Netwrix Auditor

IT 감사 부담 완화

이전에는 완료하는 데 몇 시간이 걸렸던 보안, 규정 준수 및 IT 운영 작업을 자동화하여 과도한 부담 없이 조직을 안전하고 규정을 준수하도록 유지할 수 있습니다.

데이터 유출 위험 최소화

중요 데이터를 식별하고, 최소 권한 액세스 적용을 통해 관련 위험을 완화합니다. 그리고 이를 지속적으로 유지합니다.

법규 준수 및 증명

대량 파일 시스템에 대한 최소 권한 액세스 제어 적용, 오래된 사용자 개체 정리 등 반복적인 작업을 자동화하여 시간과 비용을 절약합니다.

자동화로 IT 팀 업무 부담 완화

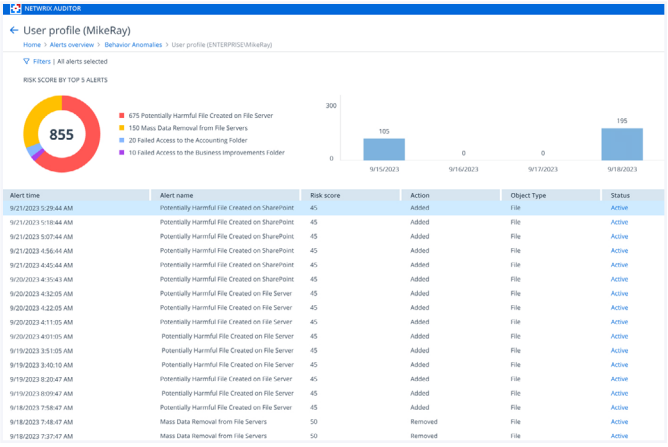
미리 구성된 보고서로 일반적인 요구 사항에 맞춰 감사 준비 속도를 높이거나 고유한 요구 사항을 충족하는 사용자 지정 보고서를 손쉽게 생성합니다.

사용 사례

보안 문제 조사

적절한 도구 부재 시, 사이버 보안 팀의 사고 조사 시간이 증가하고 의사 결정의 정확성이 떨어집니다.

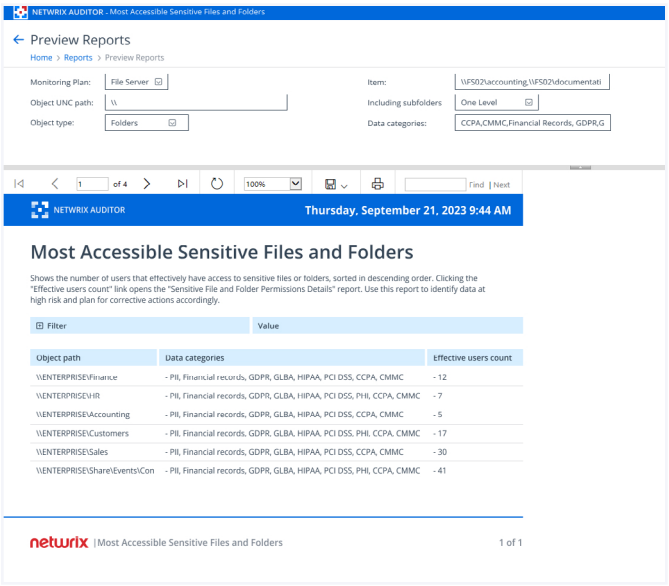
Netwrix Auditor는 Google과 유사한 검색 인터페이스를 내장하여 사용자 관련 의심스러운 활동을 쉽게 찾고 분석함으로써 데이터 유출을 예방하거나 차단할 수 있도록 돕습니다. 암호 같은 이벤트 로그를 샅샅이 뒤지지 않고도 보안 사고에 대한 명확한 가시성을 확보할 수 있니다. Netwrix Auditor는 정확히 무슨 일이 있었는지, 어떻게 발생했는지, 무엇이 영향을 받았는지, 누가 책임이 있는지 빠르게 파악하여 즉각적이고 효과적으로 대응할 수 있도록 지원합니다.



과다 노출된 데이터 식별 및 조치

대부분의 기업은 자사 파일 저장소에 있는 개인 정보, 카드 소지자 정보 등 민감한 데이터에 대한 정보가 매우 부족 합니다. 데이터 양은 얼마나 되는지, 어디에 저장되어 있는지, 누가 접근 권한을 가지고 있는지, 어떤 활동이 이루어지고 있는지, 그리고 궁극적으로 안전한지 등을 제대로 파악하지 못하고 있습니다.

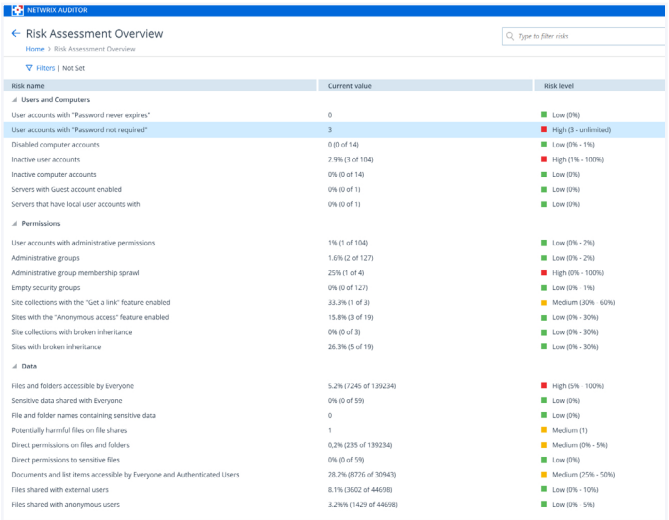
Netwrix Auditor와 Netwrix Data Classification을 결합하면 과다 노출된 민감한 데이터를 검색, 분류 및 조치할 수 있습니다. 민감한 파일과 폴더의 위치, 소유자, 읽기 및 쓰기 권한을 가진 사용자, 그리고 대부분의 사용자가 접근할 수 있는 파일과 폴더에 대한 상세 보고서와 알림을 제공합니다. 이를 통해 데이터를 완벽하게 제어하고 법규 준수를 감사 시 쉽게 입증할 수 있습니다.



위험 평가

사용자 계정, 권한 또는 데이터 액세스 권한 설정으로 인해 조직은 수많은 보안 위협에 노출될 수 있습니다. 대부분의 기업애개 이러한 위험을 찾내아내는 것은 쉽지 않습니다.

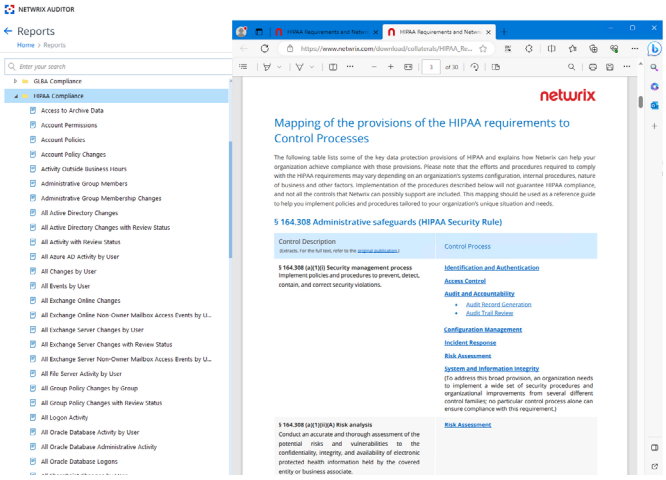
Netwrix Auditor의 위험 평가 기능을 통해 데이터, ID 및 인프라 관련 보안 취약점을 파악하고, 그리고 공격 표면을 줄이기 위한 조치를 취할 수 있습니다. Netwrix Auditor는 모든 사용자가 접근 가능한 파일 및 폴더, 암호가 없거나 만료되지 않는 계정, 빈 보안 그룹, 파일 공유 시 유해 가능성이 있는 파일 등 다양한 보안 위험을 자동으로 감지합니다.



규정 준수 보고

규정 준수 보고는 조직에 과도한 시간과 노력을 요구합니다. 다양한 요구 사항에 대한 정확하고 신뢰할 수 있는 데이터 확보와 자원 집약적인 규정 준수 프로세스로 인해 규정 준수 감사는 담당자들에게 큰 부담이 됩니다.

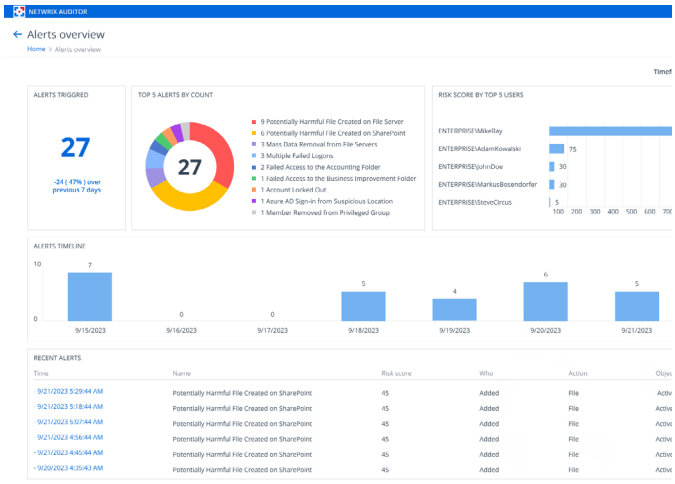
Netwrix Auditor의 규정 준수 보고서와 매핑 기능을 활용하면 규정 및 표준을 더욱 쉽게 준수하고 감사자에게 규정 준수를 입증할 수 있습니다. Netwrix Auditor의 규정 준수 매핑은 특정 규정의 요구 사항을 파악하고 조직에 필요한 조치를 구현하는 데 도움을 줍니다. 또한 Netwrix Auditor를 Netwrix Data Classification과 함께 사용하면 규제 유형별로 모든 규제 대상 데이터를 검색하고, 데이터의 위치, 수행된 작업, 시기 및 담당자를 확인할 수 있습니다.



위협 탐지

데이터 양의 증가와 정교해진 공격 기법으로 인해 기존 방식으로는 위협을 찾아내고 조사하기가 어렵습니다.

Netwrix Auditor는 비정상적인 사용자 행위를 탐지하여 사고 대응 속도를 높이고 내부자 위협을 방지합니다. 사용자 권한의 무단 상승 시도, 이전에 접근하지 않았던 민감한 데이터에 대한 접근, 생성 직후 삭제되고 권한 그룹에 추가된 계정, 또는 로그온 시도 실패와 같은 다수의 실패한 활동 등 민감한 데이터를 위협하는 행위를 즉시 탐지합니다.



주요 기능들

위험 평가 대시보드

직접 할당된 권한 과다 또는 비활성 사용자 계정 과다와 같은 데이터 및 인프라 보안 취약점을 파악하고, 공격 표면을 줄이기 위한 조치를 취하십시오.

민감한 데이터 보호

IT 환경 전반의 민감한 데이터를 파악하고, 접근 권한을 가진 사용자를 정기적으로 검토하고, 관련 활동을 모니터링하여 가장 중요한 자산을 우선적으로 보호하십시오. (Netwrix Data Classification 필요)

변경, 액세스 및 구성 보고서

스크립트, 로그 파일, 스프레드시트를 이용하는 대신 보고서에서 경영진, 감사 진행자 등 이해관계자에게 필요한 정보를 신속하게 추출할 수 있습니다.

사용자 액세스 검토

데이터 소유자에게 액세스 검토를 위임하고, 선택적 액세스 검토 모듈을 통해 현재 권한 승인 또는 변경 요청을 가능하게 하여 최소 권한 원칙을 정확하게 적용합니다.

알림

민감한 데이터 관련 의심스러운 활동에 대한 알림을 받으세요. 특정 이벤트 발생 시 알림을 받도록 설정하여 데이터 유출이나 규정 위반으로 인한 벌금 부과 전에 대응할 수 있습니다.

위협 탐지

개인별 비정상 활동알림 및 누적 위험 점수에 대한 종합적인 보기를 통해 악의적인 내부자와 해킹된 계정을 식별합니다.

구글 느낌의 검색 기능

몇 번의 클릭만으로 사용자의 모든 액세스 이벤트 또는 특정 민감한 파일 관련 모든 활동과 같은 정확한 정보를 찾아 사고 원인을 쉽게 파악하고, 사용자 문제를 해결하거나, 감사자의 질문에 즉각적으로 답변할 수 있습니다.

사전 정의 법규 준수 보고서

PCI DSS, HIPAA, SOX, GDPR, GLBA, FISMA/NIST, CJIS등 다양한 표준의 규제 사항에 맞춰 사전 구성된 보고서를 바로 사용할 수 있습니다.

통합 기능들

지원 데이터 소스

정리되지 않은 데이터

- Microsoft 365 (Exchange, Exchange Online, SharePoint Online 및 Teams)
- 네트워크 장비 (Cisco, Fortinet, Palo Alto, SonicWall, Juniper, Cisco Meraki, HPE Aruba, 및 Pulse Connect Secure)
- SharePoint 서버
- VMware
- Windows 파일 서버
- Windows Server
- NAS 스토리지
  - Netapp
  - Qumulo
  - Nutanix
  - Dell 데이터 스토리지
  - Synology

정리된 데이터

- SQL Server
- Oracle DB

디렉토리 서비스

- Active Directory
- Microsoft Entra ID

내부 통합 기능

Netwrix Data Classification

Netwrix Data Classification 은 조직 전체의 민감한 데이터 및 중요 비즈니스 콘텐츠를 식별하고 분류합니다. Netwrix Auditor와 통합하면 민감한 데이터 보안에 집중하여 "모든 사용자" 그룹에 공개된 개인 정보와 같은 주요 위험을 파악하고 완화하고, 불필요한 접근 권한을 제거하고, 위협적인 활동을 즉시 탐지할 수 있습니다.

PolicyPak

Netwrix PolicyPak은 강력한 정책 생성, 관리 및 배포 프레임워크를 제공하는 최신 데스크톱 관리 플랫폼으로, 원격 근무 환경에 적절합니다. Netwrix Auditor와의 통합을 통해 사용자는 PolicyPak 관리 콘솔에서 Netwrix Auditor 의 PolicyPak 관련 GPO 변경 사항을 직접 확인할 수 있습니다. 이는 GPO 변경 사항에 대한 검증, 감사 및 검토 프로세스를 간소화하여 별도의 보고 플랫폼에 수동으로 접근할 필요가 없도록 합니다.

외부 통합 기능

SIEM 시스템

무료 애드온 중 하나를 사용하여 RESTful API를 통해 Netwrix Auditor를 SIEM 솔루션과 쉽게 통합할 수 있습니다. 통합된 솔루션을 통해 변경 및 데이터 액세스 시도 (성공 및 실패 모두) 에 대한 이전 및 이후 값을 포함한 실행 가능한 정보를 사람이 읽을 수 있는 형식으로 SIEM 데이터에 추가할 수 있습니다. 이러한 실행 가능한 보안 분석 정보를 통해 비정상적인 활동을 신속하게 조사하고 위험을 완화하며 향후 유사한 문제를 방지하는 방법을 파악할 수 있습니다. Netwrix Auditor는 SIEM에 실행 가능한 감사 정보만 제공하여 인덱싱되는 데이터 양을 최소화하고 SIEM의 비용 효율성을 높입니다. 사용 가능한 애드온은 다음과 같습니다.

- AlienVault USM
- ArcSight
- IBM QRadar
- Intel Security
- LogRhythm
- Solarwinds 로그 & 이벤트 매니저
- Splunk
- 일반적 SIEM 솔루션[1]

전문 자동화 도구

효율적인 사고 관리, 신속한 사고 탐지 및 자동화된 티켓 생성을 위해 Netwrix Auditor를 PSA(전문 서비스 자동화) 도구와 통합 하세요. Netwrix Auditor 알림이 발생하면 티켓이 자동으로 생성 및 할당되어 사고 관리 프로세스를 중앙 집중화할 수 있습니다. 티켓에는 누가-무엇을-언제-어디서와 같은 중요 정보가 모두 포함되어 사고 대응 속도를 높이고 SLA 준수에 도움을 줍니다. 사용 가능한 애드온은 ConnectWise Manage와 ServiceNow ITSM입니다.

다른 솔루션들

Netwrix Auditor는 다양한 솔루션과 통합할 수 있습니다. 이러한 애드온을 통해 해당 솔루션의 이벤트 정보를 Netwrix Auditor 에서 확인하고 관리할 수 있습니다. 사용 가능한 애드온은 다음과 같습니다.

- Amazon Web Services
- CTERA 엔터프라이즈 파일 서비스 플랫폼
- CyberArk Privileged Access Security
- 일반적 Linux syslog
- Okta
- Microsoft 시스템 센터 VM 관리자
- Nasuni 파일 데이터 플랫폼
- 리눅스와 Unix 의 사용자 모니터링 권한
- RADIUS 서버

Netwrix Auditor 통합 API

Netwrix Auditor 통합 API는 REST API 엔드포인트를 통해 Netwrix Auditor에서 수집한 감사 데이터에 대한 액세스를 제공합니다.

[1] 이 일반 애드온은 .CEF 또는 이벤트 로그 형식의 입력 데이터를 지원하는 모든 SIEM 솔루션과 호환됩니다.

배포

하드웨어 요구사항

VMware vSphere, Microsoft Hyper-V, Nutanix AHV 등의 가상화 플랫폼에서 Microsoft Windows 게스트 OS를 실행하는 가상 머신에 Netwrix Auditor를 배포할 수 있습니다.

소프트웨어 요구사항

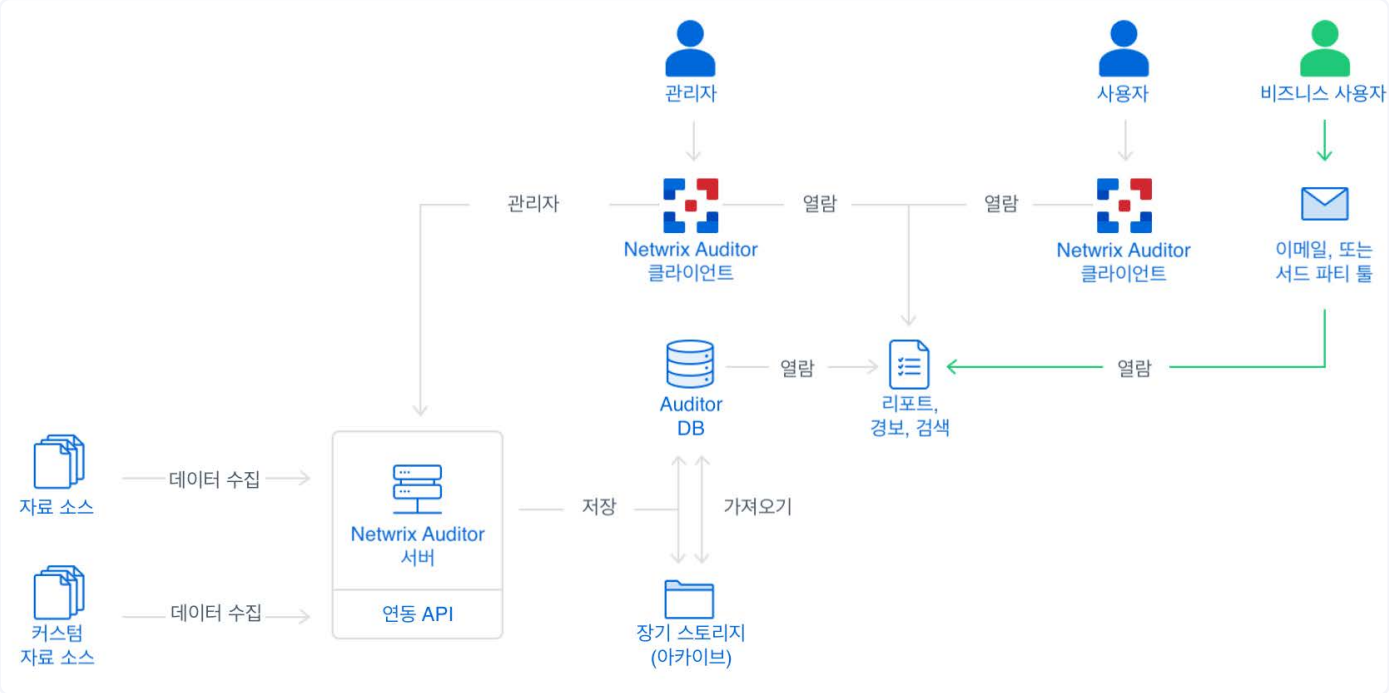
Windows Server OS:	Windows 데스크톱 OS:	.NET 프레임워크:	SQL Server	인스톨러:
▪ Windows Server 2022 ▪ Windows Server 2019 ▪ Windows Server 2016 ▪ Windows Server 2012 R2	▪ Windows 10 ▪ Windows 8.1	.NET 프레임워크 4.8 이상	SQL Server 2008 R2 이상 ▪ Standard Edition ▪ Enterprise Edition	Windows Installer 3.1 이상

라이선싱

Netwrix Auditor 애플리케이션 라이선스를 대부분 "활성화된 AD 사용자" 를 기준으로 합니다. 예외 사항은 다음 스프레드시트에서 확인할 수 있습니다.

애플리케이션 이름	라이선싱 기준
Active Directory용 Netwrix Auditor (하이브리드 라이선스)	활성화된 AD 사용자 + 클라우드 전용 Microsoft Entra ID 사용자
Exchange용 Netwrix Auditor (하이브리드 라이선스)	사서함
네트워크 장비용 Netwrix Auditor	장비
Oracle DB용 Netwrix Auditor	프로세서
Windows Server용 Netwrix Auditor	활성화된 AD 사용자 혹은 서버

아키텍처 다이어그램



다음 단계

무료 체험판 받기
일대일 데모 요청
인-브라우저 데모 실행

무료 애드온 더 알아보기
Netwrix Data Classification 더 알아보기

네트릭스 코리아: 서울특별시 송파구 법원로 11길 11, B-1501, 05836 | 전화: 1644-7718

판매처 데이터시큐어: 010-6272-2714 **코소시스솔루션:** 010-5251-5239 **빅씨엔에스:** 010-8881-3769 **이지스케이:** 010-5295-9688 netwrix.com/social