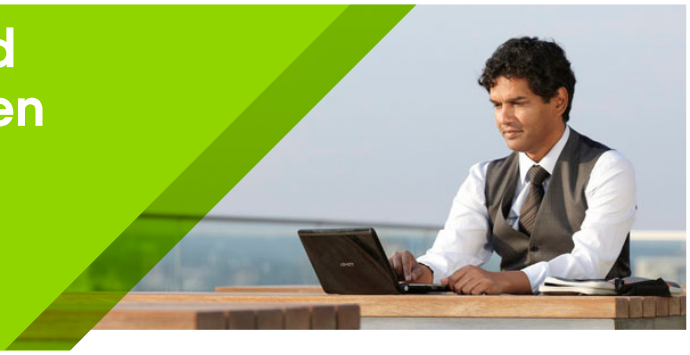
AppSense Application Manager
Produktdatenblatt

Schaffen Sie eine praktische und kosteneffiziente Balance zwischen IT Compliance und Benutzeranforderungen



Hauptmerkmale:

- Granulare, nahtlose Erweiterung der Windows-Berechtigungen
- Bedarfsgerechtes Change-Request-Management
- Unternehmensfähige Änderungsverfolgung und Kontrolle
- Kontextabhängige Anwendungsberechtigung
- Application Network Access Control (Netzwerkzugangskontrolle für Anwendungen)
- Softwarelizenzkontrolle
- Passiver Überwachungsmodus
- Integrierte Prüfungsereignisse

Vorteile:

- Erhaltung der Umgebung im gewünschten Zustand
- Mehr Transparenz in der Anwendungslandschaft
- Durchsetzung der Lizenzbestimmungen, Sicherstellung der Einhaltung
- Weniger Supportanrufe
- Höhere Benutzerproduktivität

Über AppSense

AppSense ist einer der weltweit führenden Hersteller im Bereich User Environment Management (UEM): Über 3000 Firmenkunden setzen die Lösungen auf über 7 Millionen Desktops ein. AppSense DesktopNow und DataNow ermöglichen es IT-Abteilungen sowohl auf virtualisierten als auch physikalischen Desktops eine optimale Anwenderzufriedenheit und Produktivität sicher zu stellen. Gleichzeitig wird die Sicherheit erhöht und laufende Infrastrukturkosten reduziert. Das Unternehmen hat seinen Hauptsitz in Sunnyvale, USA und weltweite Niederlassungen.

Anwendungsberechtigungen für Benutzer

Unabhängig davon, ob eine Umgebung durch ein serverbasiertes Netzwerk, virtuelle oder physische Desktops oder eine Kombination daraus bereitgestellt wird, entscheidend ist dabei, dass Benutzer nur die Anwendungen erhalten, die sie benötigen, und keine unbekannten Programme in der Umgebung ausführen können.

Die Verwendung nicht autorisierter Software beeinträchtigt die Stabilität von Benutzerumgebungen ganz erheblich und erschwert IT-Teams die Fehlerbehebung an beschädigten Desktops. In einer gemeinsamen Benutzerumgebung wie einem serverbasierten Netzwerk werden die Kosten noch weiter in die Höhe getrieben, wenn die Tätigkeit eines Benutzers Einfluss auf viele andere hat. Derzeitige Methoden zur Durchsetzung der Anwendungsnutzung sind auf komplexe Skripte oder wartungsintensive Blacklists und Whitelists beschränkt.

Trusted Ownership™

AppSense Application Manager verwendet sichere Filtertreiber auf Kernel-Ebene sowie Microsoft NTFS-Sicherheitsrichtlinien, fängt alle Ausführungsanforderungen ab und blockiert unerwünschte Anwendungen. Die Anwendungsberechtigung basiert auf dem Besitzrecht für die Anwendung, wobei der Administrator der standardmäßige Besitzer ist. Mit dieser Methode werden aktuelle Richtlinien für den Anwendungszugriff sofort („out-of-the-box“) wirksam, ohne dass Skripte oder Listen verwaltet werden müssen. Dafür steht Trusted Ownership™. Zusätzlich zu ausführbaren Dateien verwaltet AppSense Application Manager außerdem die Berechtigung für Anwendungsinhalte, wie z. B. ActiveX-Steuerelemente, VB-Skripte, Batchdateien, MSI-Pakete und Konfigurationsdateien für die Registrierung.

Verwaltung von Benutzerrechten

Die Die Benutzerrechte werden auf dynamischer Basis mit hoher Präzision kontrolliert. Dadurch werden Anwendern nur die Administratorrechte gewährt, die sie benötigen. Gleichzeitig werden die IT-Kosten niedrig gehalten. AppSense macht lokale Benutzerkonten mit Administratorrechten überflüssig und verwaltet Berechtigungen auf Ebene der Anwendung oder der spezifischen Aufgabe. Rechte können für einzelne Benutzer, Anwendungen oder Tätigkeiten zurückgenommen oder eingeschränkt werden.

Nicht nur Anwendungen

Zusätzlich zu der lokalen Anwendungskontrolle gewährleistet der AppSense Application Manager die Verwaltung ausgehender Verbindungsanfragen zu UNC-Pfaden und URLs. Dies bietet gleichzeitig eine umfassende Lösung für alle Anwendungen und Netzwerkberechtigungen. Verbindungen, URLs oder Anwendungen können auch regelbasiert beendet werden.

Kontextabhängige Berechtigung

Auf welche Unternehmensanwendungen ein Mitarbeiter zugreifen darf, kann vom Endgerät abhängen, von dem der Zugriff erfolgt. Beispielsweise hat ein Benutzer in einem Internet-Café üblicherweise einen eingeschränkteren Anwendungszugriff als ein Mitarbeiter, der innerhalb des sicheren Unternehmensnetzwerks arbeitet. AppSense Application Manager ist in der Lage, anhand von Informationen über den Benutzerkontext wie Standort, Firewall-Einstellungen oder sogar Tageszeit das nötige Maß an Berechtigung zu bestimmen.

Offline-Berechtigung

Weil Mitarbeiter zunehmend mobil werden, ist es unabdingbar, dass Berechtigungsrichtlinien durchgesetzt werden, wenn der Benutzer nicht mit dem Unternehmensnetzwerk verbunden ist. AppSense Application Manager stellt durch den Einsatz von Berechtigungsrichtlinien auf den Endpunktgeräten sicher, dass Mitarbeiter nur auf Anwendungen und Ressourcen zugreifen, für die sie die Berechtigung haben, wenn sie offline sind.

Lizenzverwaltung

AppSense Application Manager wird von Microsoft® für die Softwarelizenzkontrolle in serverbasierten Netzwerkumgebungen empfohlen. Das Ausführen der Software im passiven Modus ermöglicht Überwachung, Prüfung und Berichterstellung, um die Häufigkeit von Anwendungsaufrufen durch Benutzer und Geräte im Einzelnen aufzuzeigen. Durch die Steuerung, welcher Benutzer oder welche Geräte berechtigt sind, benannte Anwendungen auszuführen, können Beschränkungen für die Anzahl der Anwendungsinstanzen festgelegt werden und dafür, welche Geräte oder Benutzer die Anwendung zu welcher Zeit und für wie lange ausführen dürfen.

Lizenzprüfung und Zugriffsbeschränkung auf Grundlage der Anzahl von Lizenzen können jetzt unabhängig von der Methode der Anwendungsbereitstellung durchgesetzt werden. Lizenzüberprüfungen können in Umgebungen mit virtuellen und physischen Desktops verwendet werden.

AppSense Application Manager
Produktdatenblatt

Funktionen von AppSense Application Manager

Quick Start-Konfigurationsvorlagen

Nutzen Sie mit den Konfigurationsvorlagen von AppSense das volle Potenzial von Best-Practice-Unternehmensrichtlinien. AppSense Application Manager kann eine unbeschränkte Anzahl an Konfigurationsdateien importieren und diese Konfigurationen kombinieren. Eine Auswahl an Konfigurationsvorlagen, wie z. B. „common prohibited items“ (üblicherweise verbotene Elemente) oder „End Point Analysis“ (Endpunktanalyse) ist in der Vorlagenbibliothek verfügbar, die häufig überarbeitet und aktualisiert wird.

Verwaltung von Benutzerrechten

Die Rechte eines Benutzers, einer Gruppe oder einer Rolle können für Anwendungen und Elemente der Systemsteuerung erweitert oder reduziert werden. Lokale Administratorkonten können entfernt werden, während die Anwender weiterhin auf einzelne Applikationen oder Aufgaben, die Administratorrechte erfordern, zugreifen dürfen.

Erkennungsmodus für Berechtigungen

Schneller Scan und Report von zehntausenden Desktops und Identifizierung von Anwendungen und Aufgaben, die Administratorrechte erfordern. Flexible Reporting-Möglichkeiten erleichtern das schnelle Hinzufügen dieser Anwendungen in die bestehende Konfiguration.

Bedarfsgerechtes Change-Request-Management

Ermöglichen Sie es Benutzern, in Notfällen – z. B. bei einer wesentlichen Beeinträchtigung der Produktivität – eine Berechtigungserweiterung anzufordern. Die Anforderung kann vom Benutzer im Dialogfeld der jeweiligen Anwendung initiiert werden. Dringende Änderungsanforderungen können über ein einfaches Fulfillment-Portals an einen First-Level-Helpdesk-Analysten weitergeleitet werden. Die Berechtigungserweiterung kann entweder vorübergehend oder dauerhaft erfolgen.

Passives Monitoring

Überwachen Sie die Anwendungsnutzung, ohne die Benutzer an der Ausführung der Anwendungen zu hindern. Das passive Monitoring kann auf Benutzer-, Geräte- oder Gruppenebene aktiviert oder deaktiviert werden. Sie stellt ein äußerst hilfreiches Tool dar, mit dem sich das Anwenderverhalten vor der vollständigen Implementierung nachvollziehen oder die Anwendungsnutzung zur Anpassung der Softwarelizenzverwaltung untersuchen lässt.

Analyse von Endgeräten

Identifizieren Sie alle ausführbaren Dateien auf einem Zielgerät und teilen Sie die Dateien in „autorisiert“ und „nicht autorisiert“ ein, um schnell Richtlinien zu erstellen.

Konfigurationen können für einen Benutzer, eine Gruppe von Benutzern, einen Computer oder eine Gruppe von Computern bereitgestellt werden. Innerhalb von Minuten steuert die Anwendungsberechtigung automatisch die Anwendungsnutzung.

Untersuchung der Anwendungsnutzung

Untersuchen Sie ein Zielgerät und ermitteln Sie, wie oft einzelne Anwendungen pro Benutzer ausgeführt wurden. Durch Markieren der Anwendungen, die verwendet bzw. nicht verwendet werden, kann unlizenzierte Software ermittelt und beschränkt werden. Lizenzierte Software kann entfernt werden, um sowohl die Anzahl an Anwendungen auf einem Gerät als auch die Lizenzkosten dieser Anwendungen zu verringern.

Trusted Ownership™

Schützen Sie das System ohne komplexe Listen und fortwährende Verwaltung. Nur der Code, der von „trusted owners” (vertrauenswürdigen Besitzern) installiert wurde und in deren Besitz ist, darf ausgeführt werden. Die Liste der „trusted owners“ kann auf jede Umgebung oder Verzeichnisstruktur angepasst werden.

Konfiguration von Whitelists und Blacklists

Die Konfiguration von Whitelists und Blacklists kann in Verbindung mit „Trusted Ownership“ verwendet werden, um bekannte Anwendungen zu steuern, die der NTFS-Besitzerprüfung standgehalten haben. Anwendungen, auf die Benutzer keinen Zugriff haben sollten, z. B. die Tools in Administratorbesitz wie cmd.exe oder ftp.exe, werden automatisch zurückgewiesen. Oder erstellen Sie Whitelists, um zu garantieren, dass nur bekannte und vertrauenswürdige Anwendungen auf einem System ausgeführt werden können.

Digitale Signaturen

Weisen Sie Anwendungen und Dateien SHA-1-verschlüsselte digitale Signaturen zu, um die Anwendungsintegrität sicherzustellen. Veränderte und gefälschte Anwendungen werden an der Ausführung gehindert.

Umfangreiche Dateiunterstützung

Wenden Sie Richtlinien an, um die Anzahl von Anwendungsinstanzen zu steuern, die ein Benutzer ausführen kann, zusammen mit den Zeitpunkten, an denen sie ausgeführt werden können. Es können Richtlinien erstellt werden, um Lizenzmodelle zu steuern und durchzusetzen, indem Anwendungsbeschränkungen pro Gerät gesteuert werden.

Umfangreiche Dateiunterstützung

Zusätzlich zur Steuerung von Anwendungen wie .exe-Dateien werden auch Skript-, Batch- und Registrierungsdateien gesteuert. Digitale Signaturen können auf Skripte angewendet werden, um sicherzustellen, dass der Inhalt unverändert bleibt.

Anwendungsbeschränkungen und Zeitlimits

Wenden Sie Richtlinien an, um die Anzahl von Anwendungsinstanzen zu steuern, die ein Benutzer ausführen kann, zusammen mit den Zeitpunkten, an denen sie ausgeführt werden können. Mithilfe von Anwendungsbeschränkungen pro Gerät lassen sich über entsprechende Richtlinien Lizenzmodelle steuern und durchsetzen.

Netzwerkzugangskontrolle für Anwendungen

Steuern Sie den Netzwerkzugriff ohne komplexe Steuerungen wie Router, Switches und Firewalls. Ausgehende Verbindungen von einem Zielgerät unterliegen den Berechtigungsregeln.

Verbindungen umfassen den Zugriff auf UNC-Pfade (einschließlich aller Dateien und Ordner auf diesem Laufwerk), Server, IP-Adressen, URLs, Geräte und FTP-Adressen. Richtlinien können flexibel angepasst werden, um dynamisch in Abhängigkeit von Benutzer- oder Geräteeigenschaften zu wirken.

URL-Umleitung

Falls ein Webbrowser auf einer Webseite oder webbasierten Anwendung offen gelassen wurde und der Anwender sich über ein anderes Endgerät wieder einloggt, wird der Browser zu einer sicheren, vordefinierten Adresse weitergeleitet.

Bei einer Weiterleitung können Variablen definiert und Regeln erstellt werden, welche URLs gesperrt und/oder weitergeleitet werden sollen.

Selbstautorisierende Benutzer

Dedizierten „Power-Usern“ kann die Berechtigung erteilt werden, selbst eingeführte Anwendungen auszuführen. Für Abwesenheiten kann man seinen Benutzern erlauben, Anwendungen ohne Zutun des IT-Supports auf einem abgesicherten Computer zu installieren. Eine umfassende Überprüfung erfasst genaue Informationen wie Anwendungsname, Datum und Uhrzeit der Ausführung und Gerät; darüber hinaus kann eine Kopie der Anwendung zur Untersuchung zentral gespeichert werden.

Berechtigung für web-basierte Installationen

Verwaltung einer „Whitelist“ von zugelassenen Webseiten, von denen Anwender berechtigt sind, Software zu installieren, beispielsweise bekannte Webseiten wie www.adobe.com und www.gotomeeting.com. Dadurch erhalten Benutzer Zugriff auf Geschäftsanwendungen wie Adobe Reader, Adobe Air, Adobe Flash Player und den GoToMeeting-Client für Webkonferenzen, und IT-bedingte Engpässe bei der Anwendungsbereitstellung oder Produktivitätseinbußen werden vermieden.

Kontrolle von anwendungsbasierten Installationen

Einige Organisationen benötigen möglicherweise eine höhergradig granulare Kontrolle, wenn Anwender bestimmte Applikationen von autorisierten Webseiten installieren. Ein IT-Administrator kann z. B. die Installation von Adobe Reader erlauben, aber alle anderen Anwendungen von www.adobe.com sperren. Es können aber auch spezifische „Whitelist“-Anwendungen innerhalb der Webseite nach Version und ActiveX-Steuerelement-Klassen-ID in eine Whitelist aufgenommen werden. Dies gewährleistet, dass nur vertrauenswürdige Versionen bestimmter Anwendungen aus dem Internet von den Anwendern installiert werden.

Unternehmensfähige Änderungsverfolgung und Kontrolle

Erfassen Sie detaillierte Protokollinformationen über kontinuierliche Änderungen an zentralen Anwendungskontroll- und Benutzerrechtsverwaltungsrichtlinien. Die Änderungsprotokolle sind passwortgeschützt, um Manipulationen vorzubeugen.