Netwrix Auditor

Einfachere IT-Audits

Durch die Automatisierung vieler zeitaufwendiger Aufgaben in den Bereichen Sicherheit, Compliance und IT-Betrieb können Sie Ihre Teams entlasten und zugleich die Einhaltung von Sicherheitsvorschriften und Compliance-Vorgaben gewährleisten.

Das Risiko von Datenschutzverletzungen eindämmen

Identifizieren und mindern Sie Risiken für Ihre sensiblen Daten, bevor es zu Datenschutzverletzungen kommt. Minimieren Sie die Auswirkungen von Sicherheitsvorfällen durch eine rechtzeitige Bedrohungserkennung und -abwehr.

Die Compliance sicherstellen und nachweisen

Verbessern Sie die Compliance mit vorkonfigurierten Berichten für Vorschriften wie die DSGVO, PCI DSS, FISMA/NIST, HIPAA und viele mehr, mit denen Sie auch Fragen von Prüfern umgehend beantworten können.

Die Produktivität Ihrer IT-Teams steigern

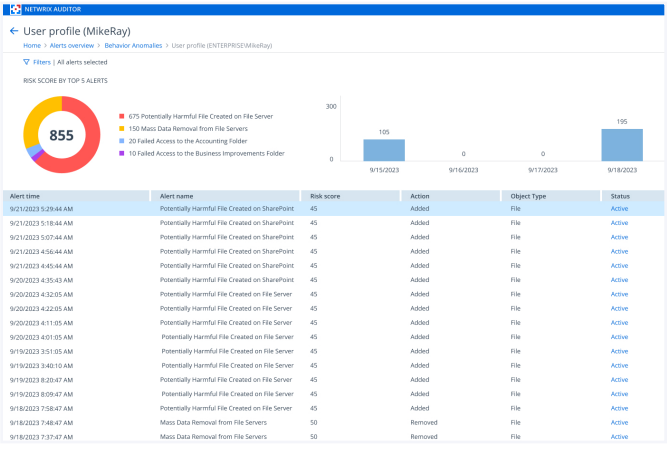
Ermöglichen Sie Ihren IT-Teams eine schnelle Erkennung, Untersuchung und Abwehr von Bedrohungen und automatisieren Sie die Berichterstellung, um den Zeitaufwand zu verringern und Stakeholder auf dem Laufenden zu halten.

ANWENDUNGSSZENARIEN

Untersuchung von Sicherheitsproblemen

Ihre Cybersicherheitsteams benötigen geeignete Tools, um Sicherheitsvorfälle schnell untersuchen und fundierte Entscheidungen treffen zu können.

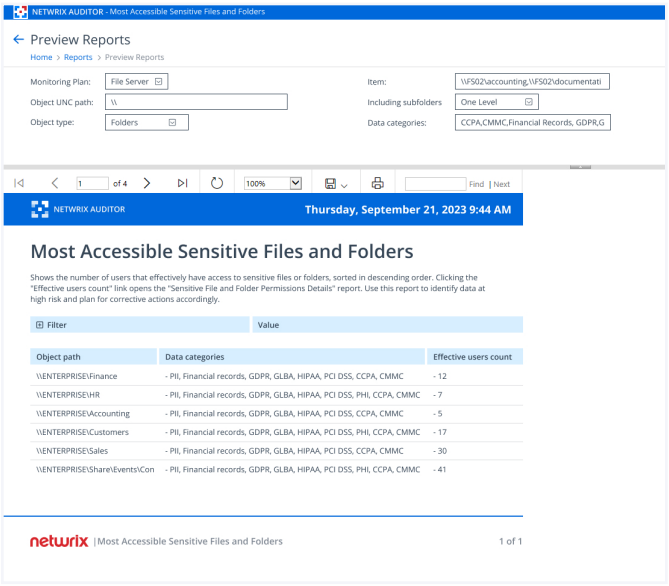
Mit der integrierten Google-ähnlichen Suche von Netwrix Auditor können Sie alle verdächtigen Aktivitäten eines Benutzers einfach anzeigen und analysieren und so Datenschutzverletzungen verhindern. Sie erhalten besseren Einblick in Sicherheitsvorfälle, ohne kryptische Ereignisprotokolle durchforsten zu müssen. Mit Netwrix Auditor können Sie schnell nachvollziehen, was genau passiert ist, wie es zu dem Vorfall kam, wer ihn verursacht hat und welche Ressourcen betroffen sind. So können Sie umgehend geeignete Gegenmaßnahmen ergreifen.



Identifizierung und Schutz exponierter Daten

Die meisten Unternehmen haben nur eine sehr ungenaue Vorstellung davon, welche personenbezogenen Daten, Informationen von Karteninhabern und sonstigen sensiblen Daten in ihren Dateiverzeichnissen gespeichert sind. Wie groß ist der Umfang dieser Informationen? Wo genau sind sie gespeichert? Wer kann darauf zugreifen? Was passiert damit? Und schließlich: Sind sie auch sicher?

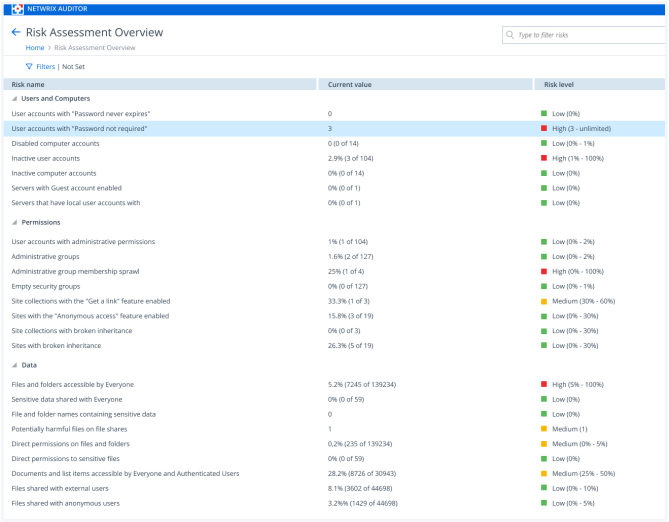
Kombinieren Sie Netwrix Auditor mit Netwrix Data Classification, um exponierte sensible Daten aufzufinden und zu klassifizieren sowie mit geeigneten Maßnahmen zu schützen. Sie erhalten ausführliche Berichte und Warnmeldungen zu allen sensiblen Dateien und Ordnern, ihrem Speicherort, ihren Besitzern, den Benutzern mit Lese- und Schreibzugriff und Systemen, auf die die meisten Benutzer Zugriff haben. Mit diesen detaillierten Informationen haben Sie umfassende Kontrolle über Ihre Daten und können bei Audits die Compliance ganz einfach nachweisen.



Risikobewertung

Die Konfiguration von Benutzerkonten, Berechtigungen oder Datenzugriffsrechten kann eine Vielzahl von Sicherheitsrisiken mit sich bringen. Den meisten Unternehmen fällt es schwer, diese Risiken zu ermitteln.

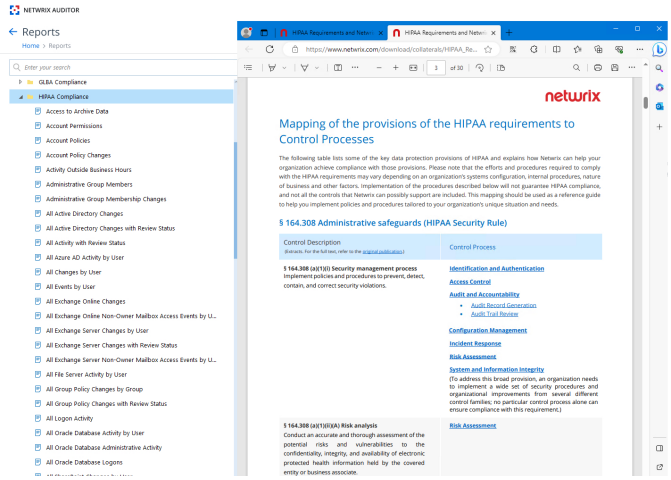
Netwrix Auditor stellt Funktionen für die Risikobewertung bereit, mit denen Sie Sicherheitslücken im Zusammenhang mit Ihren Daten, Identitäten und Infrastrukturen identifizieren und geeignete Schutzvorkehrungen ergreifen können, um Ihre Angriffsfläche zu verringern. Mit Netwrix Auditor lassen sich Sicherheitsrisiken wie für alle Benutzer zugängliche Dateien und Ordner, Benutzerkonten ohne Passwörter oder mit unbegrenzt gültigen Passwörtern, leere Sicherheitsgruppen, potenziell schädliche Dateien auf Dateifreigaben und viele weitere Gefahren automatisch erkennen.



Compliance-Berichte

Die Erstellung von Compliance-Berichten ist für Unternehmen stets mit hohem Aufwand verbunden. Für Compliance-Beauftragte sind Audits eine zeitraubende Aufgabe, da sie präzise und zuverlässige Daten für die unterschiedlichen Anforderungen bereitstellen müssen und Compliance-Prozesse naturgemäß sehr ressourcenintensiv sind.

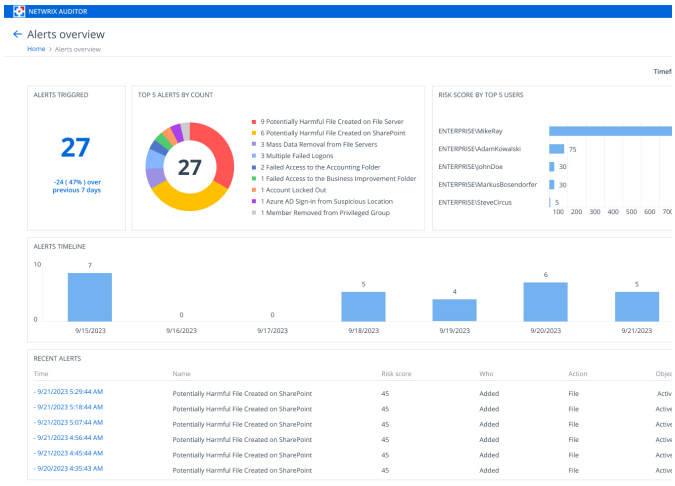
Mit den Compliance-Berichten und dem Compliance-Mapping von Netwrix Auditor können Sie Vorschriften und Standards einfacher einhalten und die erforderlichen Compliance-Nachweise erbringen. Das Compliance-Mapping von Netwrix Auditor hilft Ihnen, die Anforderungen einer bestimmten Vorschrift besser zu verstehen und Maßnahmen umzusetzen, die für Ihr Unternehmen wichtig sind. Durch die Kombination von Netwrix Auditor mit Netwrix Data Classification haben Sie außerdem die Möglichkeit, alle regulierten Daten in Ihrem Unternehmen nach Art der Vorschrift aufzufinden und zu ermitteln, wo diese gespeichert sind und welche Aktionen mit diesen Daten wann und von wem durchgeführt wurden.



Bedrohungserkennung

Angesichts wachsender Datenmengen und immer ausgefeilterer Angriffsmethoden ist es schwierig, Bedrohungen mit herkömmlichen Verfahren zu erkennen und zu untersuchen.

Durch Aufdecken von ungewöhnlichem Benutzerverhalten ermöglicht Netwrix Auditor eine schnellere Reaktion auf Vorfälle und die Abwehr von Insider-Bedrohungen. Die Lösung kann Aktivitäten, die eine Gefahr für Ihre sensiblen Daten darstellen, umgehend erkennen. Hierzu gehören beispielsweise unerlaubte Versuche, Benutzerberechtigungen auszuweiten, Benutzer, die erstmals auf sensible Daten zugreifen, Benutzerkonten, die kurz nach ihrer Erstellung und dem Hinzufügen zu privilegierten Gruppen wieder gelöscht wurden oder eine große Anzahl fehlgeschlagener Aktivitäten (z. B. Anmeldeversuche).



WICHTIGE FUNKTIONEN

Dashboard für die Risikobewertung

Identifizieren Sie Sicherheitslücken im Zusammenhang mit Ihren Daten und Ihrer Infrastruktur. Hierzu gehören beispielsweise eine große Anzahl direkt erteilter Berechtigungen oder eine zu hohe Zahl inaktiver Benutzer. Ergreifen Sie geeignete Gegenmaßnahmen, um Ihre Angriffsfläche zu verringern.

Schutz sensibler Daten

Legen Sie den Schwerpunkt auf den Schutz Ihrer wichtigsten Ressourcen, indem Sie die sensiblen Daten in Ihrer IT-Umgebung auffinden und regelmäßig überprüfen, wer darauf zugreifen kann und was damit geschieht (Netwrix Data Classification erforderlich).

Berichte zu Änderungen, Zugriffen und Konfigurationen

Greifen Sie mithilfe der Berichte schnell auf die Informationen zu, die Ihre Geschäftsführung, Prüfer und andere Stakeholder benötigen, anstatt unzählige Skripte, Protokolldateien und Tabellen zu durchsuchen.

Zugriffsüberprüfungen

Setzen Sie das Prinzip der geringsten Rechte konsequent um, indem Sie die Zugriffsüberprüfung an Datenbesitzer delegieren und es Ihnen mit dem optionalen Modul für Zugriffsüberprüfungen ermöglichen, vorhandene Berechtigungen zu genehmigen oder Änderungen anzufordern.

Warnmeldungen

Lassen Sie sich über verdächtige Aktivitäten rund um Ihre sensiblen Daten benachrichtigen. Richten Sie Warnmeldungen ein, die durch bestimmte Ereignisse ausgelöst werden, damit Sie reagieren können, bevor es zu einer Datenpanne kommt oder Sie Bußgelder infolge von Compliance-Verstößen zahlen müssen.

Bedrohungserkennung

Identifizieren Sie böswillige Insider-Angriffe und kompromittierte Konten mithilfe einer umfassenden Übersicht über alle Warnmeldungen zu ungewöhnlichen Aktivitäten eines Benutzers einschließlich der dazugehörigen Risikoeinstufung.

Google-ähnliche Suche

Mit wenigen Klicks lassen sich genau die benötigten Details auffinden, beispielsweise alle Zugriffsereignisse für einen Benutzer oder sämtliche Aktivitäten im Zusammenhang mit einer bestimmten vertraulichen Datei. So können Sie Vorfällen ganz einfach auf den Grund gehen, Benutzerprobleme beheben oder Fragen von Prüfern umgehend beantworten.

Vorkonfigurierte Compliance-Berichte

Die Lösung stellt vorkonfigurierte Berichte für die Kontrollen zahlreicher Standards wie NIS2, ISO27001, TISAX, der DSGVO, PCI DSS, HIPAA, SOX, GLBA, FISMA/NIST und CJIS bereit.

INTEGRATIONEN

UNTERSTÜTZTE DATENQUELLEN

Unstrukturierte Daten

- Microsoft 365 (Exchange, Exchange Online, SharePoint Online und Teams)
- Netzwerkgeräte (Cisco, Fortinet, Palo Alto, SonicWall, Juniper, Cisco Meraki, HPE Aruba und Pulse Connect Secure)
- SharePoint Server
- VMware
- Windows-Dateiserver
- Windows-Server
- NAS-Speicher
  - NetApp
  - Qumulo
  - Nutanix
  - Dell Data Storage
  - Synology

Strukturierte Daten

- SQL Server
- Oracle Database

Verzeichnisdienste

- Active Directory
- Microsoft Entra ID

INTERNE INTEGRATIONEN

Netwrix Data Classification
Netwrix Data Classification identifiziert und klassifiziert sensible und geschäftskritische Inhalte im gesamten Unternehmen. Durch die Integration in Netwrix Auditor sind Sie in der Lage, Ihre Datensicherheitsmaßnahmen gezielt auf diese Daten auszurichten: Ermitteln und minimieren Sie die größten Risiken (z. B. personenbezogene Informationen, auf die Gruppen wie „Jeder“ Zugriff haben), beschränken Sie den Zugriff auf das absolute Minimum und decken Sie gefährliche Aktivitäten umgehend auf.

PolicyPak
Netwrix PolicyPak ist eine moderne Desktop-Verwaltungsplattform mit einem leistungsstarken Framework für die Erstellung, Verwaltung und Implementierung von Richtlinien für Remote-Mitarbeiter. Die Integration in Netwrix Auditor ermöglicht Benutzern das Anzeigen von PolicyPak-bezogenen Änderungen an Gruppenrichtlinienobjekten direkt in Netwrix Auditor über die Admin-Konsole von PolicyPak. Dank dieser Integration können Änderungen an Gruppenrichtlinienobjekten einfacher validiert und überprüft werden, ohne manuell auf eine separate Berichtsplattform zugreifen zu müssen.

EXTERNE INTEGRATIONEN

SIEM-Systeme

Sie können Netwrix Auditor über eine RESTful API und eines unserer kostenlosen Add-ons ganz einfach in beliebige SIEM-Lösungen integrieren. Mit einer solchen integrierten Lösung können Sie Ihre SIEM-Ergebnisdaten mit aussagekräftigen Kontextinformationen in einem leicht verständlichen Format anreichern, einschließlich der Werte vor und nach einer Änderung sowie fehlgeschlagener und erfolgreicher Anmeldeversuche. Sicherheitsanalysen mit detaillierten Ergebnissen ermöglichen Ihnen eine schnelle Untersuchung ungewöhnlicher Aktivitäten. So können Sie Risiken mindern und Maßnahmen ergreifen, um künftig ähnliche Probleme zu vermeiden. Netwrix Auditor minimiert die Menge der indizierten Daten, indem aussagekräftige Audit-Informationen an Ihre SIEM-Lösung übertragen werden und damit die Kosteneffizienz verbessert wird. Folgende Add-ons sind verfügbar:

- AlienVault USM
- ArcSight
- IBM QRadar
- Intel Security
- LogRhythm
- Solarwinds Log & Event Manager
- Splunk
- Allgemeine SIEM-Lösung[1]

Professionelle Automatisierungstools

Durch die Integration von Netwrix Auditor in PSA-Tools (Professional Services Automation) profitieren Sie von einem effizienten Incident Management, einer schnellen Erkennung von Vorfällen und einer automatisierten Ticket-Erstellung. Damit sind Sie in der Lage, Ihre Incident-Management-Prozesse zentral zu steuern und automatisch Tickets zu erstellen und an den zuständigen Mitarbeiter weiterzuleiten, sobald Warnmeldungen von Netwrix Auditor ausgelöst werden. Da das Ticket alle wichtigen Details (wer, was, wann und wo) enthält, können Sie mit diesem Prozess schneller auf Vorfälle reagieren und Ihre SLAs einhalten. Es sind die Add-ons ConnectWise Manager und ServiceNow ITSM verfügbar.

Weitere Lösungen

Netwrix Auditor lässt sich in eine Vielzahl weiterer Lösungen integrieren. Mit den folgenden Add-ons können Sie Ereignisinformationen aus den entsprechenden Lösungen abrufen und in Netwrix Auditor verwalten:

- Amazon Web Services
- CTERA Enterprise File Services Platform
- CyberArk Privileged Access Security
- Allgemeiner Linux-Syslog
- Okta
- Microsoft System Center Virtual Machine Manager
- Nasuni File Data Platform
- Privileges User Monitoring unter Linux und Unix
- Radius Server

Netwrix Auditor Integration API

Die Netwrix Auditor Integration API ermöglicht den Zugriff auf Audit-Daten, die Netwrix Auditor über RESTful API-Endgeräte erfasst.

[1] Dieses allgemeine Add-on ist mit allen SIEM-Lösungen kompatibel, die Eingabedaten im Format .CEF oder Ereignisprotokollformat unterstützen.

BEREITSTELLUNG

HARDWAREANFORDERUNGEN

Netwrix Auditor kann auf virtuellen Maschinen mit Microsoft Windows-Gastbetriebssystem auf der entsprechenden Virtualisierungsplattform – insbesondere VMware vSphere, Microsoft Hyper-V und Nutanix AHV – bereitgestellt werden.

SOFTWAREANFORDERUNGEN

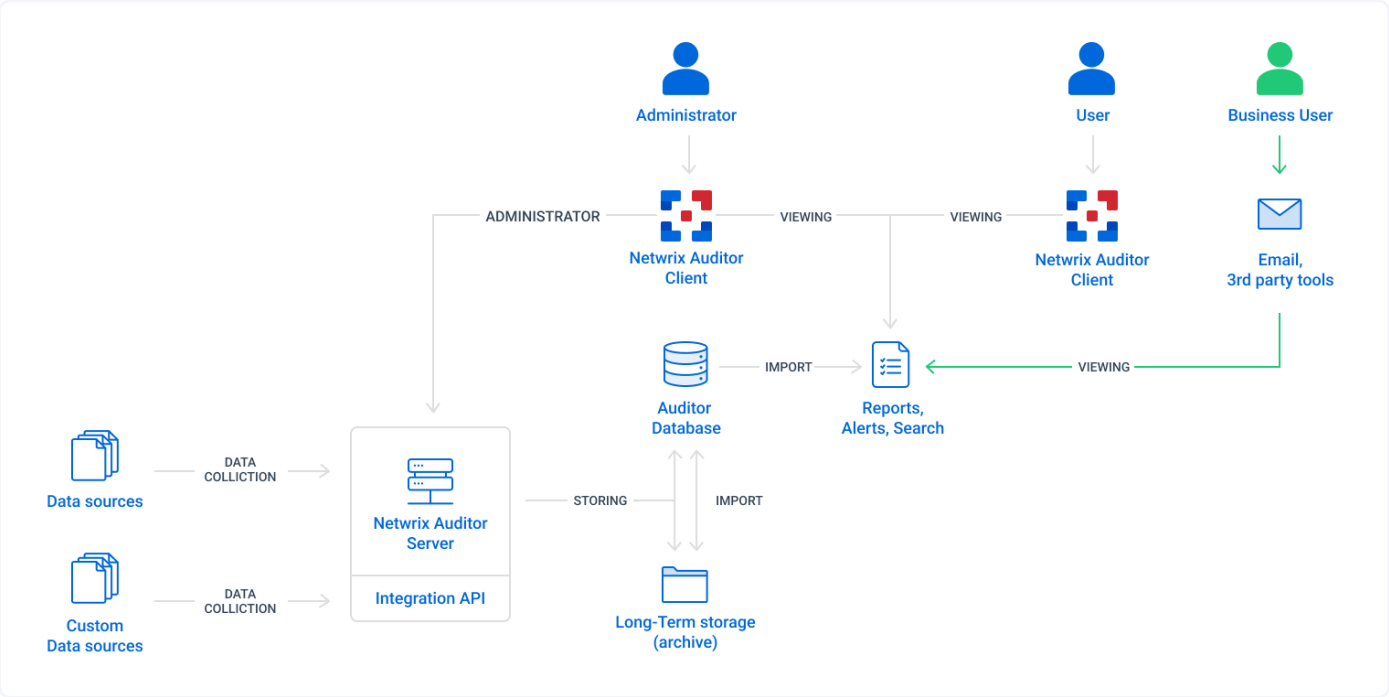
Windows Server-Betriebssystem:	Windows Desktop-Betriebssystem:	.NET Framework:	SQL Server	Installationsprogramm:
▪ Windows Server 2022 ▪ Windows Server 2019 ▪ Windows Server 2016 ▪ Windows Server 2012 R2	▪ Windows 10 ▪ Windows 8.1	.NET Framework 4.8 und höher	SQL Server 2008 R2 oder höher ▪ Standard Edition ▪ Enterprise Edition	Windows Installer 3.1 und höher

LIZENZIERUNG

Die meisten Anwendungen von Netwrix Auditor werden auf Basis aktivierter AD-Benutzer lizenziert. Ausnahmen sind in der folgenden Tabelle aufgeführt:

Name der Anwendung	Basis der Lizenzierung
Netwrix Auditor for Active Directory (hybride Lizenz)	Aktivierter AD-Benutzer + aktivierter Microsoft Entra ID-Benutzer mit reiner Cloudidentität
Netwrix Auditor for Exchange (hybride Lizenz)	Postfach
Netwrix Auditor for Network Devices	Gerät
Netwrix Auditor for Oracle Database	Prozessor
Netwrix Auditor for Windows Server	Aktivierter AD-Benutzer ODER Server

ARCHITEKTURDIAGRAMM



NÄCHSTE SCHRITTE

Kostenlose Testversion
Persönliche Demo anfordern
Browser-Demo starten

Weitere Informationen zu kostenlosen Add-ons
Weitere Informationen zu Netwrix Data Classification

Firmenzentrale:
6160 Warren Parkway, Suite 100 Frisco, TX, US 75034
DE: +49 221 599 88 029 **UK:** +44 203 588 3023

netwrix.com/social