netwrix

Netwrix Auditor

WER hat WAS WANN und WO in ihrer IT-Infrastruktur geändert? Wer hat Zugriff worauf?
Netwrix macht das Transparent. Umfassend.

01
Produktüberblick

Netwrix Auditor macht durch die Lieferung entscheidungsrelevanter Daten klar sichtbar, wer was wann und wo in ihrer IT-Infrastruktur geändert hat. Netwrix Auditor hilft Sicherheitslücken aufzudecken, die auch meist durch Insider genutzt werden, Audits einzuhalten und Compliance-Kosten zu minimieren, oder auch einfach im Auge zu behalten was privilegierte Nutzer in der IT-Umgebung tun.

Netwrix Auditor erlaubt das Audit für eine Vielzahl von IT-Systemen, darunter Active Directory, Exchange, Dateiserver, SharePoint, SQL Server, VMware und Windows Server. Mittels activity video recording können selbst Aktivitäten von privilegierten Nutzern in anderen Systemen überwacht werden, selbst wenn diese Systeme keine Protokolle ausgeben.

> *Wir haben schnell die Vorteile von Netwrix erkannt. Regelmäßige Berichtserstattung helfen uns interne Regeln und Sicherheitsanforderungen einzuhalten, und besonderes , die kontinuierliche Überwachung hilft uns schnelle eventuelle Sicherheitsvorfällen an die Zentrale zu melden. Somit war unsere Wahl eindeutig.*

Nigel Lim, IT Manager, ADEKA Singapore Pte Ltd
Read the success story: www.netwrix.com/go/adeka

02 Anwendungen

Netwrix Auditor for Active Directory

Netwrix Auditor for Exchange

Netwrix Auditor for File Servers
ermöglicht auch die Überwachung von EMC und NetApp

Netwrix Auditor for SharePoint

Netwrix Auditor for SQL Server

Netwrix Auditor for VMware

Netwrix Auditor for Windows Server
ermöglicht die Überwachung von Event Logs, Syslog,Cisco, IIS, DNS und mehr

Netwrix Auditor unterstützt auch die Überwachung der Aktivitäten von priviligierten Nutzern in allen anderen Systemen, selbst wenn diese Systeme keine Protokolle ausgeben, durch die Videoaufzeichnung mitder Möglichkeit aufzur ufen und abzuspielen.

03 Vorteile

Verstärkung der Sicherheit

Erkennen von Insider Angriffen durch plötzliche Veränderungen des Nutzerverhaltens, der Systemkonfiguration oder plötzliche Wechsel der Berechtigungen und der Mitgliedschaften, sowohl ungewöhnliche Zugriffsversuche.

Untersuchung von sicherheitsrelevanten Zwischenfällen und Verhinderung von Sicherheitslücken durch die Analyse von strukturellen Auffälligkeiten und Änderungen der Sicherheitseinstellungen oder besonders geschützten Inhalten, sowie Zugriffen auf wichtige Unternehmensressourcen.

Herausfiltern von allen nichtrelevanten Auditdaten durch unsere systeminternen Prüffunktionen mithilfe der AuditAssurance™-Technologie.

Vereinfachung derCompliance

Implementierung und Validierung interner Kontrollmechanismen, die sich aus den verschiedensten Vorschriften, Normen und Standards ergeben.

Out-of-the-box Zugriff auf Berichte, wie PCI DSS, HIPAA, SOX, FISMA/ NIST800-53, COBIT, ISO/IEC 27001 u. a. Compliance-Audits.

Langzeitarchivierung der vollständigen Prüfdaten, damit Auditoren auch später noch regelmäßig Prüfungen vornehmen und das während des gesamten Aufbewahrungszeitraums. Schnellster Zugriff auf Prüfdaten.

Optimierung der Prozesse

Automatisierung von zeitaufwändigen manuellen Aufgaben im Zusammenhang mit der Erstellung von Ereignisberichten und der Überwachung von Zugriffsberechtigungen.

Minimierung von System- und Ausfallzeiten durch die Behebung von Störungen, die durch menschliche Fehler verursacht wurden, und die Wiederherstellung der Systemkonfiguration, bei fehlerhaften Änderungen.

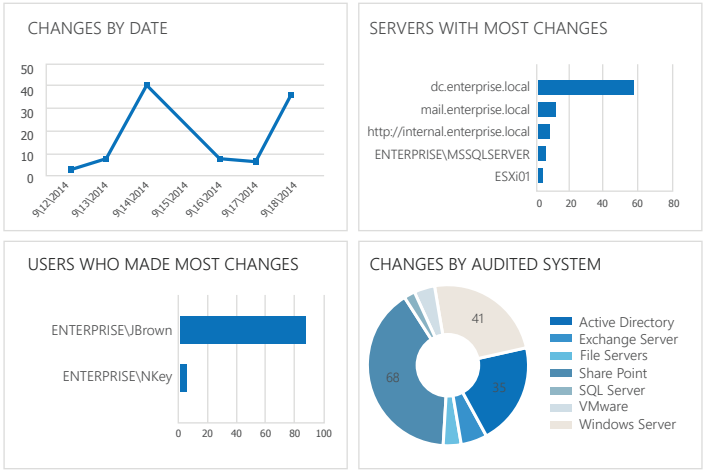
Einfache Analyse von Fehlerursachen durch die Untersuchung von Ereignisabfolgen und die Feststellung der zugrunde liegenden Ursachen.

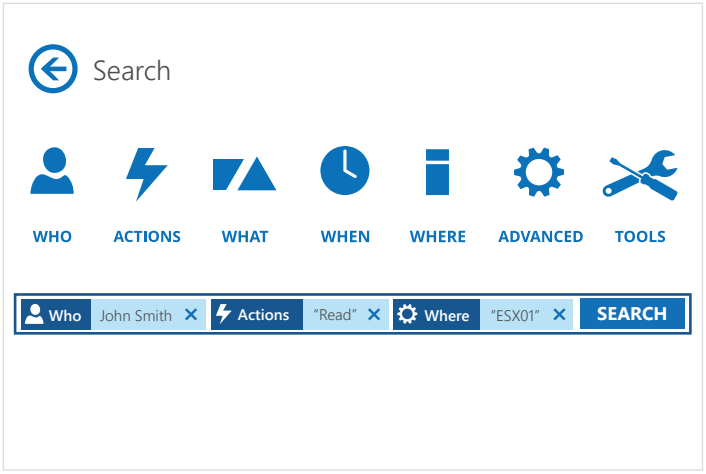
Vereinheitlichung der Überwachung für die gesamte IT-Infrastruktur, wodurch der zusätzliche Zeit- und Kostenaufwand für die Schulung von Mitarbeitern für verschiedene Standalone-Systeme entfällt.

04
Sorge für mehr Sicherheit

Verdächtige Aktionen frühzeitig erkennen

Verschaffen Sie sich mit den Enterprise Overview Dashboards einen Überblick über das Tun der Mitarbeiter innerhalb der gesamten IT- Infrastruktur. Hier sehen Sie beispielsweise, wie oft Änderungen vorgenommen werden, welche Nutzer verdächtige Aktionen durchführen oder welche Systeme davon betroffen sind.





Verdächtige Aktionen untersuchen

Wenn Sie eine Änderung entdecken, die nicht den Sicherheitsvorschriften des Unternehmens entspricht, können Sie mit Interactive Search feststellen, was vorgefallen ist und wie sich ähnliche Vorkommnisse künftig verhindern lassen.

05
Sorge für mehr Sicherheit

Berechtigungen überwachen und sensible Daten schützen

Verschaffen Sie sich einen Überblick über die Berechtigungen, die für eine bestimmte Datei oder einen bestimmten Ordner vergeben wurden und sorgen Sie dafür, dass nur Mitarbeiter mit entsprechender Befugnis Zugriff auf verschiedene Dateien haben.

Object Permissions by Object

Shows accounts with their inherited or explicitly assigned basic permissions allowing them to access folders and subfolders, results are grouped by object path.

Folder path: \Enterprise\Users\/ dministrator\Documents\Shared Documents\Accounting\Invoices

User Account	Permissions	User Permissions Inheritance
Enterprise\Administrators	List folder/ read data Read attributes Read extended attributes Read permissions Change permissions	Explicit
Enterprise\JSmith	List folder/ read data Read attributes Read extended attributes Read permissions Change permissions	Explicit

Failed Read Attempts

Shows unauthorized file access attempts. This report can be used for compliance audit to show that all unauthorized data access activities are traceable and easily auditable.

Action	Object Type	What	Who	When
Read (Failed Attempt)	**File**	\finance\cardholders\JSmith.txt	ORG\BGreen	9/26/2014 3:03:08 PM
Where:	NY-025-M			
Read (Failed Attempt)	**File**	\accounting\statements\2014.xls	ORG\SBlack	10/1/2014 9:01:18 PM
Where:	NY-018-G			
Read (Failed Attempt)	**File**	\hr\salary\ADavis.txt	ORG\NRed	9/26/2014 6:11:32 PM
Where:	NY-005-L			

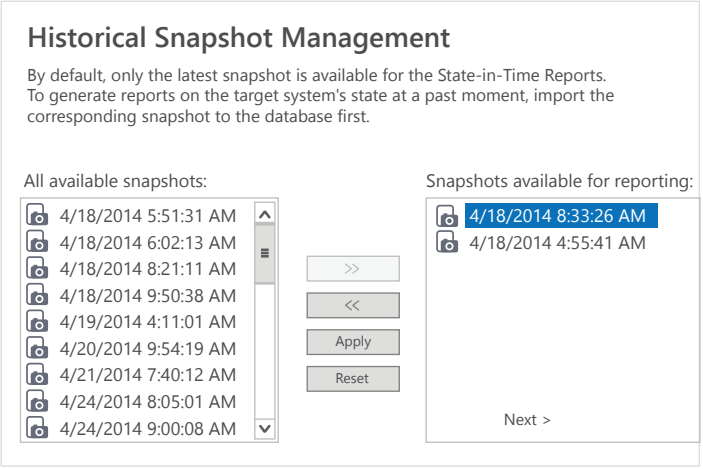
Zugriffsversuche überwachen

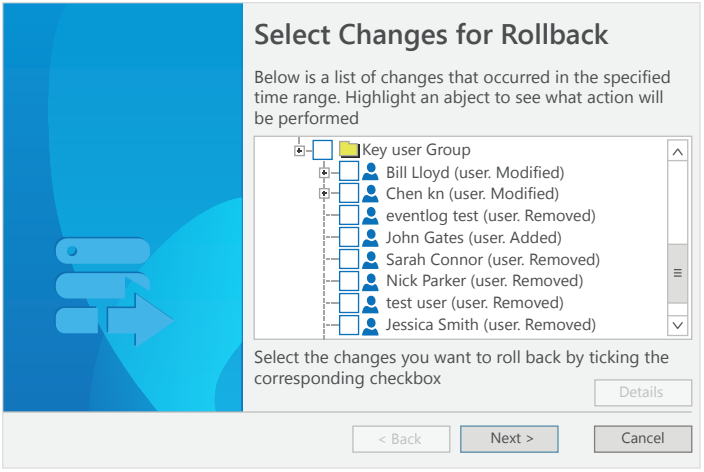
Stellen Sie fest, wer auf vertrauliche Dateien zugreifen will, und lassen Sie sich dazu tagesgenaue Berichte ausgeben. Ganz gleich, ob es sich um Kreditkartnerinhaber, medizinische Dokumente oder Finanzberichte handelt, mit Netwrix Auditor wissen Sie, wer wann wo versucht hat, die entsprechenden Dateien zu lesen oder zu ändern.

06
Sorge für mehr Sicherheit

Systemkonfigurationen jederzeit prüfen

Mit den State-in-time™-Berichten können Sie die Konfigurationseinstellungen jederzeit einsehen, z.B. Gruppenmitgliedschaft oder Passwortrichtlinien, wie wurden die vor einem Jahr konfiguriert. Mit dieser Art der Informationen können Sie sicher sein, dass Systeme "gesperrt" und weniger risikoanfällig sind.





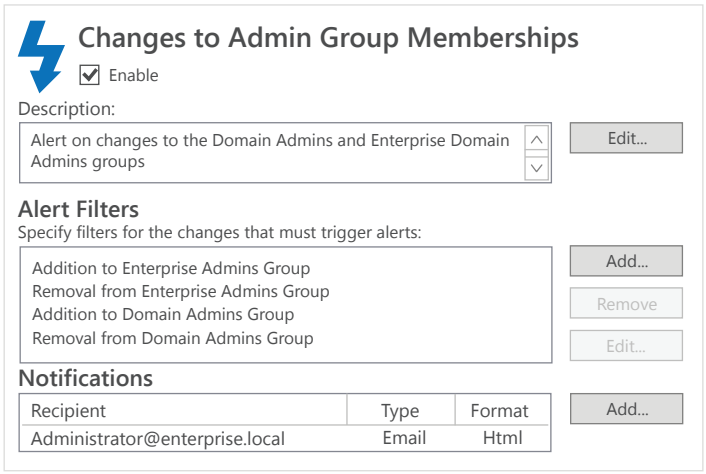
Fehlerhafte Systemkonfigurationen wiederherstellen

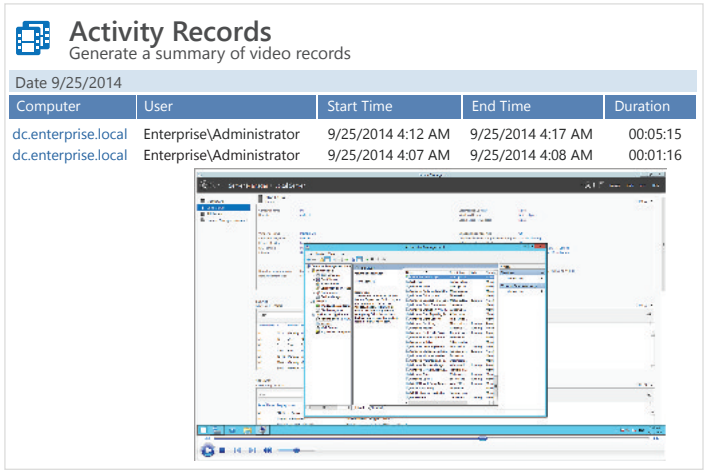
Falls Einstellungen unbefugt oder vorsätzlich geändert werden, können Sie die Änderungen rückgängig machen und auf einen früheren Konfigurationsstand zurückgehen, ohne dass das System ausfällt oder aus einem Backup wiederhergestellt werden muss. So haben Sie eine ganz unkomplizierte Möglichkeit, „die Zeit zurückzudrehen“, um sicherheitsgefährdende oder versehentliche Systemänderungen rückgängig zu machen.

07
Sorge für mehr Sicherheit

Meldung von kritischen Änderungen

Lassen Sie sich über unbefugte Konfigurationsänderungen informieren, sobald diese vorgenommen werden. Dadurch wissen Sie genau, wann es zu der Änderung gekommen ist – beispielsweise, dass zu einem bestimmten Zeitpunkt eine Person zu der Gruppe Enterprise Admins oder Domain Admins hinzugefügt wurde – und können das entsprechende Sicherheitsrisiko sofort ausschalten.





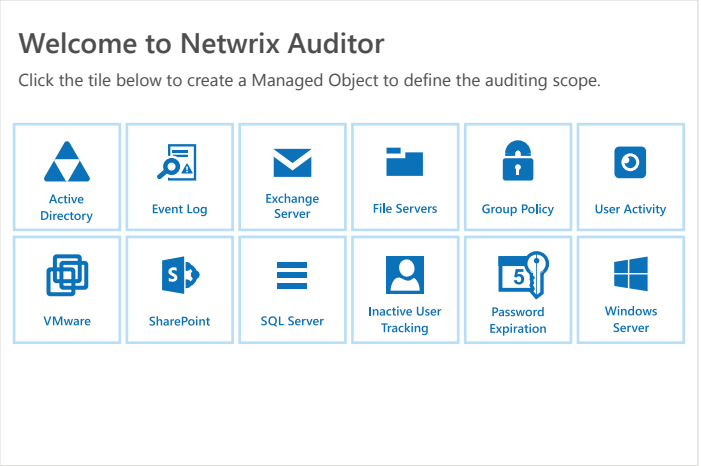
Dinge erkennen, die sich sonst nicht erkennen lassen

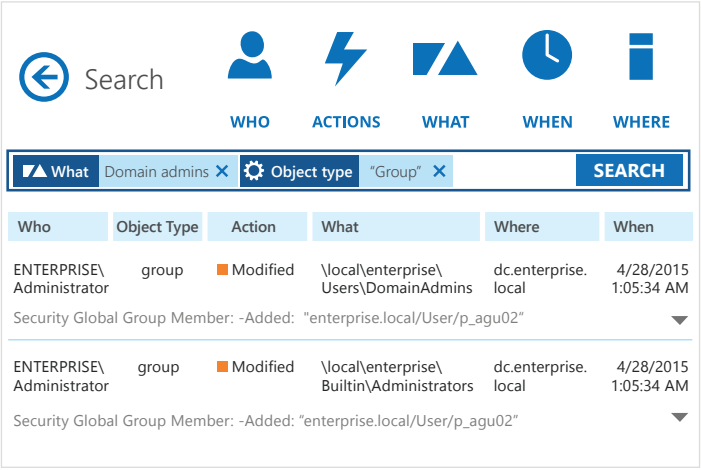
Auch wenn ein System keine Protokolle ausgibt, bietet Netwrix Auditor die Möglichkeit, die Nutzeraktionen durch Videoaufzeichnungen zu überwachen. Diese können gezielt aufgerufen und abgespielt werden.

08
Vereinfachung der Compliance

Sicherheitskontrollen in der gesamten IT-Infrastruktur ermöglichen

Durch die Unterstützung einer Vielzahl von Plattformen ermöglicht Netwrix Auditor die komplette Sicherheitskontrollen der gesamten IT-Infrastruktur durch ein einziges Tool.





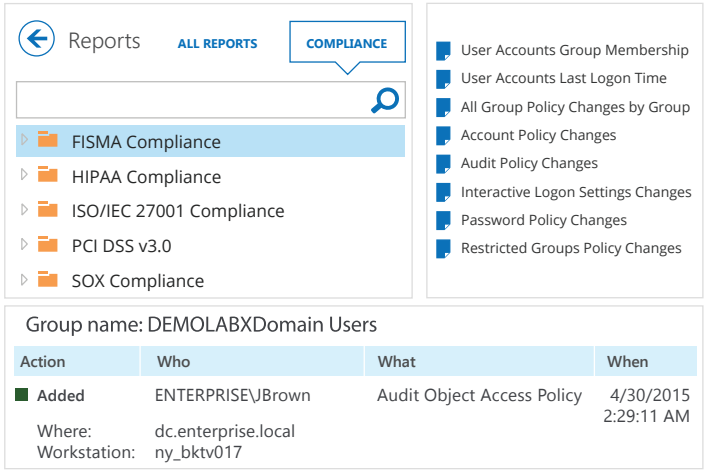
Fragen des Prüfers schneller beantworten

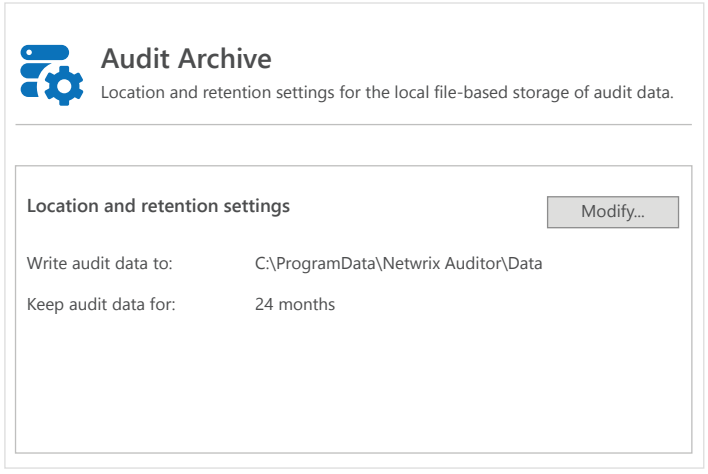
Mit Netwrix Auditor haben Sie schnell Antworten auf die Fragen des Prüfers parat und können ihm sagen, wer wem umfassendere Rechte eingeräumt hat und welche Änderungen in der Enterprise Domain Admins-Gruppe vor einem Jahr vorgenommen wurden. Was Sie früher Wochen gekostet hat, ist mit Netwrix Auditor in fünf Minuten erledigt.

09
Vereinfachung der Compliance

Out-of-the-box Compliance-Berichte

Wenn Sie bei einer Compliance-Prüfung nachweisen müssen, dass bestimmte Prozesse und Kontrollmechanismen bestehen (und bereits in der Vergangenheit vorhanden waren), können Sie dies Anhand von Daten belegen. Netwrix Auditor liefert Ihnen sofort verwendbare Berichte, die die spezifischen Anforderungen der jeweiligen Compliance-Standards erfüllen. Zu diesen gehören u. a. PCI DSS 3.0, HIPAA, SOX, FISMA/NIST800-53 und ISO/ IEC 27001.





Prüfpfade dokumentieren und für viele Jahre speichern

Mithilfe der zweistufigen AuditArchive™-Speicherung (dateibasiert + SQL-Datenbank) lassen sich Prüfdaten für einen Zeitraum von mehr als 10 Jahren in einem komprimierten Dateiformat archivieren. Dabei kann jederzeit schnell und einfach auf die Daten zugegriffen werden.

10
Optimierung des Betriebs

Änderungen in der IT-Umgebung überwachen

Verfolgen Sie, wer genau welche konkreten Änderungen vorgenommen hat, und verschaffen Sie sich einen Überblick über die Werte vor und nach der Änderung. Diese Informationen stehen für alle Systeme wie Active Directory, Group Policy, Exchange, Dateiserver, SharePoint, SQL Server, VMware und Windows Server zur Verfügung.

All Changes by User

Shows all changes across the entire IT infrastructure grouped by the users who made the changes.

Who Changed: CITY\Megan

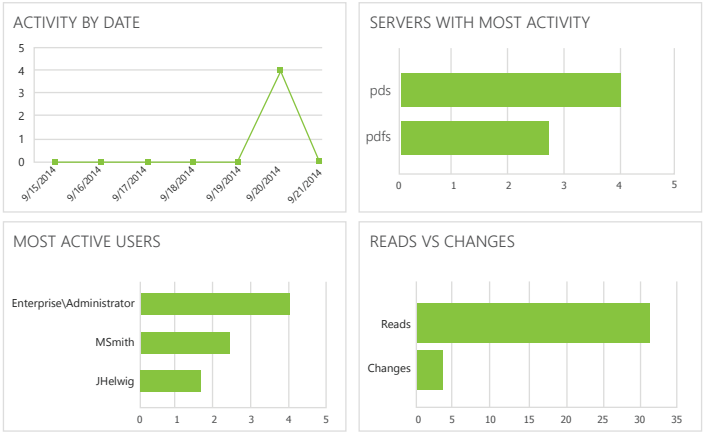
Audited System: Active Directory

Action	Object Type	What	When
Modified	**User**	\local\city\People\Bill	9/10/2014 4:31:49 AM
Where:	Chicago.city.local Principal Name set to "Bill@city.local"		

Audited System: VMware

Action	Object Type	What	When
Removed	**VirtualMachine**	\ha-folder-root\ha-datacenter\vm	9/10/2014 8:47:37 AM
Where:	https://10.04.48:43		

File Servers Overview



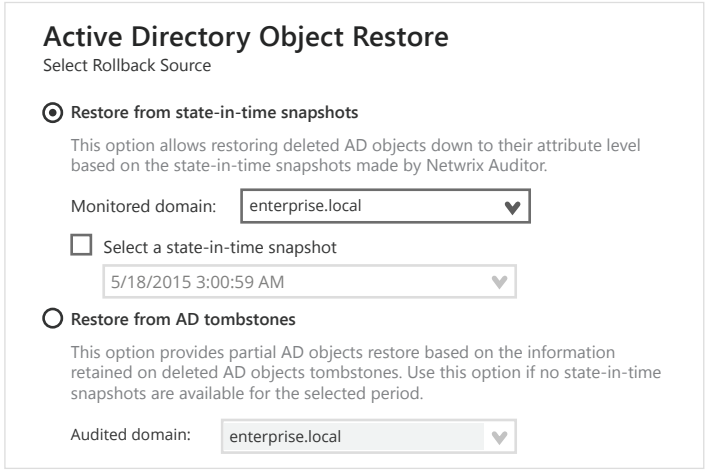
Einfaches Berichtswesen

Mit Netwrix Auditor gehören die manuelle Überprüfung zahlloser Ereignisprotokolle oder die Erzeugung von PowerShell-Berichten, aus denen hervorgeht, was sich in der IT-Umgebung verändert hat, wer welche Berechtigungen hat, welche Nutzer inaktiv sind und wessen Passwörter demnächst ablaufen, endlich der Vergangenheit an. Nutzen Sie mehr als 150 Berichtsvorlagen und Dashboards mit zahlreichen Möglichkeiten zum Filtern, Gruppieren, Sortieren und Exportieren (PDF, XLS, usw.) sowie die E- Mail- Abonnements von Netwrix Auditor.

11
Optimierung des Betriebs

Berichte schneller bereitstellen und Zeit sparen

Mit Netwrix Auditor müssen Sie nicht mehr unzählige Berichtsanfragen aus verschiedenen Abteilungen bearbeiten, sondern können allen Mitarbeitern, die darauf angewiesen sind, direkten und uneingeschränkten Zugriff auf entscheidungsrelevante Berichte einräumen.



Systemausfallzeiten minimieren

Falls eine unbefugt vorgenommene Änderung die Systemverfügbarkeit beeinträchtigt, können Sie die Änderung schnell rückgängig machen und auf einen früheren Konfigurationsstand zurückgehen, ohne dass das System dadurch ausfällt oder aus einem Backup wiederhergestellt werden muss.

12
Optimierung des Betriebs

Konzentration auf das, was wirklich zählt

Lassen Sie sich über die wichtigsten Konfigurationsänderungen informieren, sobald diese vorgenommen werden. Entscheiden Sie, über welche Änderungen sie informiert werden wollen – beispielsweise können Sie Netwrix Auditor so einrichten, dass Sie eine Meldung erhalten, sobald es zu Änderungen bei den Mitgliedern der Gruppen Enterprise Admins oder Domain Admins kommt.

Tue 11/25/2014 6:22 AM
Administrator@enterprise.local

Alert Changes to Admin Group Memberships at ENTERPRISE.LOCAL

Changes to Admin Group Memberships

Severity:	Critical
Domain:	ENTERPRISE.LOCAL
Change Type:	Modified
Object Type:	Group
When Changed:	11/25/2014 AM
Who Changed:	Enterprise\Administrator
Where Changed:	dc1.enterprise.local
Object Name:	\local\enterprise\Users\Domain Admins
Details:	Security Global Group Member: Added: "enterprise.local/Test/Nick Key"

All Group Policy Changes

Shows all changes to Group Policy objects, settings, GPO links and permissions with the name of the originating workstation from which a user made the change.

Action	What	Who	When
Modified	Default Domain Policy	Enterprise\Administrator	7/23/2015 7:55:11 AM
Where:	dc1.enterprise.local		
Workstation:	192.168.7.11		
Path:	Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/ Account Policies/Password Policy		
Modified	Policy: Enforce password history; Setting: 24 passwords remembered -> 3 passwords remembered;		
Modified	Modified Policy: Maximum password age; Setting: 20 days -> 200 days;		
Modified	Modified Policy: Minimum password length; Setting: 7 characters-> 4 characters;		

Fehlerursachen schneller finden und beseitigen

Netwrix Auditor liefert Ihnen aussagekräftige und entscheidungsrelevante Daten für die Untersuchung von Ereignisabfolgen und die Analyse von Fehlerursachen. Durch die zentrale Zugriffsmöglichkeit auf die gesamte Ereignishistorie können Sie schnell auf Probleme reagieren, die sich abzeichnen.

13 Bewältigung von IT- Aufgaben Ihrer Abteilung und Ihres Unternehmens

IT Administrator

Kann Audit- und Compliance-Berichte schneller erzeugen und zur Verfügung stellen.

Kann auffällige Nutzeraktionen untersuchen, bevor diese zu einer Sicherheitsverletzung werden.

IT Sicherheits-Administrator

IT Manager

Kann sich die Kontrolle über die IT-Infrastruktur zurückholen und dem nächsten Compliance-Audit entspannt entgegensehen.

Kann Sicherheitsrisiken mindern und die Compliance-Kosten minimieren.

CIO/CISO

MSP

Profitiert von einer transparenten gemanagten IT- Umgebung und kann seinen Kunden „Compliance as a Service" anbieten.

Analystenberichte

Gartner

"...Konfiguration-Audit-Tools können Ihnen helfen, Ihre Konfigurationen im Einklang mit den best pratices zu analysieren, Audit-Standards durchzusetzen und gesetzliche Anforderungen zu erfüllen..."

Redmond MAGAZINE

"...das Audit ist generell eine ziemlich schwere Aufgabe, besonders bei manueller Durchführung. Um all die zahlreichen Details, die Sie berücksichtigen und sich merken müssen, kümmert sich Netwrix Auditor..."

Windows IT Pro

"...das beste Active Directory/Group Policy Produkt und das beste Audit/ Compliance-Produkt 4 Jahren hintereinander..."

Petri IT Knowledgebase

“... 5 von 5 Sternen und für alle im AD-Umfeld empfohlen, auf den Fall probieren...”

14 Leistungsmerkmale

Überwachung von Änderungen, Konfigurationen und Zugriffsversuchen

Überwachung von Änderungen: Erkennung und Meldung aller Konfigurationsänderungen in der gesamten ITInfrastruktur mit Details Wer, Was, Wann, Wo und alten sowie die geänderten Werten.

Konfigurationsprüfung: State-in-time™-Berichte geben Aufschluss über die aktuellen sowie alle früheren Konfigurationseinstellungen, z. B. in Bezug auf Regeln, die vor einem Jahr für die Mitgliedschaft in Gruppen oder Passwörter festgelegt wurden.

Zugriffsüberwachung: Überwachung und Meldung von erfolgreichen oder fehlgeschlagenen Versuchen, auf Systeme und Daten zuzugreifen.

Überwachung der Aktivitäten von privilegierten Nutzern in jedem IT-System, selbst wenn diese keine Protokolle ausgeben mittels der Videoaufzeichnung, die aufgerufen und abgespielt werden kann.

Einheitliche Audit-Plattform

Einheitliche Plattform: Prüfung der gesamten IT-Infrastruktur von einer zentralen Konsole aus im Gegensatz zu den zahlreichen Standalone-Tools mühselig integriert werden mussten

AuditAssurance™: führt Prüfdaten aus zahlreichen, voneinander unabhängigen Quellen automatisch zusammen. Wenn wichtige Daten aus einer Quelle fehlen, ergänzt AuditAssuranceTM die erfassten Daten mit Informationen aus anderen Quellen. So erhalten Sie ein genaues, fehlerfreies Bild des Sachverhalts.

AuditIntelligence™: Wandelt komplexe, maschinell erstellte Prüfdaten in aussagekräftige und entscheidungsrelevante Berichte um.

AuditArchive™: Archiviert konsolidierte Prüfdaten für bis zu zehn Jahre und darüber hinaus in einem zweistufigen, skalierbaren Speichersystem (dateibasiert + SQL-Datenbank) und garantiert den schnellen und einfachen Zugriff Altdaten während des gesamten Aufbewahrungszeitraums .

Delegierter Zugriff auf Prüfdaten: Der Netwrix Auditor-Client kann auf einer unbegrenzten Anzahl an Rechnern installiert werden und bietet dann vollständigen Zugriff auf entscheidungsrelevante Informationen.

Agentenlose oder kompakte agentenbasierte Betriebsarten werden unterstützt.

15 Lesitungsmerkmale

Datensuche, Berichtsvorlagen, Meldungen und Dashboards

Interaktive Suche: Mit Netwrix Auditor können Sie Prüfdaten schnell sortieren und Suchkriterien verfeinern, bis Sie genau die Informationen erhalten, die Sie suchen. Exportieren Sie die Suchergebnisse oder erstellen einen individuellen Bericht für die spätere Verwendung.

Mehr als 150 Berichtsvorlagen bieten neben verschiedenen Filter-, Sortier- und Exportmöglichkeiten Darstellungen mit unterschiedlicher Detailtiefe, einen Webzugriff, eine fein abgestufte Berechtigungsstruktur u.v.m.

Out-of-the-box Compliance-Berichte: diese erfüllen die spezifischen Anforderungen der jeweiligen Compliance-Standards, darunter PCI DSS 3.0, HIPAA, SOX, FISMA/NIST800-53 und ISO/ IEC 27001.

Echtzeit-Meldungen informieren Sie über kritische Konfigurationsänderungen, unbefugte Versuche, auf sensible Daten zuzugreifen (gleich ob erfolgreich oder fehlgeschlagen), sowie andere, potenziell sicherheitsrelevante Ereignisse.

Dashboards verschaffen Ihnen einen vollständigen Überblick über das Geschehen in der IT-Infrastruktur des Unternehmens. Mit diesem Feature können Sie sich die Einzelheiten zu jeder Änderung anzeigen lassen, die in einem der überwachten Systeme aufgetreten ist. Hier sehen Sie beispielsweise, wie oft Änderungen vorgenommen werden, welche Nutzer verdächtige Aktionen durchführen oder welche Systeme davon betroffen sind.

SIEM, Rollback, FIM

Integration mit SIEM leitet optional aussagekräftige Ereignisdaten an ein vorhandenes SIEM-System weiter. Dadurch können die Möglichkeiten bestehender Prozesse besser ausgeschöpft, Investitionen in Technik geschützt und die Nutzung einer Vielzahl an Konsolen vermieden werden.

Event-Log-Management: Erfassung von nicht änderungsbezogenen Ereignissen aus Windows- und System-Protokollen (z. B. Anmeldung/Abmeldung, Kontosperren usw.).

Change Rollback: macht unbefugt oder vorsätzlich vorgenommene Änderungen rückgängig stellt den frühere Zustand wieder ohne dass das System ausfällt oder aus einem Backup wiederhergestelltwerden muss.

File Integrity Monitoring (FIM): überwacht Änderungen, die an kritischen Systemen, Dateien und Konfigurationen vorgenommen werden.

Gebaut für die IT-Umgebungen aller Größen, Netwrix Auditor-Architektur unterstütz auch das Wachstum Ihrer Organisa tion

HERITAGE BANK

Banking and Finance, 100 Mitarbeiter
Heritage Bank verlässt sich auf Netwrix Auditor, um die Sicherheit und Compliance-Richtlinien zu erfüllen.

belkin

Technology, 1,3K Mitarbeiter
Auch mit der IT-Erweiterung, kontrolliert Belkin Änderungen in Active Directory und Exchange Servermit Netwrix.

american career college®

Ausbildung, 5,5K Mitarbeiter
American Career College gewährleistet Campus Datensicherheit mit Netwrix Auditor for Active Directory.

L3

Aerospace & Defense, 45K Mitarbeiter
L-3 Communications benutzt Netwrix für Verfolgung der Änderungen in Active Directory und Group Policy zur Erfüllung von SOX-Compliance Anforderungen.

netwrix

Nächste Schritte

Kostenlose Demoversion: Richten Sie Ihre eigene Testumgebung ein.
netwrix.com/freetrial

Testen in der Cloud: virtueller POC zum Testen in einem von Netwrix gehosteten Labor netwrix.com/testdrive

Live Demo: Produkt-Tour mit einem Experten vonNetwrix
netwrix.com/livedemo

Nähere Informationen erhalten Sie von unserenVertriebsbeauftragten.
netwrix.com/contactsales

AUSZEICHNUNGEN

Alle Auszeichnungen:
netwrix.com/awards

Hauptsitz des Unternehmens:
300 Spectrum Center Drive, Suite 1100
Irvine, CA 92618

Tel.DE: + 49 711 899 89 187
Tel.CH: + 41 43 508 34 72
Handy: + 49 171 698 42 42

netwrix.com/social