

FILE SYSTEM AUDITOR™

Versuchen Sie einmal herauszufinden, wer gestern auf Ihre vertraulichen Daten zugegriffen hat. Gar nicht so einfach? Sie sollten sich fragen, ob Sie den Standards von IT-Verwaltung und Richtlinien einhaltung wirklich gerecht werden. System-eigene Tools stellen Ihnen zahllose Ereignisprotokolleinträge ohne Logik oder Zusammenhang zur Verfügung. Jetzt gibt es eine Lösung: File System Auditor von ScriptLogic gibt Ihnen die Möglichkeit, den Datenzugriff auf NTFS-Dateisysteme schnell und einfach zu überwachen und Berichte und Warnungen zu erstellen.

Heutzutage geht es bei Richtlinienstandards vor allem um den Schutz vor Missbrauch von Kunden-, Finanz und Patientendaten. Durch den Einsatz von NTFS-Sicherheitsstandards kann zwar der Zugriff auf Dateien eingeschränkt werden, Unternehmen müssen jedoch auch die Möglichkeit haben, diese Zugriffsbeschränkungen zu überprüfen und möglichen Datenmissbrauch durch legitime Benutzer zu verfolgen. Dies kann nur mit einem Überwachungspfad der Dateiaktivität erreicht werden. File System Auditor bietet Ihnen folgende Funktionen: Aufzeichnen der Dateiaktivitäten auf untersten Ebenen, zentrale unternehmensweite Speicherung der überwachten Ereignisse, Bereitstellen eines Berichts- und Filter-Frameworks sowie E-Mail-Warnungen bei bestimmten Dateisystemereignissen, z. B. fehlgeschlagenen Zugriffsversuchen oder Änderungen an einem bestimmten Satz von Daten.

INTELLIGENTE ÜBERWACHUNG

Mit File System Auditor werden nicht viele einzelne Überwachungseinträge umständlich durchsucht, sondern mehrere zusammengehörige Ereignisse werden sinnvoll

kombiniert und als einzelnes überwacht Transaktionsereignis dargestellt, z. B. das Verschieben einer Datei von einem Ordner in einen anderen. Dadurch kann der Administrator die gesuchte Antwort schneller finden, und Sie haben die Größe der Überwachungsdatenbank im Griff.

FLEXIBLE BERICHTERSTATTUNG

File System Auditor bietet Echtzeit-Berichterstattung, geplante Berichterstattung und Berichterstattung bei Bedarf. IT-Unternehmen verfügen so über Berichterstattungsoptionen, die gleichermaßen für Administratoren wie für Sicherheitsmanager und Leiter von IT-Bereichen geeignet sind. Berichtsauswahlen können gespeichert und für spätere Überwachungen erneut verwendet werden.

VEREINFACHTE RICHTLINIENEINHALTUNG

Durch Berichte über die Sicherheit der kritischen Daten Ihres Unternehmens und die Möglichkeit, Missbrauch und Manipulation geschützter Informationen zu untersuchen, wird die Einhaltung von vorgeschriebenen Richtlinienstandards wie HIPAA, SOX, GLBA und CISP in Ihrem Unternehmen vereinfacht.

SICHERHEITSSZYKLUS-SCHEMA

Bewerten	Zuweisen	Überwachen
Verfügbarkeit	Verantwortlichkeit	Sicherheit

<http://www.scriptlogic.com/slm>

HAUPTVORTEILE

Einhalten von Richtlinienanforderungen
HIPAA, SOX, GLBA, CISP und andere Standards erfordern Zugriffskontrollen für Finanz-, Kunden- und Patientendaten. FSA zeigt an, dass Kontrollen eingerichtet sind, und unterstützt Sie bei der Verfolgung von Datenmissbrauch und -manipulation.

Verbesserte Serversicherheit
Das Überwachen der Verwendung eines Dateisystems ermöglicht Administratoren, die Wirksamkeit der Sicherheitskontrollen zu überprüfen.

Sicherer Überwachungspfad
Überwachungsereignisse werden in einer SQL-Datenbank mit einem gesicherten Verlaufsdatensatz der Datei-Zugriffsereignisse gespeichert.

HAUPTFUNKTIONEN

Zentrale Berichterstattung
Überwachte Ereignisse werden in einer zentralen MSDE- oder SQL-Datenbank gespeichert. Berichte können bei Bedarf oder geplant erstellt und per E-Mail gesendet werden.

Echtzeitüberwachung und -benachrichtigung
Ein Dateisystemtreiber ermöglicht Echtzeitüberwachung. Berichte können zwecks schneller Benachrichtigung so geplant werden, dass sie alle 5 Minuten ausgeführt werden.

Intelligente Überwachung
File System Auditor interpretiert zusammengehörige Ereignisse und zeigt sie als einzelnen Überwachungseintrag an.

SYSTEMANFORDERUNGEN

Audit Collection
Windows 2000/2003-Dateiserver
MSDE oder SQL 2000/2005-Datenbank

Reporting and Alerting Console
Jeder Computer mit Windows 2000/XP/2003

LIZENZIERUNG

File System Auditor wird **pro Server** lizenziert. Auf unsere Website finden Sie Informationen zu internationalen Niederlassungen.

Weitere Informationen zu Preisen erhalten Sie bei Ihrem ScriptLogic-Händler oder bei ScriptLogic unter der Telefonnummer **001.800.813.6415** oder **001.561.886.2420**.

Mit der benutzerfreundlichen Oberfläche von File System Auditor können Unternehmen den Zugriff auf wichtige Firmendaten ganz einfach einrichten und überwachen, sowie Berichte über den Zugriff zu erstellen und so die Richtlinien einhaltung sicherstellen.

Time	Account	Event	Path
006 11:13:44 AM	Administrator...	Folder - Renamed	C:\Shared Files\New Folder
006 11:14:12 AM	Administrator...	Folder - Renamed	C:\Shared Files\Payroll
006 11:14:24 AM	Administrator...	Folder - Modified Security	C:\Shared Files\Accounts Payable
006 11:14:24 AM	Administrator...	File - Read	C:\Shared Files\My Documents\Desktop.ini
006 11:15:14 AM	Administrator...	File - Created	C:\Shared Files\Accounts Payable\New Microsoft Exc
006 11:15:14 AM	Administrator...	File - Modified	C:\Shared Files\Accounts Payable\New Microsoft Exc
006 11:15:26 AM	Administrator...	File - Renamed	C:\Shared Files\Accounts Payable\New Microsoft Exc
006 11:15:35 AM	Administrator...	File - Created	C:\Shared Files\Accounts Payable\SS142000
006 11:15:35 AM	Administrator...	File - Modified	C:\Shared Files\Accounts Payable\SS142000
006 11:15:35 AM	Administrator...	File - Modified Security	C:\Shared Files\Accounts Payable\SS142000
006 11:15:35 AM	Administrator...	File - Created	C:\Shared Files\Accounts Payable\Companies to Pay