netwrix

Netwrix Auditor

Controlla i tuoi dati. Proteggi ciò che conta.

Panoramica del Prodotto

Piattaforma Netwrix Auditor

Netwrix Auditor è una **piattaforma agentless per la sicurezza dei dati** che consente alle società di identificare con precisione le informazioni sensibili, regolamentate e mission-critical e di applicare controlli di accesso coerenti, indipendentemente da dove sono archiviate le informazioni. Consente loro di **ridurre al minimo il rischio di violazione dei dati e garantire la conformità normativa** riducendo proattivamente l'esposizione di dati sensibili e rilevando tempestivamente violazioni delle policy e comportamenti sospetti degli utenti.

Identificare

Comprendi quali dati necessitano di protezione e quanto sono esposti.

Proteggere

Riduci al minimo il rischio di una violazione dei dati.

Rilevare

Rileva tempestivamente le minacce alla sicurezza dei dati.

Rispondere

Prendi decisioni di risposta agli incidenti più rapide e mirate.

Recuperare

Facilita il recupero dei dati chiave e impara dagli incidenti del passato.

Rispettare

Raggiungi e dimostra la conformità alle normative.

Vantaggi

01 | Comprendere quali dati necessitano di protezione e quanto sono esposti

Identifica e classifica i dati sensibili, sia strutturati che non strutturati, e i rischi relativi ai dati e all'infrastruttura che potrebbero metterne in pericolo la sicurezza.

02 | Ridurre al minimo il rischio di una violazione dei dati

Scopri chi ha accesso a cosa e poni rimedio alla sovraesposizione di dati sensibili, regolamentati e mission-critical in maniera proattiva.

03 | Rilevare tempestivamente le minacce alla sicurezza dei dati

Individua comportamenti anomali dell'utente e violazioni delle norme che minacciano la sicurezza dei dati.

04 | Prendere decisioni di risposta agli incidenti più rapide e mirate

Riduci il tempo medio necessario per rispondere alle minacce alla sicurezza dei dati e contenere gli incidenti.

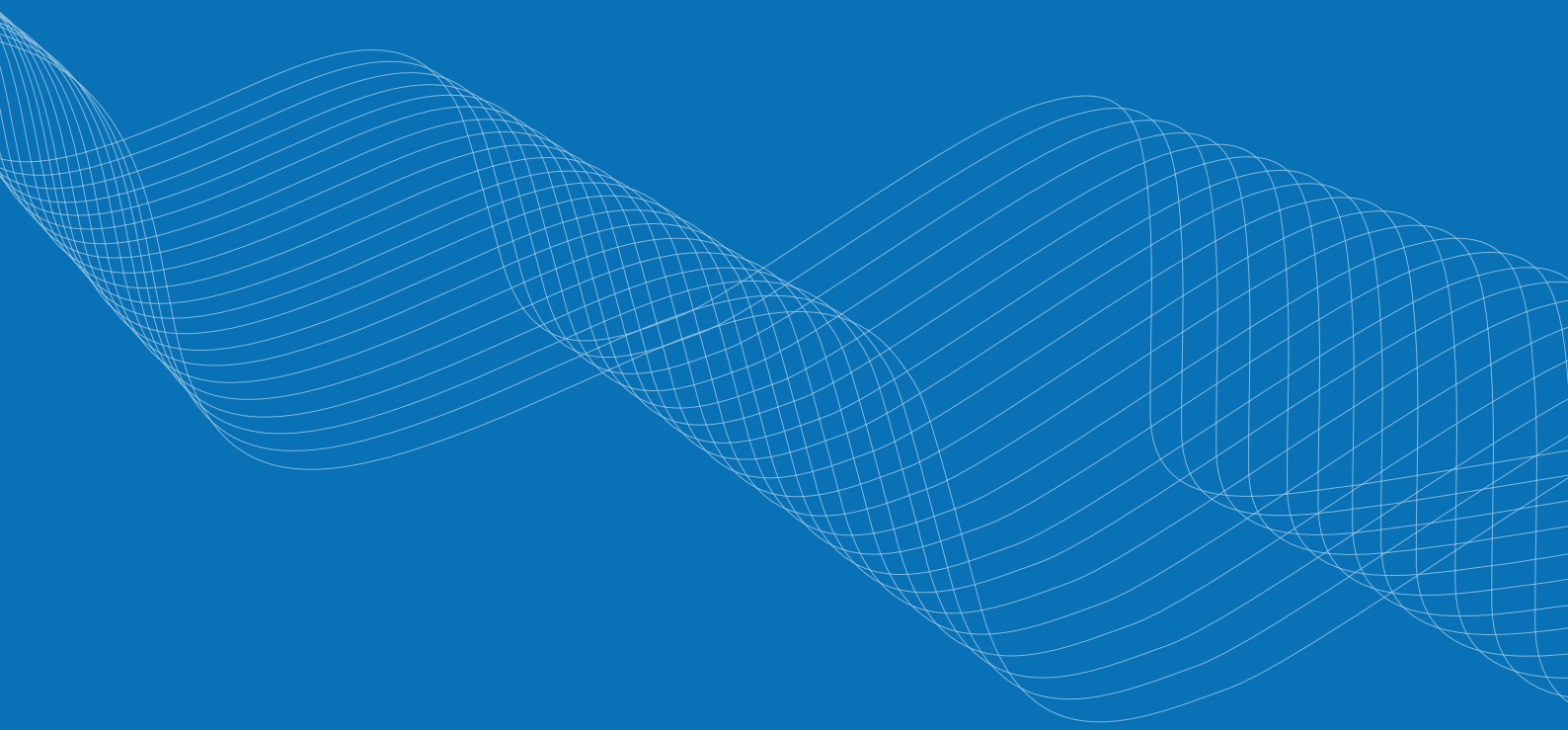
05 | Facilitare il recupero dei dati chiave e imparare dagli incidenti del passato

Esamina i dettagli completi su come si è verificato un incidente di sicurezza e quali dati ne hanno risentito.

06 | Raggiungere e dimostra la conformità alle normative

Valuta in modo proattivo l'efficacia dei controlli in materia di sicurezza dei dati e dimostra la propria conformità agli auditor con prove concrete.

01 | Comprendere quali dati necessitano di protezione e quanto sono esposti



Dai priorità alla sicurezza dei dati sensibili attraverso più silos di dati

Classifica e tagga sia i dati non strutturati che quelli strutturati indipendentemente dalla loro posizione, in modo da dare la priorità alla sicurezza delle informazioni sensibili. Applica policy di sicurezza coerenti tra repository multipli di dati.

Sensitive Files Count by Source

Shows the number of files that contain specific categories of sensitive data. Clicking the "Categories" or "Source" link narrows your results down to a certain file in this report. Use this report to estimate amount of your sensitive data in each category, plan for data protection measures and control their implementation.

Content source	Categories	Files count
\\fs1\Accounting	GDPR	1300
	PCI DSS	585
\\fs1\Finance	GDPR	715
	HIPAA	1085
	PCI DSS	952
\\fs1\HR	GDPR	1500
	HIPAA	250
\\fs1\Public	PCI DSS	15

Overexposed Files and Folders

Shows sensitive files and folders accessible by the specified users or groups, based on the combination of folder and share permissions. Clicking the "Object path" link opens the "Sensitive File and Folder Permission Details" report. Use this report to identify data at high risk and plan for corrective actions accordingly.

Group Name: Everyone

Object path	Categories
\\fs1\Accounting\Contractors	GDPR
	PCI DSS
	PII
\\fs1\Accounting\Payroll	GDPR
	PCI DSS
\\fs1\Accounting\Invoices	GDPR
	PCI DSS

Identifica i dati sensibili sovraesposti

Scopri quali sono i dati sensibili più a rischio, per dare la priorità alla risoluzione di tali rischi. Scopri quali sono le informazioni sensibili esposte a un numero elevato di utenti senza necessità aziendali o archiviate in una posizione non protetta.

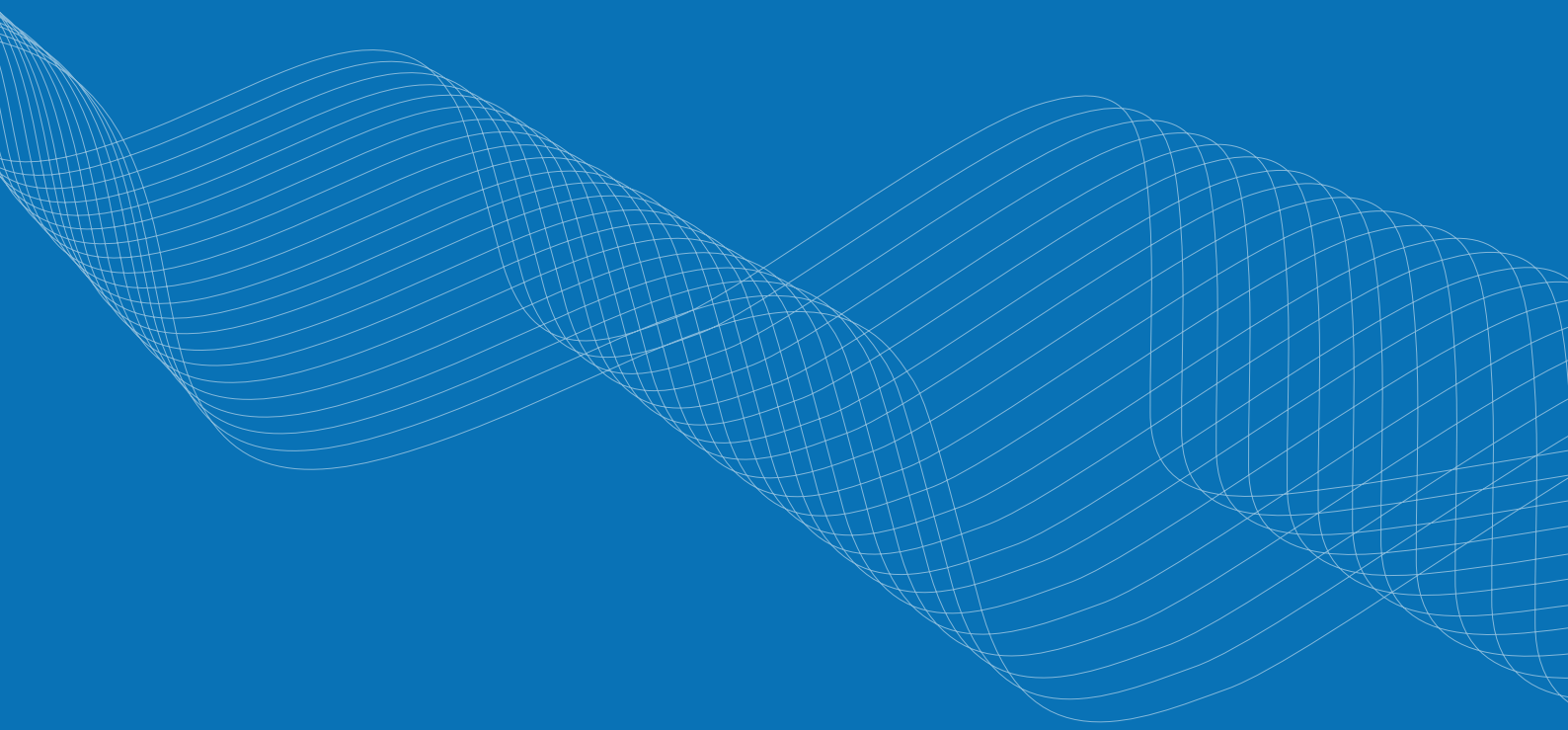
Valuta i rischi di sicurezza dei dati e dell'infrastruttura

Identifica sia i dati che le lacune di sicurezza dell'infrastruttura, quali un numero elevato di autorizzazioni assegnate in maniera diretta o troppi account utente inattivi. Valuta continuamente questi parametri di sicurezza e concentrati su quelli più importanti.

Risk Assessment – Overview

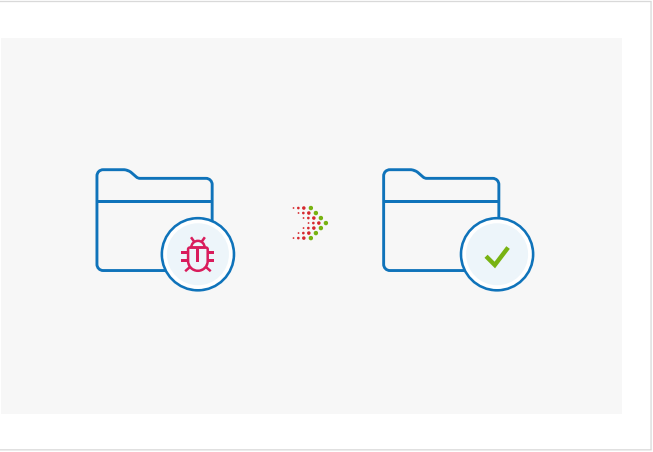
Risk name	Current value	Risk level
Users and Computers		
User accounts with Password never expires	2	Medium (1-4)
User accounts with Password not required	0	Low (0)
Disabled computer accounts	0% (0 of 20)	Low (0)
Inactive user accounts	10% (3 of 30)	High (1% - 100%)
Inactive computer accounts	20% (4 of 20)	High (3% - 100%)
Permissions		
User accounts with administrative permissions	20% (6 of 30)	High (3% - 100%)
Administrative groups	12% (6 of 50)	High (3% - 100%)
Empty security groups	6% (3 of 50)	High (2% - 100%)
Data		
Shared folders accessible by Everyone	14% (2145 of 15321)	High (5% - 100%)
File names containing sensitive data	2	High (2 - unlimited)

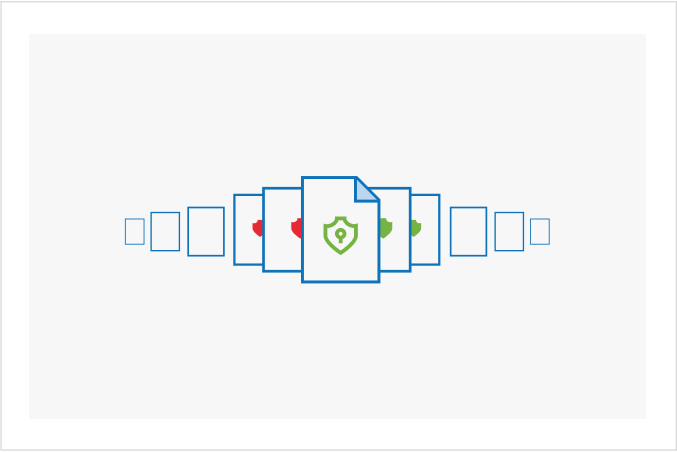
02| Ridurre al minimo il rischio di una violazione dei dati



Metti automaticamente in quarantena i dati sensibili per ridurre il rischio di una violazione o di una perdita

Se un documento sensibile si apre in una posizione in-aspettata, viene spostato automaticamente in un'area di quarantena fino a quando non verrà stabilito dove deve essere archiviato e chi deve accedervi.





Blocca immediatamente i dati sensibili sovraesposti

Se i controlli di accesso relativi ai dati sensibili non sono appropriati al rischio, rimuovi automaticamente tutti i diritti alla lettura o modifica di queste informazioni dai gruppi di accesso globali, quali Everyone.

Semplifica le regolari attestazioni di privilegio

Scopri chi ha accesso a quali dati sensibili e in che modo ha ottenuto quell'accesso, abilita i proprietari dei dati a verificare regolarmente che tali diritti siano in linea con le esigenze aziendali. In caso contrario, rimuovi le autorizzazioni in eccesso per applicare il principio del minimo privilegio e mantenere il rischio a un livello accettabile.

Sensitive File and Folder Permissions Details

Shows permissions granted on files and folders that contain certain categories of sensitive data. Use this report to see who has access to a particular file or folder, vie either group membershir or direct assignment. Reveal sensitive content that has permissions different from the parent folder.

Object: \\fs1\Accounting (Permissions: Different from parent)

Categories: GDPR, PCI DSS

Account	Permissions	Means Granted
ENTERPRISE\J.Carter	Full Control	Group
ENTERPRISE\T.Simpson	Full Control	Directly
ENTERPRISE\A.Brown	Full Control	Group

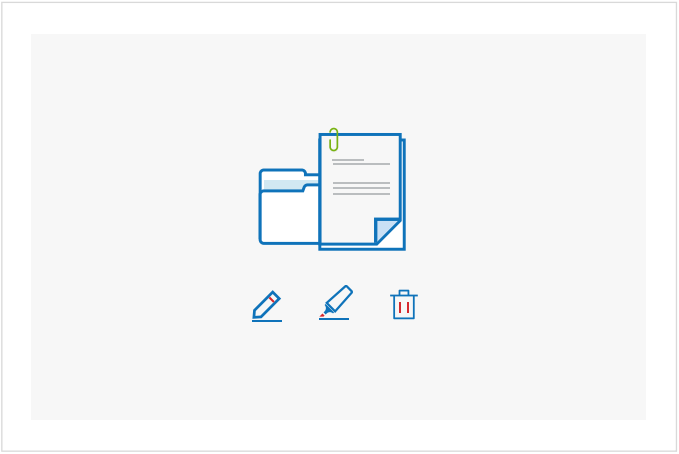
Object: \\fs1\Accounting\Europe (Permissions: Different from parent)

Categories: GDPR

Account	Permissions	Means Granted
ENTERPRISE\M.Smith	Full Control	Group
ENTERPRISE\A.Gold	Full Control	Group

Aumenta la precisione della tua soluzione DLP

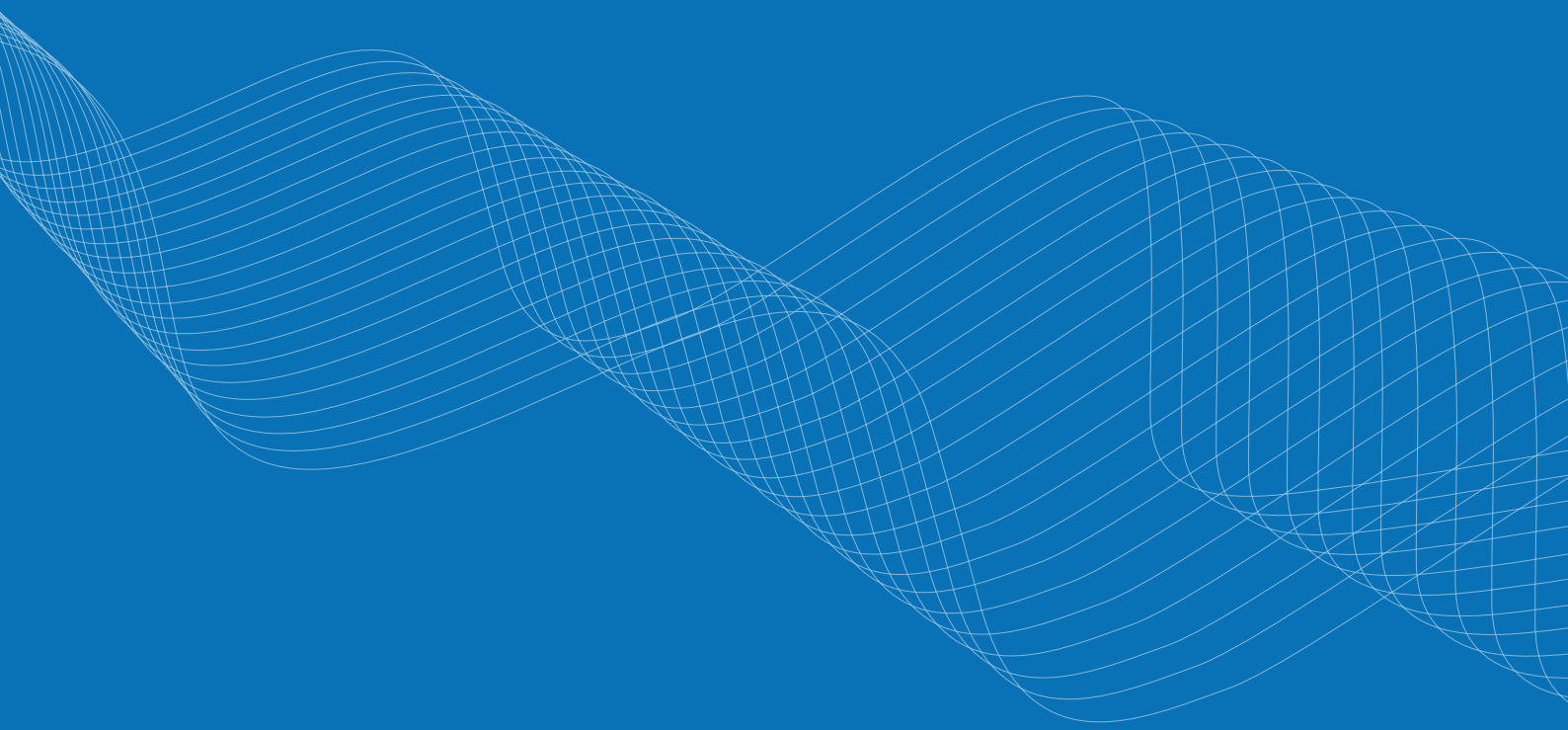
Gli oggetti non sensibili taggati per errore non richiedono protezione. Ottimizza i tuoi sforzi per garantire la sicurezza dei dati aumentando la precisione del tuo strumento di prevenzione della perdita di dati (DLP) usando i tag di classificazione ad alta precisione scritti da Netwrix Auditor.



Oscura le informazioni sensibili in base alla politica aziendale

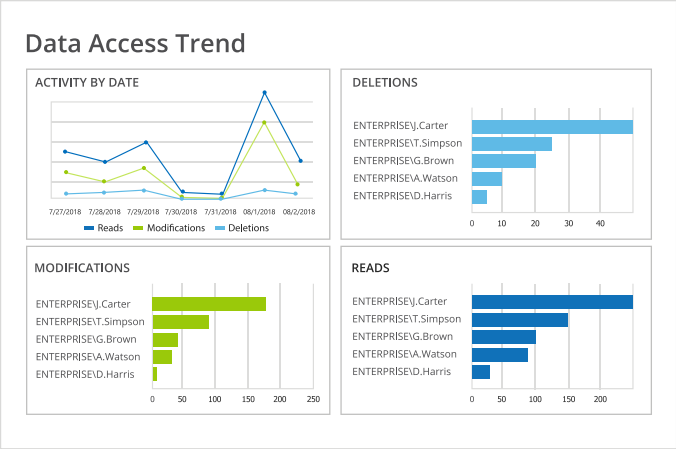
Riduci il rischio di esposizione di informazioni riservate mediante l'oscurazione automatica del contenuto sensibile dai documenti se non vi è alcuna esigenza aziendale per cui debbano essere lì. Mantieni la produttività conservando intatto il resto del documento.

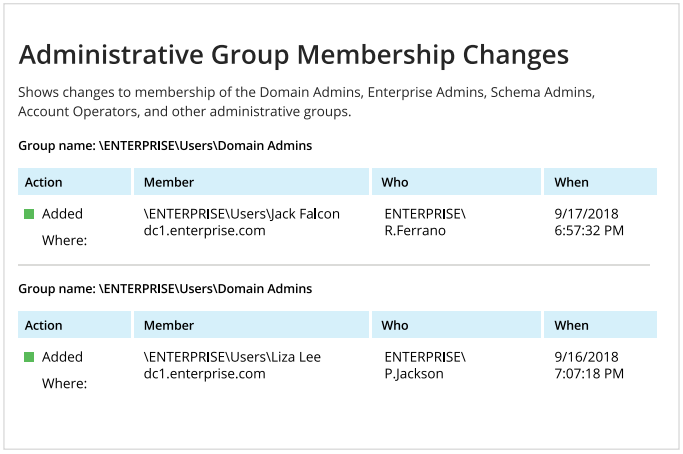
03 | Rilevare tempestivamente le minacce alla sicurezza dei dati



Stabilisci una rigida responsabilità sull'uso degli account privilegiati

Monitora continuamente l'attività degli utenti privilegiati in tutti i sistemi per garantire che seguano le politiche interne e non abusino dei loro privilegi per accedere, modificare o eliminare dati sensibili senza essere colti in flagrante.





Administrative Group Membership Changes

Shows changes to membership of the Domain Admins, Enterprise Admins, Schema Admins, Account Operators, and other administrative groups.

Group name: \ENTERPRISE\Users\Domain Admins

Action	Member	Who	When
Added Where:	\ENTERPRISE\Users\Jack Falcon dc1.enterprise.com	ENTERPRISE\ R.Ferrano	9/17/2018 6:57:32 PM

Group name: \ENTERPRISE\Users\Domain Admins

Action	Member	Who	When
Added Where:	\ENTERPRISE\Users\Liza Lee dc1.enterprise.com	ENTERPRISE\ P.Jackson	9/16/2018 7:07:18 PM

Controlla l'escalation dei privilegi

Rileva eventuali modifiche ai diritti di accesso o all'appartenenza al gruppo, in modo da poter valutare se le eventuali autorizzazioni ai dati sensibili sono state modificate senza un motivo legittimo. Ripristina rapidamente eventuali modifiche improprie per ridurre i rischi.

Individua gli attacchi ransomware in corso

Ricevi avvisi sui segnali di possibili attività ransomware, ad esempio la presenza di un gran numero di modifiche ai file in un periodo di tempo molto breve. Isola rapidamente l'account utente responsabile per impedire al ransomware di crittografare tutti i file a cui l'account ha accesso attraverso la rete.

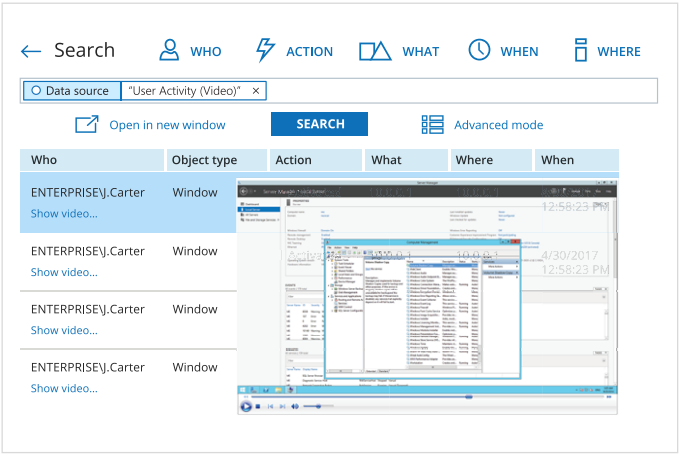
Netwrix Auditor Alert

Possible ransomware activity

The alert was triggered by 150 activity records being captured within 60 seconds. The most recent of those activity records is shown below. To review the full activity trail, use the interactive search in Netwrix Auditor.

Who:	ENTERPRISE\J.Carter
Action:	Modified
Object type:	File
What:	\\fs3.enterprise.com\Documents\Contractors\payroll2017.docx
When:	4/28/2018 11:35:17 AM
Where:	fs3.enterprise.com
Workstation:	mkt025.enterprise.com
Data source:	File Servers
Monitoring plan:	Enterprise Data Visibility Plan
Details:	Size changed from "807936 bytes" to "831488 bytes"

This message was sent by Netwrix Auditor from **au-srv-fin.enterprise.com.**

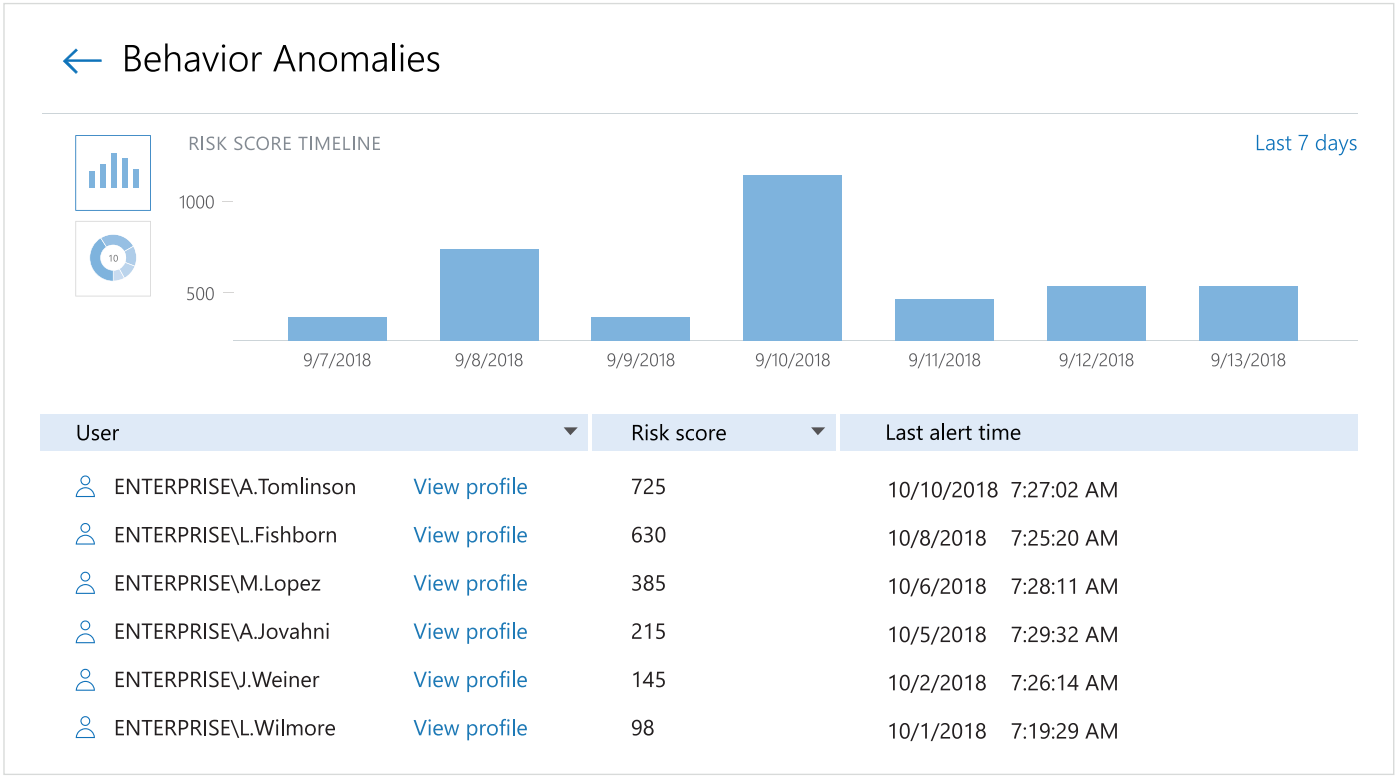


Tieni sotto stretta sorveglianza l'attività di terzi

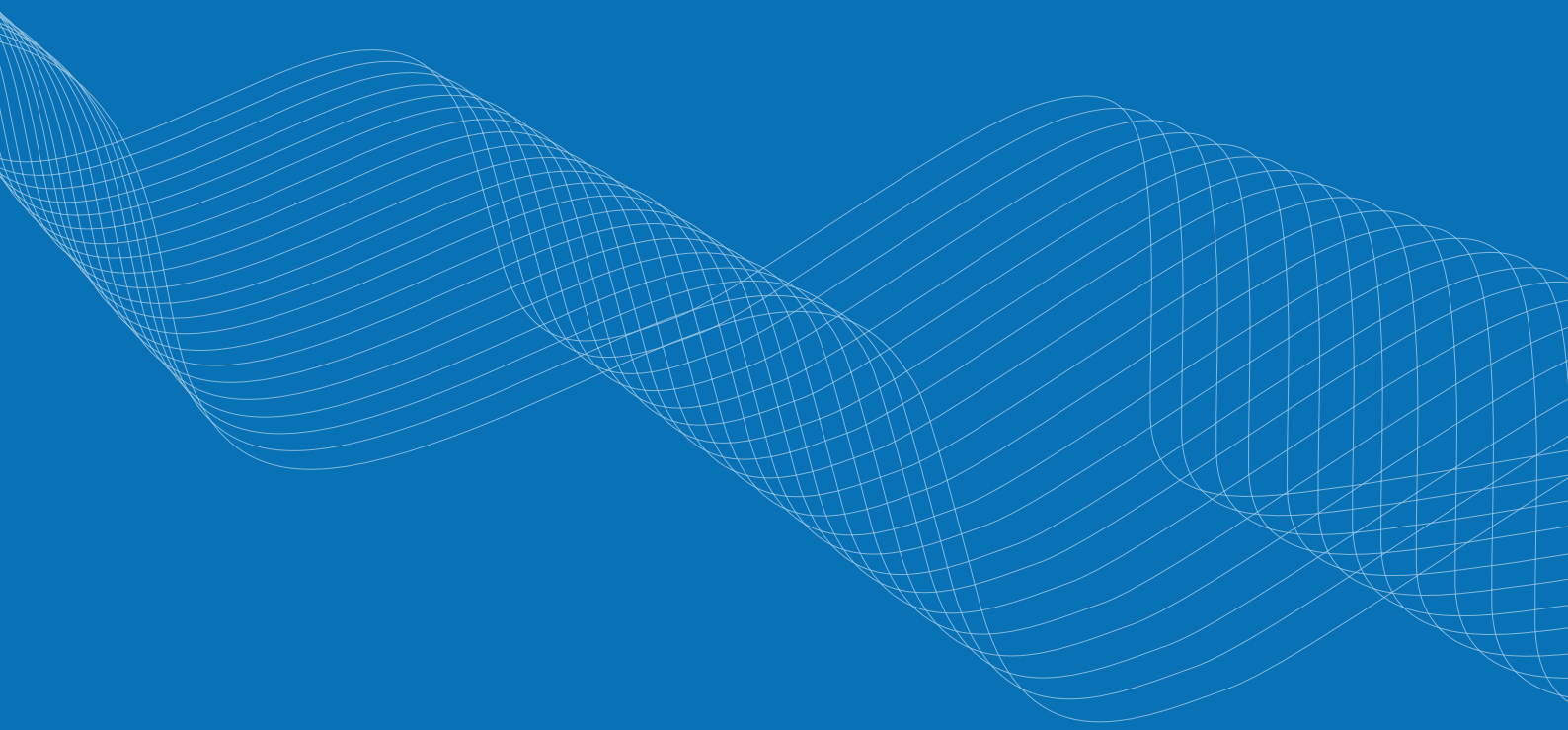
Monitora attentamente l'attività degli account utente di terzi in qualsiasi sistema o applicazione, anche se non genera alcun registro, per garantire la piena responsabilità. Ricevi una notifica ogni volta che un fornitore compie qualcosa che non rientra nel proprio ambito di attività, poiché le azioni non autorizzate potrebbero mettere a rischio i tuoi dati.

Rileva account compromessi e addetti ai lavori malintenzionati

Rileva prontamente anche i segnali impercettibili di probabili minacce alla sicurezza dei dati in corso, quali accessi insoliti o utenti che accedono a dati sensibili ai quali prima non avevano accesso. Identifica e analizza facilmente gli utenti che presentano il maggior rischio con una vista aggregata dell'attività anomala di ciascun individuo.

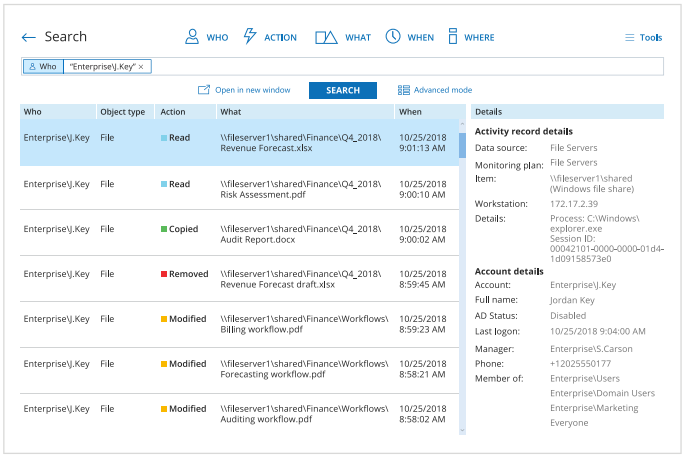


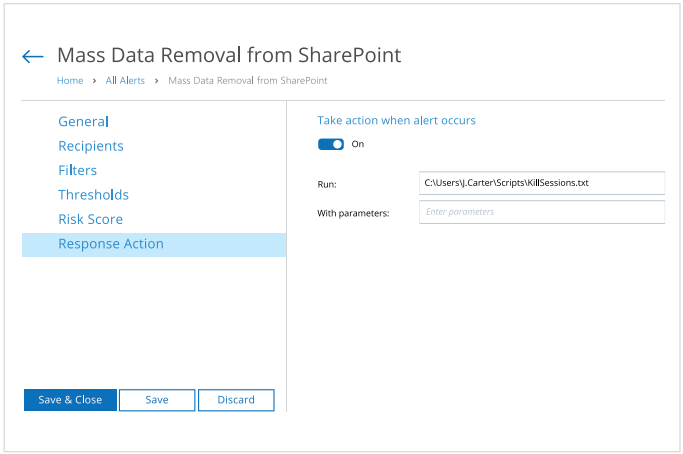
04| Prendere decisioni di risposta agli incidenti più rapide e mirate



Snellisci le indagini sugli incidenti

Risolvi rapidamente gli incidenti che riguardano i dati sensibili: potrai comprendere esattamente cosa è successo, com'è successo, chi c'è dietro e quali informazioni sono state coinvolte. Utilizza queste informazioni per formulare la migliore risposta possibile all'incidente.





Riduci il tempo medio per rispondere

Reagisci più velocemente alle minacce alla sicurezza dei dati automatizzando la risposta agli incidenti prevedibili. Fornisci un supporto iniziale per gli incidenti e consenti lo svolgimento di indagini più rapide e accurate, integrando Netwrix Auditor nel processo SecOps.

Determina e segnala la gravità di una perdita di dati

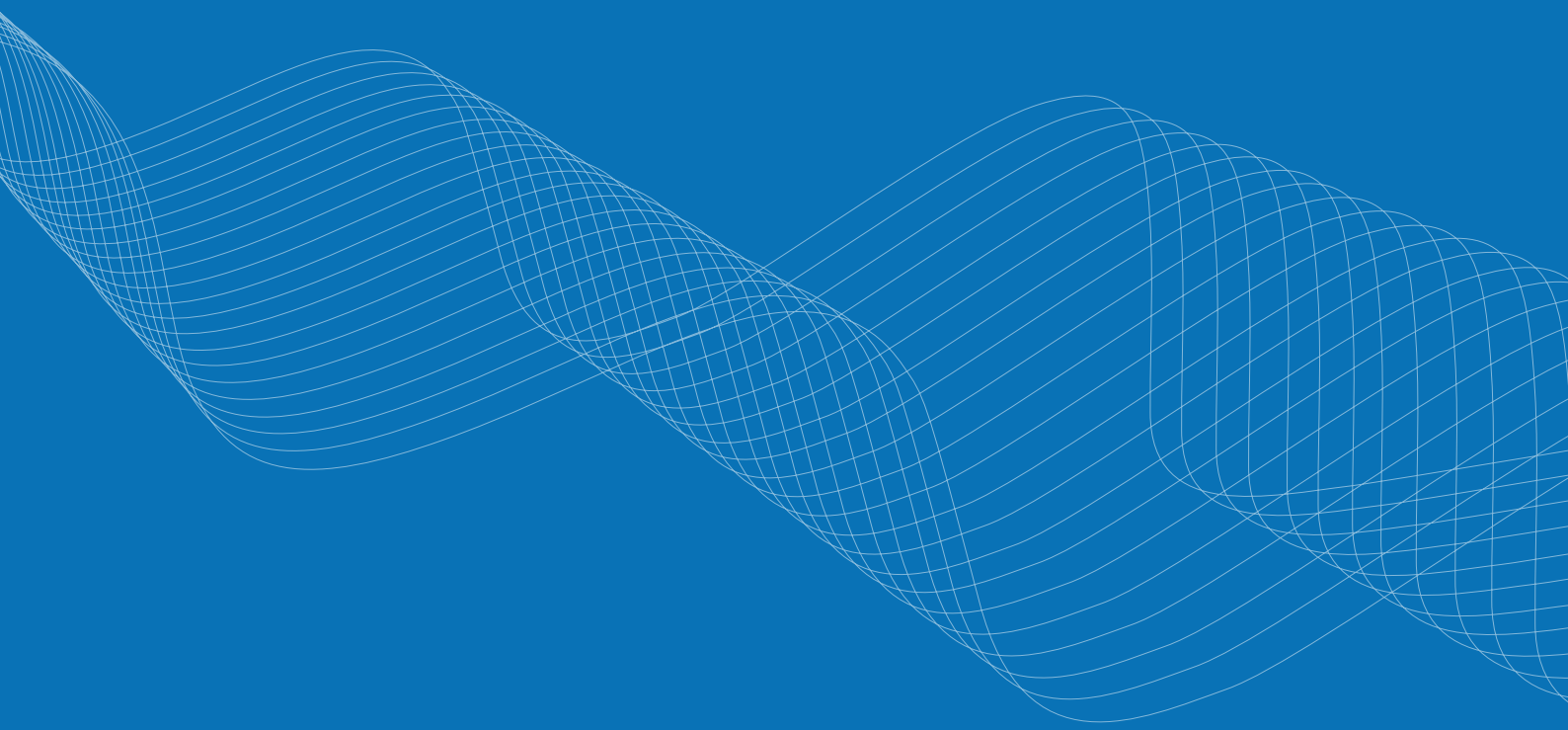
Analizza la quantità di dati a cui un utente malevolo o un account compromesso ha avuto accesso e quali dati sono stati effettivamente visualizzati, modificati o eliminati. Utilizza queste informazioni per stabilire se è necessario segnalare l'incidente e, se dovuto, informare tutte le parti interessate e adottare ulteriori misure appropriate.

Activity Related to Sensitive Files and Folders

Shows all access attempts (failed and successful changes, and successful and failed read attempts) to files and folders that contain certain categories of sensitive data.

Action	Object type	What	Who	When
Read (Failed Attempt) Where: Workstation: Categories:	Folder fs1 192.168.77.25 PCI DSS	\\fs1\Accounting\Payroll	ENTERPRISE\ M.Smith	3/12/2018 9:25:49 AM
Read Where: Workstation: Categories:	Folder fs1 192.168.77.25 PCI DSS	\\fs1\Accounting\Payroll	ENTERPRISE\ M.Smith	3/12/2018 9:25:55 AM

05 | Facilitare il recupero dei dati chiave e imparare dagli incidenti del passato



Comprendi l'importanza e la sensibilità dei dati per pianificare i processi di recupero delle informazioni

Cataloga i tuoi dati e scopri dove si trovano quelli più sensibili o business-critical. Crea piani di recupero delle informazioni che rendano prioritario il ripristino di queste informazioni.

Sensitive Files Count by Source

Shows the number of files that contain specific categories of sensitive data. Clicking the "Categories" or "Source" link narrows your results down to a certain file in this report. Use this report to estimate amount of your sensitive data in each category, plan for data protection measures and control their implementation.

Content source	Categories	Files count
\\fs1\Accounting	GDPR	1300
	PCI DSS	585
\\fs1\Finance	GDPR	715
	HIPAA	1085
	PCI DSS	952
\\fs1\HR	GDPR	1500
	HIPAA	250
\\fs1\Public	PCI DSS	15

Activity Related to Sensitive Files and Folders

Shows all access attempts (failed and successful changes, and successful and failed read attempts) to files and folders that contain certain categories of sensitive data.

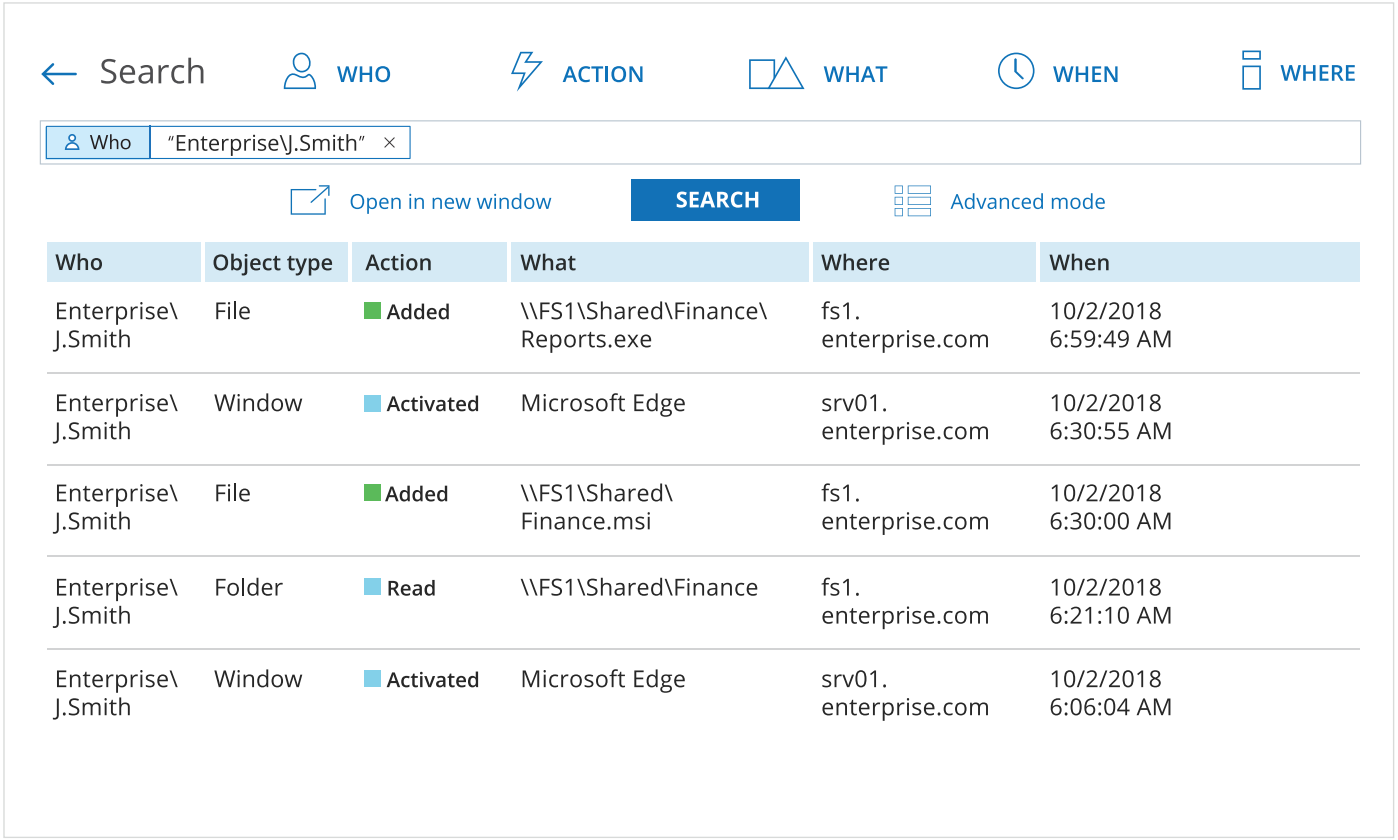
Action	Object type	What	Who	When
Removed	File	\\fs1\Finance\Revenue2018.xlsx	ENTERPRISE\ T.Simpson	12/22/2018 4:30:33 PM
Where: fs1 Workstation: 192.169.55.34 Categories: PCI DSS Date created: "1/24/2018 10:11:42 AM"				
Removed	File	\\fs1\Finance\Revenue2017.xlsx	ENTERPRISE\ T.Simpson	12/22/2018 4:35:47 PM
Where: fs1 Workstation: 192.169.55.34 Categories: PCI DSS Date created: "1/23/2017 11:34:54 AM"				

Ripristina più velocemente i dati dando la priorità al recupero dei dati chiave

Stabilisci quali dati (sensibili, confidenziali o mission-critical) sono stati danneggiati durante l'attacco e quali sono le priorità per recuperarli. Scopri chi ha avuto accesso a questi documenti per rendere produttivi i tuoi utenti aziendali il prima possibile.

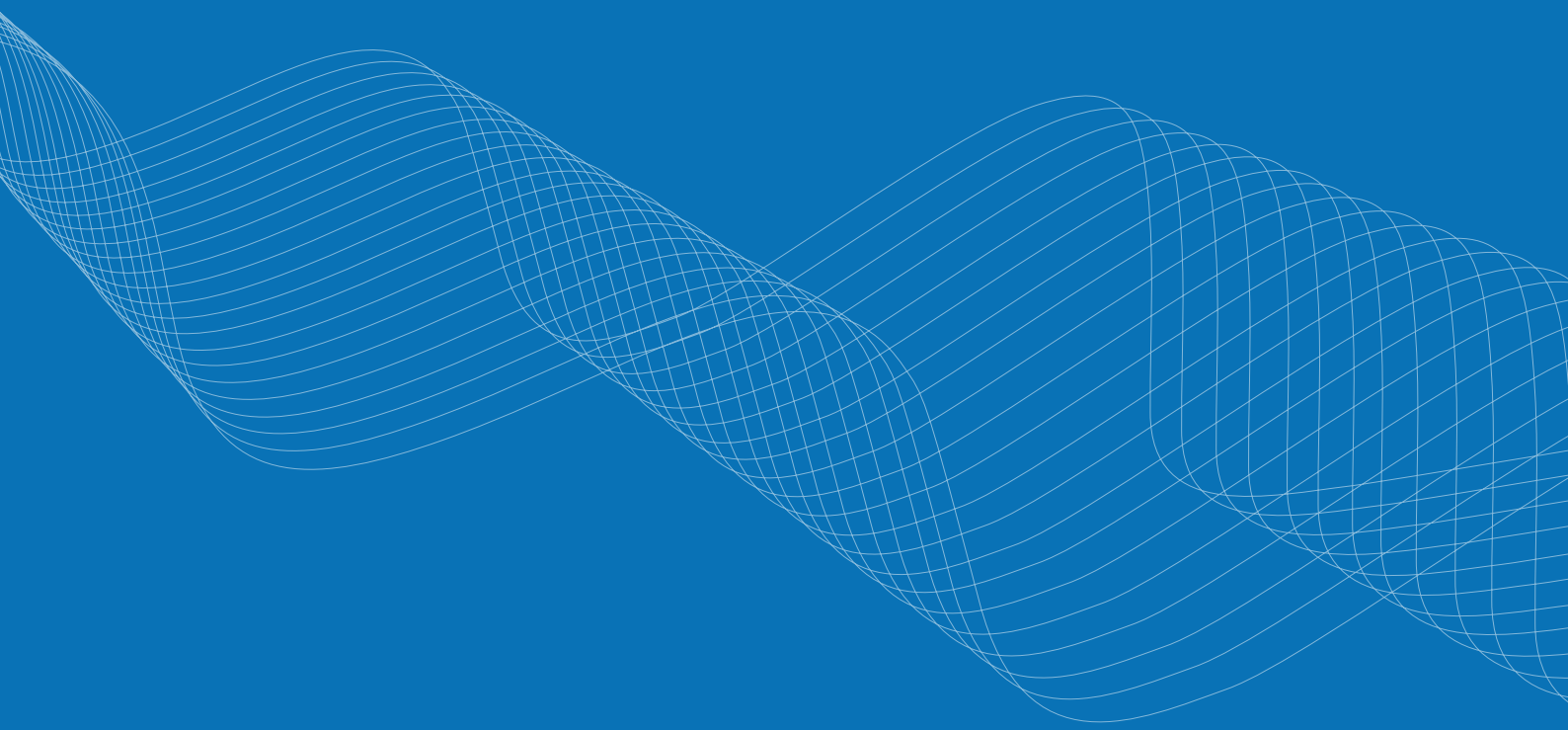
Includi le lezioni apprese nella strategia di sicurezza dei dati

Analizza come si è verificato esattamente un incidente di sicurezza e utilizza queste informazioni per migliorare la strategia di sicurezza dei dati e prevenire incidenti simili in futuro.



Who	Object type	Action	What	Where	When
Enterprise\ J.Smith	File	Added	\\FS1\Shared\Finance\ Reports.exe	fs1. enterprise.com	10/2/2018 6:59:49 AM
Enterprise\ J.Smith	Window	Activated	Microsoft Edge	srv01. enterprise.com	10/2/2018 6:30:55 AM
Enterprise\ J.Smith	File	Added	\\FS1\Shared\ Finance.msi	fs1. enterprise.com	10/2/2018 6:30:00 AM
Enterprise\ J.Smith	Folder	Read	\\FS1\Shared\Finance	fs1. enterprise.com	10/2/2018 6:21:10 AM
Enterprise\ J.Smith	Window	Activated	Microsoft Edge	srv01. enterprise.com	10/2/2018 6:06:04 AM

06 | Raggiungere e dimostrare la conformità alle normative



Valuta l'efficacia dei controlli di sicurezza dei dati

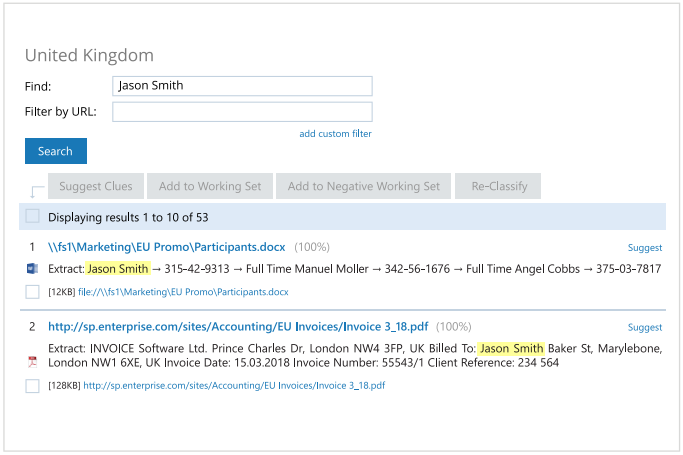
Implementa i controlli di conformità nell'intera infrastruttura e verifica regolarmente se funzionano come previsto. Se le politiche scritte in materia di sicurezza differiscono da quelle effettivamente esistenti, correggi i controlli di sicurezza dei dati difettosi prima che gli auditor li rilevino.

Account Permissions

Shows accounts with permissions granted on files and folders (either directly or via group membership). Use this report to see who has access to files and folders and ensure these settings comply with your policies.

Group name: Everyone

Object Path	Permissions	Means Granted
\\pdc\shared\Accounting	Read (Execute, List folder content)	Directly
\\pdc\shared\Customer Data	Full Control	Directly
\\pdc\shared\Orders	Read (Execute, List folder content)	Directly
\\pdc\shared\Finance	Read (Execute, List folder content)	Directly
\\pdc\shared\Internal	Full Control	Directly
\\pdc\shared\Sales	Full Control	Directly

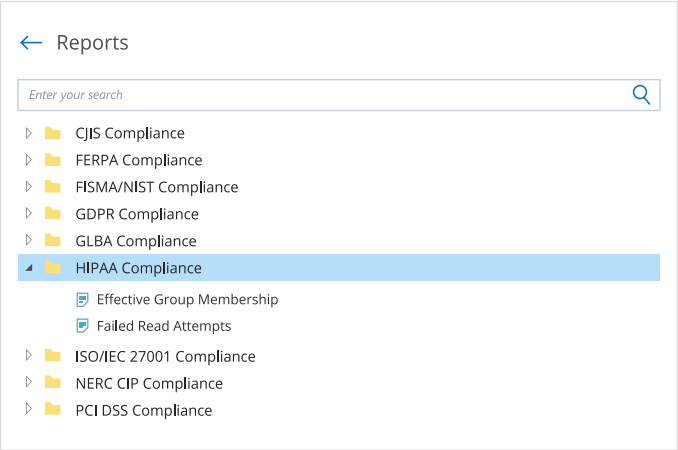


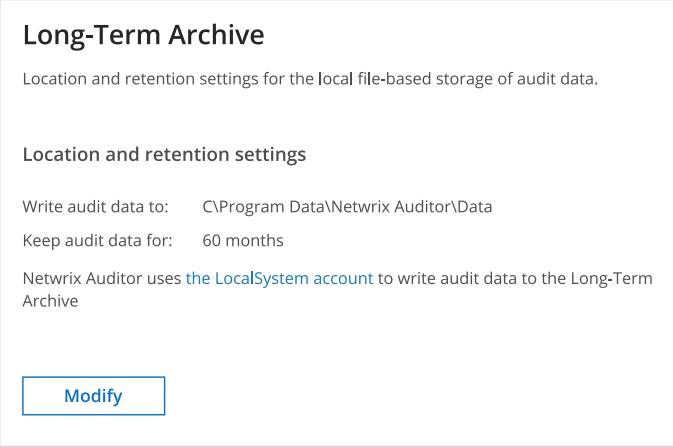
Rispetta le richieste di accesso

Trova facilmente tutti i dati memorizzati su un particolare soggetto interessato quando esercita i diritti alla privacy secondo GDPR, CCPA e altre normative moderne. Forniscigli un elenco di queste informazioni o gli cancelli completamente qualora dovesse ritirare il consenso.

Riduci il tempo impiegato per la preparazione e gli audit di conformità

Preparati alla maggior parte delle richieste degli auditor avvalendoti di report pronti all'uso in linea con i controlli di conformità di HIPAA / HITECH, PCI DSS, GDPR e altre normative comuni. Se durante l'audit ci sono domande inattese, utilizza la ricerca interattiva per ottenere rapidamente le informazioni richieste.





Archivia e accedi al tuo audit trail per anni

Conserva in archivio il tuo audit trail in un formato compresso per oltre 10 anni, come richiesto da molte normative, assicurando al contempo che tutti i dati di audit possano essere facilmente accessibili dagli utenti autorizzati in qualsiasi momento.

Applicazioni

Applicazioni Netwrix Auditor

La piattaforma Netwrix Auditor include una vasta gamma di applicazioni che forniscono un unico pannello di controllo per monitorare ciò che accade sia ai **sistemi di archiviazione di dati** che ai **sistemi backbone IT**. Questa visibilità consente alle società di capire dove si trovano i dati sensibili, quali sono i rischi che li riguardano e quale attività rappresenta un pericolo per la loro sicurezza.

Dati strutturati

- Netwrix Auditor for SQL Server
- Netwrix Auditor for Oracle Database

Dati non strutturati

- Netwrix Auditor for Windows File Servers
- Netwrix Auditor for SharePoint
- Netwrix Auditor for EMC
- Netwrix Auditor for NetApp
- Netwrix Auditor for Exchange

Infrastruttura

- Netwrix Auditor for Active Directory
- Netwrix Auditor for Network Devices
- Netwrix Auditor for Windows Server
- Netwrix Auditor for VMware

Cloud

- Netwrix Auditor for Office 365
- Netwrix Auditor for Azure AD

Opzioni di installazione

On-premises, virtuale o cloud: installa Netwrix Auditor ovunque sia necessario.

Virtuale

Disponibile in appliance per **VMware vSphere e Microsoft Hyper-V**

In locale

Completamente supportato su **Microsoft Windows Server**

Cloud

Completamente supportato in **Microsoft Azure e AWS**

Microsoft Hyper-V

vmware READY

Windows Server

Microsoft Azure

awsmarketplace

API RESTful: infinite capacità di integrazione per una maggiore sicurezza dei dati e reporting semplificato

Centralizza l'auditing e il reporting

Netwrix Auditor raccoglie gli activity trail di qualsiasi applicazione, locale o cloud, e le memorizza in un archivio centrale sicuro, predisposto per le revisioni storiche e le richieste di conformità.

Ottieni il massimo dal tuo investimento per i SIEM

Netwrix Auditor aumenta il rapporto segnale-rumore e massimizza il valore SIEM alimentando un audit dettagliato dei dati nelle soluzioni HP Arcsight, Splunk, IBM QRadar (o altre soluzioni SIEM).

Automatizza Flussi di lavoro IT

Netwrix Auditor si integra con altri strumenti di sicurezza IT, conformità e strumenti per la gestione dei dati, automatizzando e migliorando i flussi di lavoro IT e i processi SecOps.

Visita l'Add-on Store Netwrix Auditor all'indirizzo **www.netwrix.com/go/add-ons** per trovare add-on gratuiti creati per integrare Netwrix Auditor con il tuo ecosistema IT.

Creato per ambienti IT di tutte le dimensioni, l'architettura Netwrix Auditor favorisce la crescita della tua società

Non profit, 150 dipendenti

Horizon Leisure Centres accelera classificazione dei dati per garantire la sicurezza dei dati sensibili e conformarsi a GDPR.

Istruzione, 1000 impiegati

La William Woods University utilizza Netwrix Auditor per ridurre il rischio di esposizione dei dati e migliorare la sicurezza generale.

Governo, 3.800 impiegati

Johnson County in Kansas ottimizza il rilevamento e l'analisi di eventi sospetti con Netwrix Auditor.

Energia, 5.800 impiegati

Pike Electric risolve i problemi di sicurezza più rapidamente e garantisce la continuità aziendale grazie a Netwrix Auditor.

Premi

Prossime fasi

Prova gratuita

Installazione nel proprio ambiente di prova

On-premises | www.netwrix.it/auditor

Virtuale | netwrix.com/go/appliance

Cloud | netwrix.com/go/cloud

Demo nel browser

Demo interattiva del prodotto nel browser

netwrix.com/it/product_online_demo

Live Demo

Product tour con un esperto Netwrix

netwrix.com/livedemo

Hotline

Per contattarci chiama il numero diretto

Telefono | 1-949-407-5125

Numero verde | 888-638-9749

Italia| +39 02 947 53 539

Contatta l'ufficio vendite

Contatta l'ufficio vendite per avere maggiori informazioni

netwrix.it/contatti

Ufficio centrale

300 Spectrum Center Drive, Suite 200, Irvine, CA 92618, USA

netwrix.it

Social

netwrix.com/social