netwrix

Netwrix Auditor

Visibilità completa su chi ha fatto cosa, quando, dove e chi ha accesso a cosa attraverso l'intera infrastruttura IT

netwrix.it

01
Descrizione del prodotto

Netwrix Auditor fornisce **visibilità completa** sia sulle configurazioni che sull'accesso ai dati all'interno dell'infrastruttura IT, mostrando dati di audit accurati su chi ha fatto cosa, quando, dove e chi ha accesso a cosa. Netwrix Auditor aiuta a prevenire le violazioni di sicurezza interne (insider-caused), a passare gli audit, minimizzare i costi di conformità, e semplicemente tenere sotto controllo ciò che gli utenti privilegiati stanno facendo nell'ambiente e perché lo fanno.

Netwrix Auditor è l'unica piattaforma che combina sia la gestione della configurazione della sicurezza che la governance di accesso ai dati attraverso **la più ampia varietà** di sistemi IT, incluso Active Directory, Exchange, File Servers, SharePoint, SQL Server, VMware e Windows Server. Supporta anche il monitoraggio dell'attività degli utenti privilegiati in altri sistemi, anche se non producono alcun log, tramite la registrazione video di attività degli utenti con capacità di ricerca e riproduzione.

> *"Avevamo bisogno di essere conformi alle normative internazionali dell'audit, e siamo stati istruiti dai nostri auditor per trovare una soluzione in grado di soddisfarli. Netwrix ci ha permesso di monitorare tutti gli aspetti critici della nostra infrastruttura IT, in modo da soddisfare i requisiti rigorosi degli auditor.*

Mervyn Govender, CIO, CreditEdge
Leggi il caso di studio: netwrix.com/creditedge

02
Applicazioni

Netwrix Auditor for Active Directory

Netwrix Auditor for Exchange

Netwrix Auditor for File Servers
Include l'audit di EMC e NetApp

Netwrix Auditor for SharePoint

Netwrix Auditor for SQL Server

Netwrix Auditor for VMware

Netwrix Auditor for Windows Server
Include l'audit di Event Logs, Syslog, Cisco, IIS, DNS e altro...

Netwrix Auditor supporta anche **il monitoraggio dell'attività degli utenti privilegiati in altri sistemi**, anche se non producono alcun log, tramite la registrazione video di attività degli utenti con capacità di ricerca e riproduzione.

03 Vantaggi

Aumenta la Sicurezza

Rilevate le minacce interne controllando le modifiche dei dati utente, configurazioni, autorizzazioni, appartenenze ai gruppi e tentativi di accesso.

Indagate sugli incidenti di sicurezza e prevenite le violazioni di informazioni attraverso l'analisi dei cambiamenti strutturali, modifiche di impostazioni di sicurezza o di qualsiasi contenuto specifico garantito e di accesso alle risorse organizzative critiche.

Superate i limiti delle soluzioni delle soluzioni di audit native colmando le lacune e eliminando il SNR nei dati dell'auditing utilizzando la tecnologia Audit Assurance™.

Semplifica il Processo di Compliance

Attuate e convalidate i controlli interni per una varietà di normative di compliance .

Accedete facilmente ai report richiesti per dimostrare che il programma di compliance IT è conforme a D.Lgs. 196/03, EU GDPR, PCI DSS, HIPAA, SOX, FISMA/NIST800-53, COBIT, ISO/IEC 27001 e altri.

Tenete audit trail archiviato fino e oltre 10 anni per ogni successiva revisione o per I controlli periodici degli auditor garantendo un rapido accesso ai dati di audit per tutto il periodo di detenzione.

Ottimizza le Operazioni

Automatizzate laboriosi attività manuali associati alla generazione di report su cosa sta accadendo nel proprio ambiente e sulle autorizzazioni degli utenti.

Diminuite il downtime dei sistemi e le interruzioni di servizio risolvendo i problemi causati da errore umano o da cambiamenti delle configurazioni non corretti.

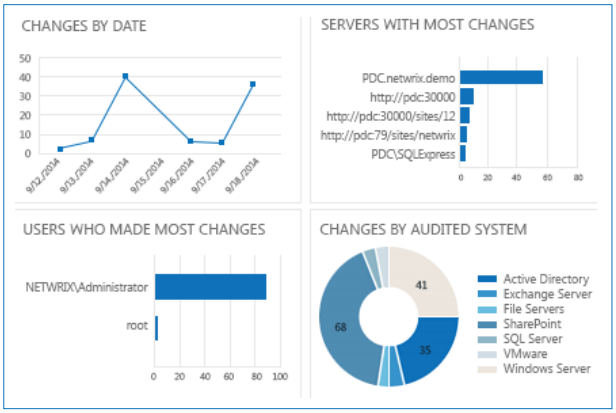
Semplifica l'analisi delle cause (Incident Management): indagando sequenze di eventi e determinandone la loro causa.

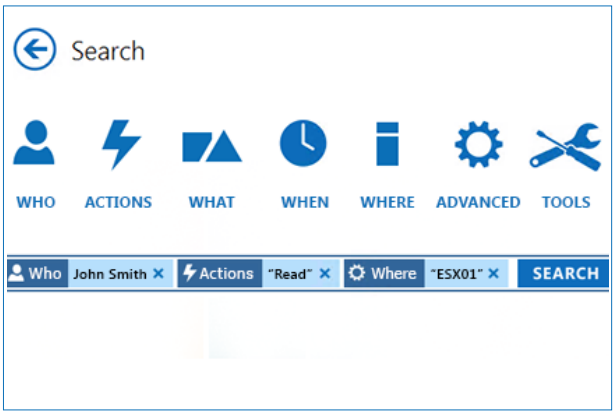
Unifica l'auditing attraverso l'intera infrastruttura IT, eliminando la necessità di ulteriori spese e corsi di formazione del personale sui molteplici prodotti indipendenti.

04
In Azione: Aumenta la Sicurezza

Rilevate Attività Sospetta nelle Fasi Iniziali

Ottenete una panoramica ad alto livello di attività dei dipendenti in tutta l'infrastruttura IT con Dashboard Globali. Scoprite quanto spesso vengono apportate le modifiche, quali utenti le stanno facendo, quali sistemi vengono influenzati, e altro.



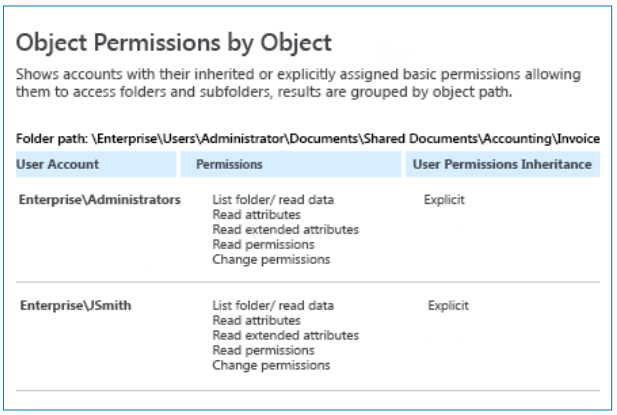


Investigate su Attività Sospette

Ogni volta che vedete un'azione che non corrisponde alla politica di sicurezza, siate certi che potrete capire perché è successo e evitare il ripetersi di simili incidenti.

Controllate le Autorizzazioni e Proteggete i Dati Sensibili

Assicuratevi che solo le persone giuste abbiano accesso ai dati appropriati, ottenendo un panorama completo delle autorizzazioni effettive per un file o una cartella specifica.



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.

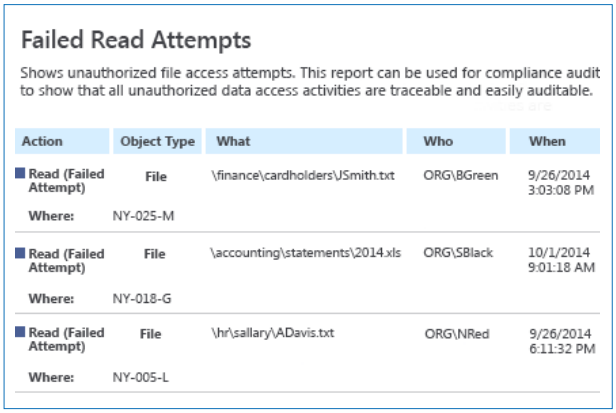
Folder path: \Enterprise\Users\Administrator\Documents\Shared Documents\Accounting\Invoice

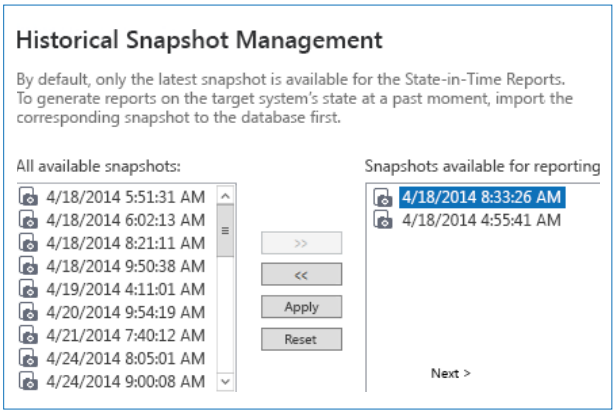
User Account	Permissions	User Permissions Inheritance
Enterprise\Administrators	List folder/ read data Read attributes Read extended attributes Read permissions Change permissions	Explicit
Enterprise\JSmith	List folder/ read data Read attributes Read extended attributes Read permissions Change permissions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

05
In Azione: Aumenta la Sicurezza

Monitorate i Tentativi di Accesso ai File

Scoprite chi sta cercando di accedere ai file confidenziali sottoscrivendo ai report giornalieri. Se si tratta di report fiscali, cartelle cliniche o di bilancio, Netwrix Auditor mostrerà chi ha cercato di leggere/modificare i file, quando e dove.



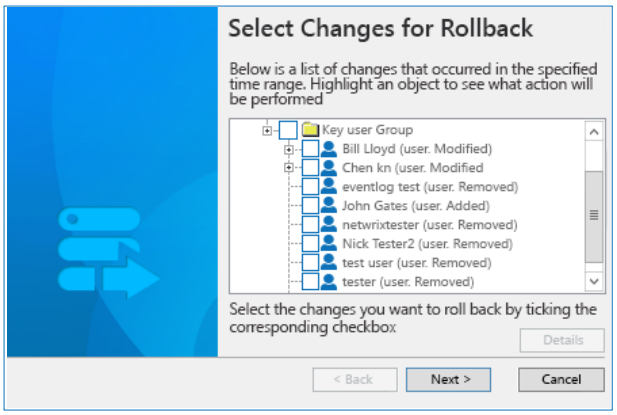


Controllate le Configurazioni del Sistema in Ogni Momento

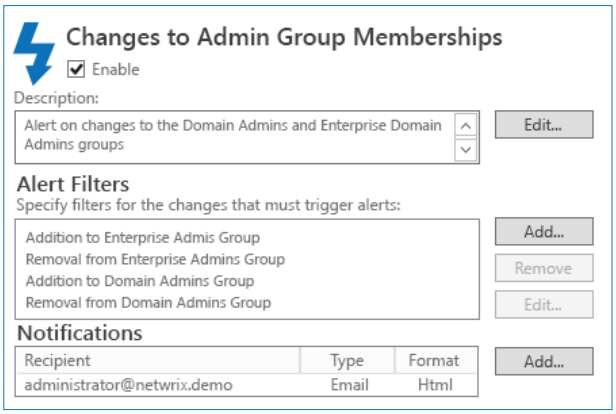
I report State-in-Time™ mostrano i parametri di configurazione in qualsiasi momento, per esempio - vedete le impostazioni di appartenenza al gruppo o di criteri di password, come erano configurati un anno fa. Con questo tipo di informazioni si può garantire che i sistemi siano "bloccati" e meno soggetti al rischio.

Recuperate Configurazioni del Sistema Danneggiato

Nel caso in cui una modifica non autorizzata o dannosa si verifica, potete ripristinare le impostazioni allo stato precedente senza alcun downtime o ripristino da un backup. In questo modo potete rapidamente "riposrtare indietro l'orologio" ai cambiamenti di sistema che indicano una minaccia alla sicurezza.



06
In Azione: Aumenta la Sicurezza

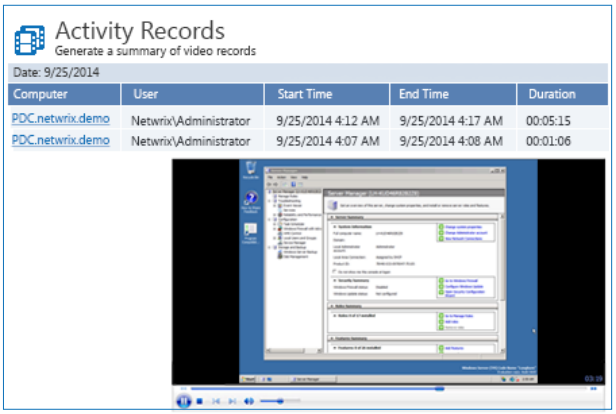


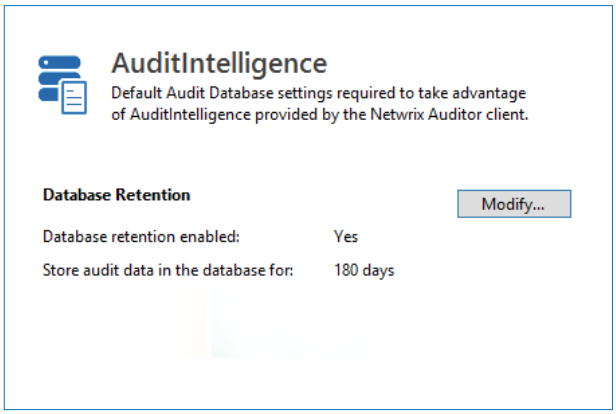
Ricevete gli Avvisi sulle Modifiche Critiche

Utilizzate gli avvisi per informarvi delle modifiche non autorizzate della configurazione nel momento in cui queste accadono. Prevenite le violazioni della sicurezza sapendo esattamente quando un cambiamento critico si verifica, per esempio - ricevete avvisi su quando qualcuno si aggiunge al gruppo Amministratori di Impresa/ Dominio.

Rilevate l'Inosservabile

Mantenete la visibilità di qualsiasi altro sistema, anche se non produce alcun registro, tramite la registrazione video dell'attività degli utenti con possibilità di ricercare e riprodurre il video in ogni momento.





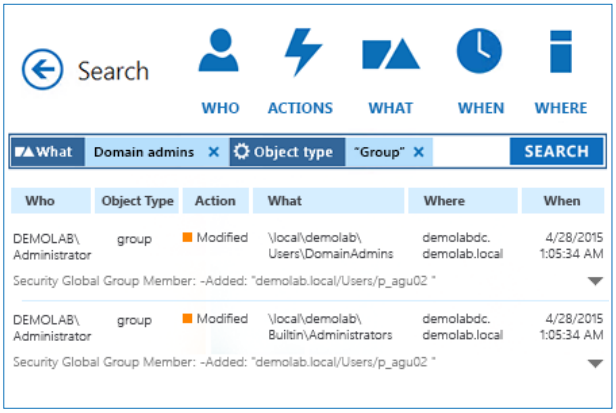
Archiviate un Audit Trail per Anni

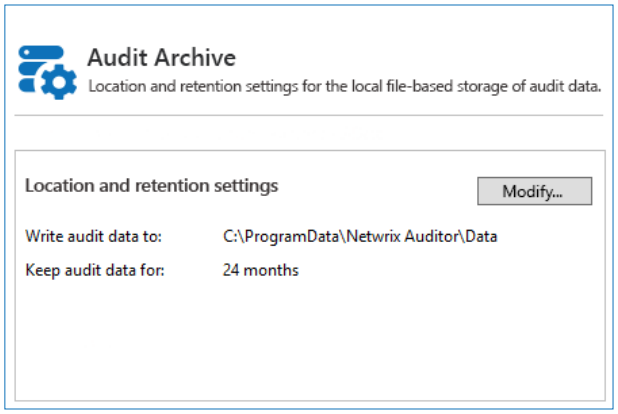
AuditArchive™, l'archiviazione scalabile a due livelli (basato su file + database SQL), permette di mantenere i dati di audit archiviati per gli indagini di sicurezza per 10 anni o più.

07
In Azione: Semplifica il Processo di Compliance

Affrontate le Domande degli Auditor più Velocemente

Trovate rapidamente le risposte alle domande degli auditor come chi ha effettuato l'elevazione di privilegi e cosa è stato cambiato nel gruppo amministratori di dominio un anno fa. Ora ci vogliono 5 minuti per ciò che prima richiedeva settimane di tempo.



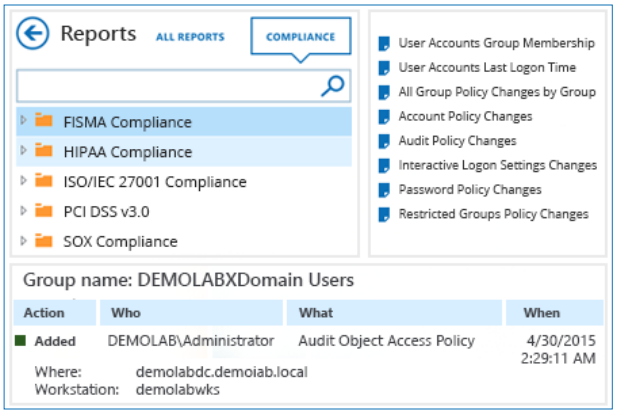


Archiviate un Audit Trail per Anni

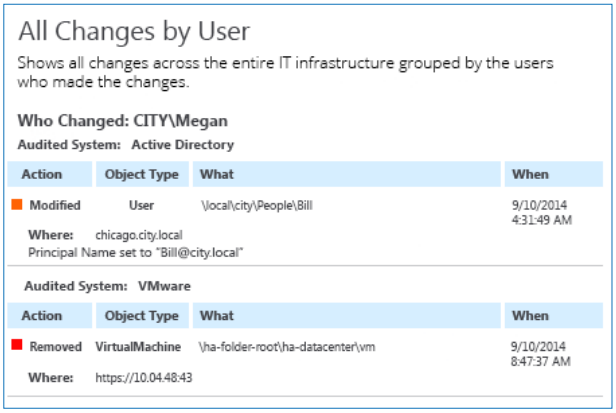
AuditArchive™, l'archiviazione scalabile a due livelli (basato su file + database SQL), permette di mantenere i dati di audit archiviati in formato compresso per 10 anni o più. I dati possono essere facilmente accessibili in qualsiasi momento.

Report su Compliance «Out-of-the-box»

Ogni volta che avete bisogno di dimostrare agli auditor che i processi e controlli specifici previsti sono eseguiti correttamente, potete dimostrarlo con i dati. Netwrix Auditor Vega fornisce i report che rispondono alle esigenze specifiche delle normative di compliance, tra cui PCI DSS 3.0, HIPAA, SOX, FISMA / NIST e ISO.



08
In Azione: Ottimizza le Operazioni

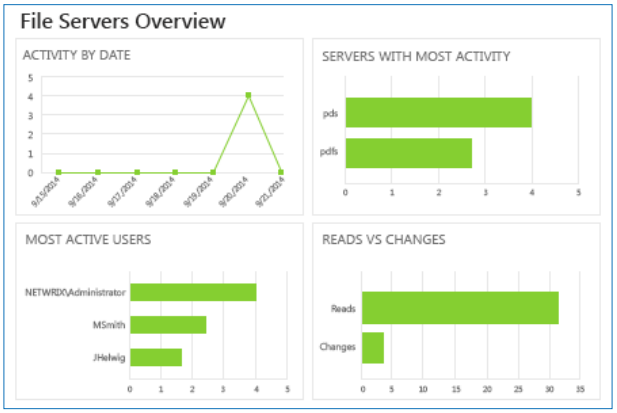


Tenete sotto Controllo i Cambiamenti nell'Ambiente

Scopri quando è stata apportata la modifica specifica, chi l'ha fatta e che cosa è stato cambiato con cronologia completa su "prima e dopo" ogni modifica effettuata in Active Directory, Group Policy, Exchange, File Server, SharePoint, SQL Server, VMware e Windows Server.

Semplificate il Reporting

Non è necessario rivedere manualmente numerosi eventi o utilizzare PowerShell per generare i report su cosa sta cambiando nel vostro ambiente, chi ha le autorizzazioni a cosa, quali utenti sono inattivi, le password che stanno per scadere. Ottenete l'accesso a oltre 150 report predefiniti e dashboard con filtraggio, raggruppamento, ordinamento, l'esportazione (PDF, XLS, ecc), iscrizioni e-mail e altro.



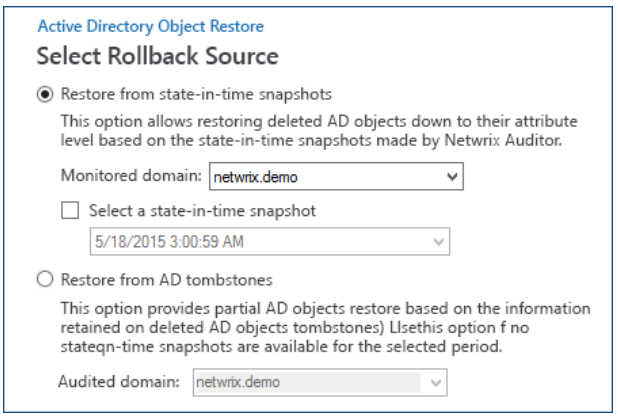
Risparmiate Tempo su Consegna di Report

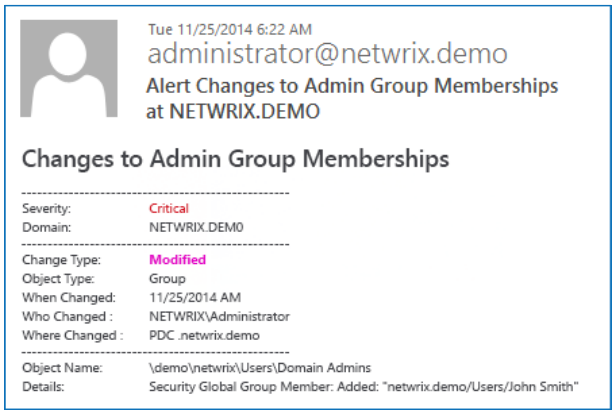
Abilitate l'accesso ai dati di audit accurati per le persone interessate quando ne hanno bisogno invece di affrontare le numerose richieste di report provenienti da diversi dipartimenti.

09
In Azione: Ottimizza le Operazioni

Minimizzate i Downtime di Sistema

Nel caso in cui una modifica non autorizzata o dannosa si verifica, potete rapidamente "riportare indietro l'orologio" e ripristinare le impostazioni allo stato precedente senza alcun downtime o ripristino da un backup.



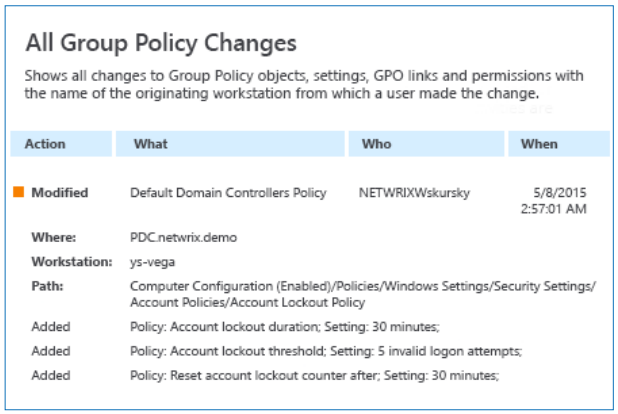


Concentratevi sul Fattore Davvero Importante

Utilizzate gli avvisi per essere informati sulle modifiche alla configurazione di sistema critiche e in tempo reale. Scegliete specifici tipi di modifiche sui quali desiderete essere avvisati, per esempio – impostate gli avvisi sulle modifiche ai membri del gruppo “Enterprise Admins” o “Domain Admins”.

Identificate Causa e Risoluzione di Problema più Veloce

Utilizzate i dati significativi e accurati per indagare sulle sequenze di eventi e determinare le loro cause. Avere un unico punto di accesso all’audit trail assicura una risposta rapida ai problemi derivanti.



10
Affrontate le Sfide del Vostro Dipartimento e Business

IT Administrator

Generate e fornite i report su compliance più velocemente.

Indagate l'attività sospetta degli utenti prima che diventi una violazione.

IT Security Administrator

IT Manager

Riprendete il controllo di ciò che sta accadendo nella vostra infrastruttura IT ed eliminate lo stress del prossimo audit di conformità.

Mitigate i rischi di sicurezza e minimizzate i costi della compliance.

CIO/CISO

MSP

Assicurate trasparenza negli ambienti gestiti e monetizzate l'offerta 'Compliance as a Service'.

> *Con Netwrix Auditor abbiamo ottenuto una soluzione molto facile da usare che mostra i dati dettagliati su chi / cosa / quando / dove per tutte le modifiche risparmiandoci le ore di lavoro investigativo.*
>
> *Jeff Salisbury, Direttore, Global IT Operations, Belkin International Inc.*

> *Netwrix Auditor garantisce la nostra sicurezza. Utilizzando le soluzioni Netwrix per l'audit delle modifiche apportate attraverso i sistemi IT siamo in grado di ottenere i numerosi report che ci aiutano a trovare rapidamente se ci fossero tentativi di accesso non autorizzato ai dati sensibili, soprattutto in caso di dipendenti che non sono autorizzati. È il modo migliore per garantire la sicurezza e la protezione dei dati.*
>
> *Richard Staats, Membro di IT Team, VTM Group*

11
Caratteristiche

Audit delle Modifiche, Configurazioni e Accessi

Audit delle modifiche: rilevazione, report e avvisi su tutte le modifiche di configurazione dando completa visibilità su Chi ha fatto Cosa, Quando e Dove, attraverso l'intera infrastruttura IT con cronologia completa su "prima e dopo" ogni modifica effettuata.

Valutazione della configurazione: i rapporti State-in-Time™ mostrano i parametri di configurazione in qualsiasi momento, quali per esempio le impostazioni di appartenenza ad un determinato gruppo o le password policy, come erano stati configurati un anno prima.

Access Auditing (Audit degli Accessi): reporting e monitoraggio dell'accesso riuscito o fallito ai sistemi e ai dati.

Monitoraggio dell'attività degli utenti privilegiati in ogni sistema IT anche se non producono alcun log tramite la registrazione video di attività con capacità di cercare e riprodurre.

La Piattaforma Unificata

Piattaforma unificata per la revisione dell'intera infrastruttura IT, a differenza di altri fornitori che propongono diversi programmi difficili da integrare.

AuditAssurance™: consolida i dati di audit da più fonti indipendenti. Se i dettagli chiave mancano da una fonte, la tecnologia integra i dati raccolti con i dettagli provenienti da un'altra fonte che assicura dati accurati e senza errori.

AuditIntelligence™: trasforma i dati di audit complessi in cambiamenti significativi e accurati.

AuditArchive™: tiene audit trail archiviato per oltre 10 anni per la successiva revisione e per I controlli periodici degli auditor garantendo un rapido accesso ai dati di audit per tutto il periodo di detenzione.

Accesso delegato ai dati di audit : il client di Netwrix Auditor può essere installato su un numero illimitato di desktop e laptop, abilitando la collaborazione globale e fornendo il pieno accesso all'«actionable intelligence» .

Sono supportate le modalità di funzionamento **agentless o con agenti lightweight** non intrusive**.**

12
Caratteristiche

Ricerca dei dati, Report Predefiniti, Avvisi e Dashboard

Ricerca Interattiva: Smistate rapidamente i dati di audit, ottimizzate i criteri di ricerca e ottenete tutte le informazioni di cui avete bisogno. Esportate i risultati o create un report personalizzato che risponde alle vostre specifiche esigenze.

Più di 150 report predefiniti sono inclusi con filtraggio, raggruppamento, ordinamento, l'esportazione (PDF, XLS, ecc), drill-down, l'accesso al Web, permessi granulari e altro.

Report su compliance «out-of-the-box» rispondono alle esigenze specifiche delle normative di compliance, tra cui PCI DSS 3.0, HIPAA, SOX, FISMA/NIST800-53 e ISO/IEC 27001.

Avvisi in tempo reale e report sulle modifiche di configurazione critiche e sui tentativi di accesso ai dati sensibili, sia su quelli andati a buon fine che su quelli falliti.

Enterprise Overview Dashboard forniscono visibilità completa su tutto quello che sta accadendo nella vostra infrastruttura IT e forniscono i dati dettagliati su ogni modifica effettuata attraverso tutti i sistemi sottoposti ad audit. Scoprite come spesso vengono apportate le modifiche, quali utenti stanno facendo azioni sospette, quali sistemi sono influenzati e altro.

SIEM, Rollback, FIM

Integrazione con SIEM: possibilità di inviare i dati di audit significativi nel vostro sistema SIEM, sfruttando i processi esistenti, proteggendo gli investimenti tecnologici e riducendo il lavoro di gestione.

Event Log Management: registrazione e raccolta di Windows logs e Syslog come logon/logoff, account lockouts, ecc.

Funzionalità di rollback: Ripristina modifiche non autorizzate o dannose allo stato precedente senza alcun tempo d'inattività di sistema e senza dover ripristinare dal backup.

Monitoraggio dell'integrità dei file (MIF) attraverso il monitoraggio e la tracciatura di cambiamenti ai sistemi critici, ai file, ai folder e alle configurazioni come richiesto dalle normative di conformità.