ManageEngine
ADAudit Plus

UBA 기반의 변경 감사 도구

Active Directory, Windows 서버, 파일 서버 및 워크스테이션의 보안 및 규정 준수 유지

ADAudit Plus의 역할

ManageEngine ADAudit Plus는 실시간 변경 감사 및 보고 소프트웨어로 다음 기능을 수행합니다.

- AD(Active Directory), Azure AD, Windows 파일 서버, 멤버 서버 및 워크스테이션을 모니터링하고 HIPAA, GDPR, SOX, CCPA, GLBA 등과 같은 규정을 준수하도록 돕습니다.
- 클릭 몇 번만으로 원시 이벤트 로그 데이터를 실행 가능한 보고서로 변환하여 Windows 에코시스템에서 누가 언제 무엇을 했는지 표시
- UBA(사용자 행동 분석) 기능을 사용하여 비정상적인 활동을 식별하고 기업에 대한 잠재적 위협을 탐지합니다.

규정준수 된 감사보고서

SOX, HIPPA, PCI-DSS, FISMA & GLBA 규정준수 요구사항을 충족합니다.

- SOX Compliance
- PCI-DSS Compliance
- HIPPA Compliance
- FISMA Compliance
- GLBA Compliance
- GDPR Compliance

컴플라이언스에 의해 관리되는 조직은 ADAudit Plus와 같은 자동환 된 정보 모니터링 시스템에 의존해야 합니다. 이러한 시스템은 효과적인 정보 보안 통제, 지속적이고 철저한 모니터링 및 많은 감사보고서를 최고의 기밀성, 무결성 및 정확성을 보장합니다.

ADAudit Plus가 조직에 도움을 주는 분야

ManageEngine ADAudit Plus로 다음 기능을 수행할 수 있습니다.

1. 온-프레미스 AD 및 Azure AD의 변경에 대한 자세한 보고서 보기
2. Windows 사용자 로그온 활동에 대한 가시성 제공
3. AD 계정 잠금에 대한 보고, 분석 및 문제 해결
4. 도메인에서 특수 권한사용자의 활동을 면밀히 모니터링
5. 로그인/로그오프, 사용자, 그룹 변경 등을 추적
6. Windows, NetApp, EMC, Synology, Huawei 및 Hitachi 스토리지에서 파일 활동 감사
7. UBA(사용자 행동 분석)로 위협 탐지 강화
8. SOX, HIPAA, PCI DSS, GDPR 및 기타 규정에 대한 사전 준비된 감사 보고서 출력

ADAudit Plus의 하이라이트

1. AD 및 Azure AD 변경 감사 및 보고
2. 파일 서버 감사(Windows, NetApp, EMC, Synology, Huawei, Hitachi)
3. 그룹 정책 설정 변경 감사
4. Windows 서버 및 멤버 서버 감사 및 보고
5. 워크스테이션 감사
6. 사용자 행동 분석(UBA)
7. 특수 권한 사용자 모니터링

Active Directory 감사

AD 개체 및 GPO의 변경 사항에 대한 보고;
사용자 로그온 활동 추적, 계정 잠금 분석 등

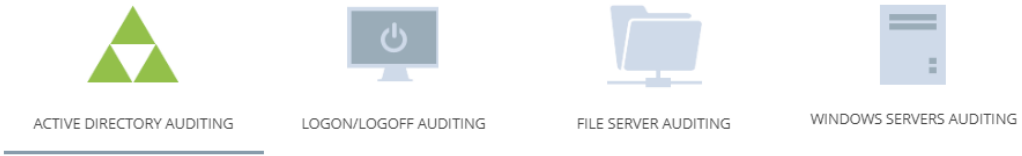
AD 감사

- **모든 AD 개체 변경 감사**: 변경된 속성의 이전 및 새 값과 같은 세부 정보를 사용하여 OU, 사용자, 그룹, 컴퓨터 및 기타 AD 개체에 대한 변경 사항을 추적.
- **GPO 설정 변경 추적**: 컴퓨터 구성 변경, 암호 및 계정 잠금 정책 변경 등을 포함하여 GPO 및 해당 설정에 대한 변경 사항을 감사
- **사용자 로그온 활동 모니터링**: 사용자의 성공적인 로그온 시도 및 실패한 로그온 시도에 대한 자세한 보고서 출력
- **계정 잠금 문제 해결**: 경고를 통해 계정 잠금을 빠르게 감지하고 광범위한 Windows 구성 요소 목록에서 해당 원인을 식별.
- **특수 권한 사용에 대한 가시성 확보**: 특수 권한 사용자 계정을 지속적으로 감사하고 상세한 감사 추적을 유지함으로써 기업의 권한 사용을 면밀히 주시.
- **하이브리드 AD 환경 감**사: 중요한 이벤트에 대한 경고를 통해 하이브리드 환경에서 발생하는 모든 활동에 대한 상호 연관된 통합 보기 제공

Windows Active Directory 실시간 감사

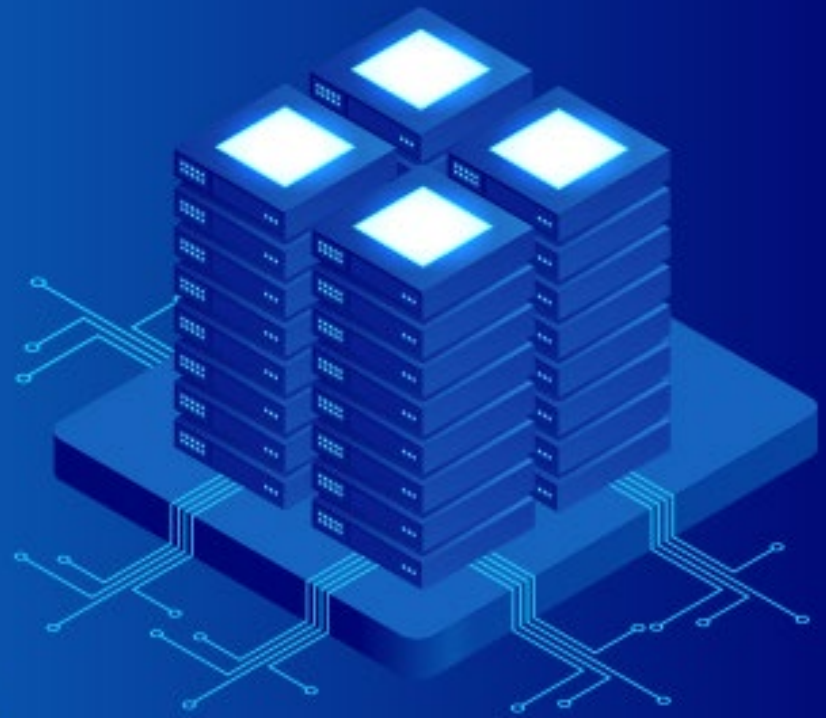
사용자, 그룹, GPO, 컴퓨터 및 OU 변경사항에 대한 전체정보를 감사, 모니터링 및 보고됩니다.

- Active Directory 감사
- Active Directory 감사보고서
- 사용자 관리 작업에 대한 추적
- 사용자 관리 감사 보고서
- Active Directory 사용 권한 변경 감사
- 계정 잠김 분석
- SIEM 감사 솔루션
- Active Directory 그룹 감사 보고서
- 직원 근무 시간
- 실시가 AD 모니터링
- 사용자 로그온 작업 추적
- 사용자 로그온 감사 보고서
- GPO 변경 감사
- GPO 감사 보고서
- AD 신규/ 이전 속성 변경 사항
- AD 경고에 대한 알람 및 이메일 발송
- Windows 보안 로그 감사
- Active Directory LAP 감사
- Active Directory 보안 감사
- 내부자 위험 탐지
- Active Directory 변경 보고서
- 백업 데이터의 보고서
- Windows DNS 스키마 감사
- 이동식 저장소 감사
- 규정 준수 감사 보고서
- 실시간 AD 변경 감사 보고서
- SIEM 통합
- Azure AD 감사
- 계정 잠김 시험 도구
- 사용자 행동 분석(UBA)



파일 서버 감사

Windows, NetApp, EMC 및 Synology 저장 장치 전반에 걸친 파일 액세스 및 수정에 대한 감사 및 보고



파일 서버 감사

- **파일 및 폴더 액세스 모니터링**: 읽기, 삭제, 수정, 복사하여 붙여넣기, 이동 등을 포함한 모든 파일 활동을 실시간으로 추적
- **실패한 파일 액세스 시도 감지**: 파일 또는 폴더에 대한 액세스 시도 실패에 대한 보고서
- **권한 변경 감사**: NTFS를 추적하고 이전 및 새 값과 같은 세부 정보와 함께 권한 변경 사항을 공유.
- **파일 무결성 모니터링**: 특정 파일, 특정 사용자 또는 이러한 이벤트에 대한 이메일 및 SMS 알림을 통해 변경한 것과 같은 중요한 이벤트를 쉽게 감지.
- **파일 공유 감사**: 다음을 사용하여 도메인의 공유 파일 및 폴더에 대한 모든 액세스 및 변경 사항을 추적. 누가 무엇을, 언제, 어디서 액세스했는지에 대한 세부 정보

Windows 파일 서버 감사

파일 및 폴더 구조, 공유 및 권한의 문서 변경에 대한 포렌식을 사용하여 파일 생성, 수정 및 삭제를 안전하게 추적합니다.

- Windows 파일 서버 감사
- 수정 및 액세스 권한
- NetAPP 필터 감사
- EMC 파일 서버 감사
- 사전 정의된 보고서 및 알림
- 파일 서버 클러스터 감사
- 규격 준수 감사 보고서
- 모든 Windows 파일 서버 변경 감사 보고서

그룹 정책 설정 변경 감사

암호 및 계정 잠금 정책 변경, 컴퓨터 변경 등을 포함하여 그룹 정책 설정에 대한 변경 사항을 감사.

그룹 정책 설정 변경 감사

- **그룹 정책 개체 감사**: 그룹 정책 개체(GPO) 생성, 삭제, 수정 등에 대한 감사 및 보고
- **GPO 설정 변경 추적**: 포괄적인 보고서를 통해 누가, 언제, 어디서 어떤 GPO 설정을 변경하는지 면밀히 주시.
- **중요한 변경 사항에 대한 경고 구성**: 컴퓨터 구성 변경, 암호 및 계정 잠금 정책 변경 등과 같은 중요한 변경 사항에 대한 즉각적인 이메일 및 SMS 경고를 수신.
- **감사 추적 유지**: 모든 변경 전후에 GPO 설정 값에 대한 보고서를 생성하여 원치 않는 변경을 즉시 탐지.

Windows 서버 감사

실시간 보고서 및 경고로 멤버 서버를 모니터링하여 Windows 네트워크의 활동을 면밀히 주시합니다.

Windows 서버 감사

- Windows 서버 감사: 로컬 관리 그룹 멤버, 로컬 사용자, 사용자 권한, 로컬 정책 등에 대한 변경 사항 모니터링
- 예약된 작업 및 프로세스 추적: 예약된 작업 및 프로세스의 생성, 삭제 및 수정을 감사.
- 이동식 장치 사용 모니터링: USB 플러그인 및 이동식 저장 장치에 대한 파일 전송 활동 식별
- PowerShell 프로세스 감사: Windows 서버에서 실행되는 명령과 함께 Windows 서버에서 실행되는 PowerShell 프로세스를 모니터링.
- ADFS(Audit AD federation services): ADFS 인증 시도의 성공 및 실패를 실시간으로 보고.

워크스테이션 감사

사용자의 로그온 및 로그오프 정보, 생산 시간, 로그온 기록 세부 정보, 이동식 저장소 사용 등을 추적.

워크스테이션 감사

- 로그온 및 로그오프 활동 감사: Windows 네트워크에서 로그온 및 로그오프 활동을 추적하고, 로그온 기간을 기록하고, 현재 로그온한 사용자를 식별.
- 사용자 로그온 기록 추적: 모든 로그온 활동 기록, 여러 컴퓨터에 로그온한 사용자 식별, RADIUS 로그온 모니터링 등
- 로그온 실패 식별: 로그온을 시도한 사람, 로그온을 시도한 컴퓨터, 시기 및 실패 이유에 대한 정보를 사용하여 실패한 모든 로그온 시도를 추적.
- 파일 무결성 모니터링: 시스템 및 프로그램 파일에 대한 모든 변경 사항에 대한 자세한 보고서 수신
- 직원 생산성 측정: 직원의 유휴 시간과 실제 작업 시간을 추적하여 기업 전체에서 높은 생산성을 보장.

사용자 행동 분석

악의적인 로그인, 측면 이동, 권한 남용, 데이터 침해 및 맬웨어와 같은 위협 감지 및 완화

UBA를 통한 위협 헌팅

- 기업 전반적인 환경에서 로그 처리: 구성된 DC, 멤버 서버 및 워크스테이션에서 로그를 수집하고 처리합니다.
- 안전한 기준선 식별: 처리된 로그 데이터는 일반 로그온, 파일 사용자 관리 및 프로세스 활동에 대한 사용자별 기준선을 생성하는 데 사용됩니다.
- 이상 징후 식별 및 관리자에게 알림: 수신 로그 데이터와 처리된 기준선을 비교하여 이상 징후를 감지하고 관리자에게 알리므로 추가 조사가 가능.
- 잠재적 보안 위협 탐지: 악성 로그온, 권한 남용, 권한 상승, 데이터 유출, 맬웨어 공격 등의 잠재적 사례를 신속하게 탐지
- 사건 대응 자동화: 보안 사건 발생에 따라 장치를 즉시 종료하거나 사용자 세션을 종료하는 등 피해를 완화하는 데 걸리는 시간을 단축.

특수 권한 사용자 모니터링

도메인 전체에서 권한 있는 사용자 계정을 감사하고 감사 추적을 유지하여 의심스러운 행동을 빠르게 감지합니다.

특수 권한 사용자 모니터링

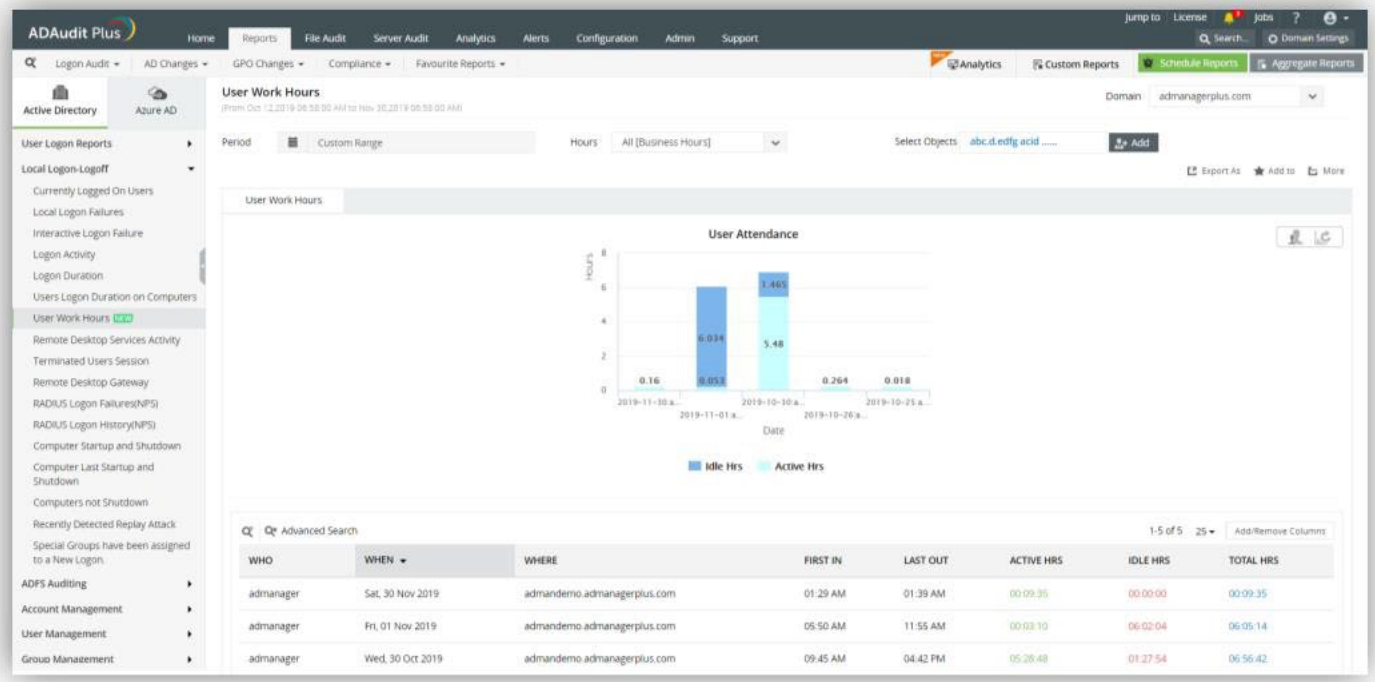
- 관리자 활동 감사: AD(Active Directory) 스키마, 구성, 사용자, 그룹, OU(조직 구성 단위), GPO(그룹 정책 개체) 등에 대한 관리 사용자 작업 추적
- 특수 권한 사용자 활동 검토: 도메인에서 권한 있는 사용자가 수행한 활동에 대한 감사 추적을 유지 관리하여 다양한 IT 규정을 준수.
- 권한 상승 탐지: 사용자의 최초 권한 사용을 문서화한 보고서로 권한 상승을 식별하고 사용자의 역할 및 의무에 필요한지 확인
- 이상 행동 탐지: 일반적인 액세스 패턴에서 벗어나는 작업을 식별하여 권한 있는 계정의 도용 또는 공유 자격 증명을 사용하여 공격자를 찾습니다.
- 의심스러운 활동에 대한 경고 수신: 경고를 구성하여 감사 로그 삭제 또는 업무 시간 외에 중요한 데이터 액세스와 같은 중요한 이벤트를 신속하게 감지하고 대응합니다.

주요 특징

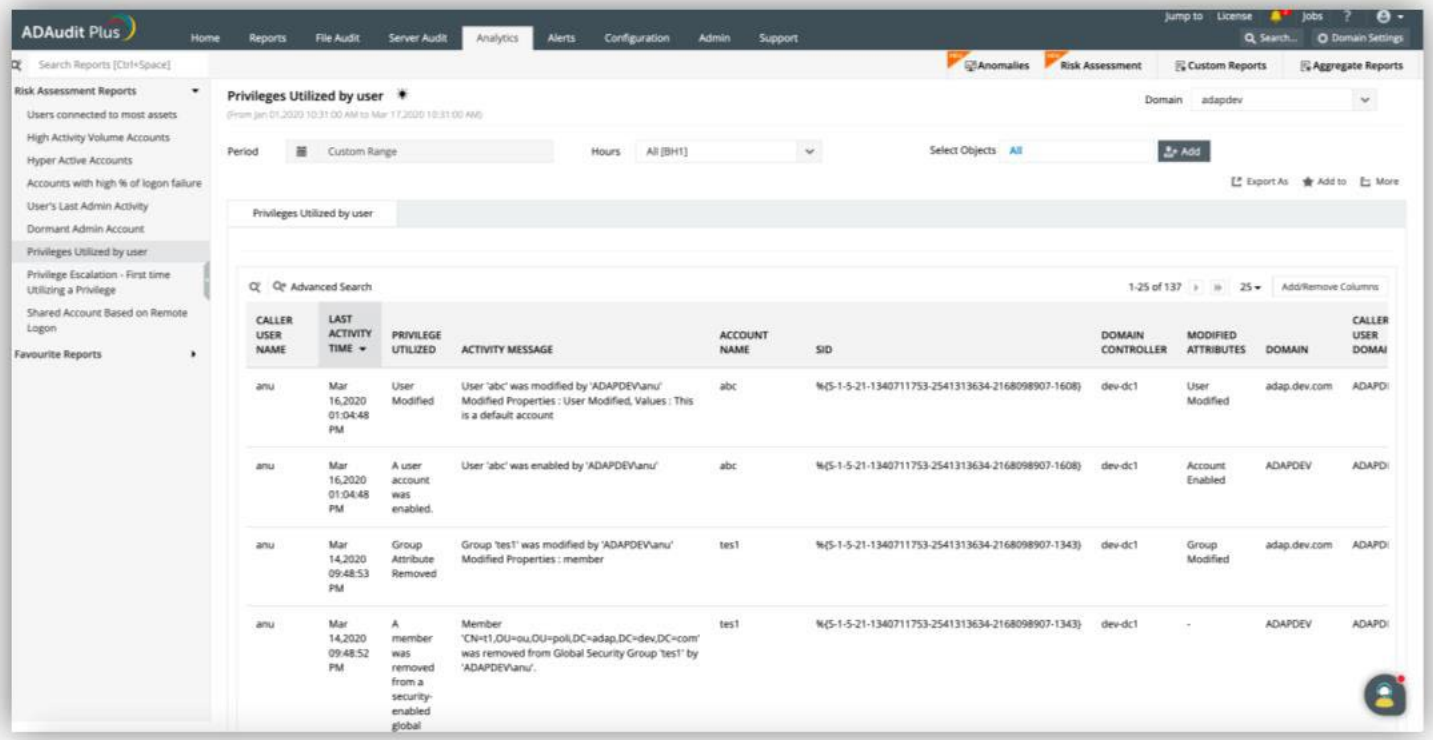
고객이 선호하는 대시보드

고객이 선호하는 기능

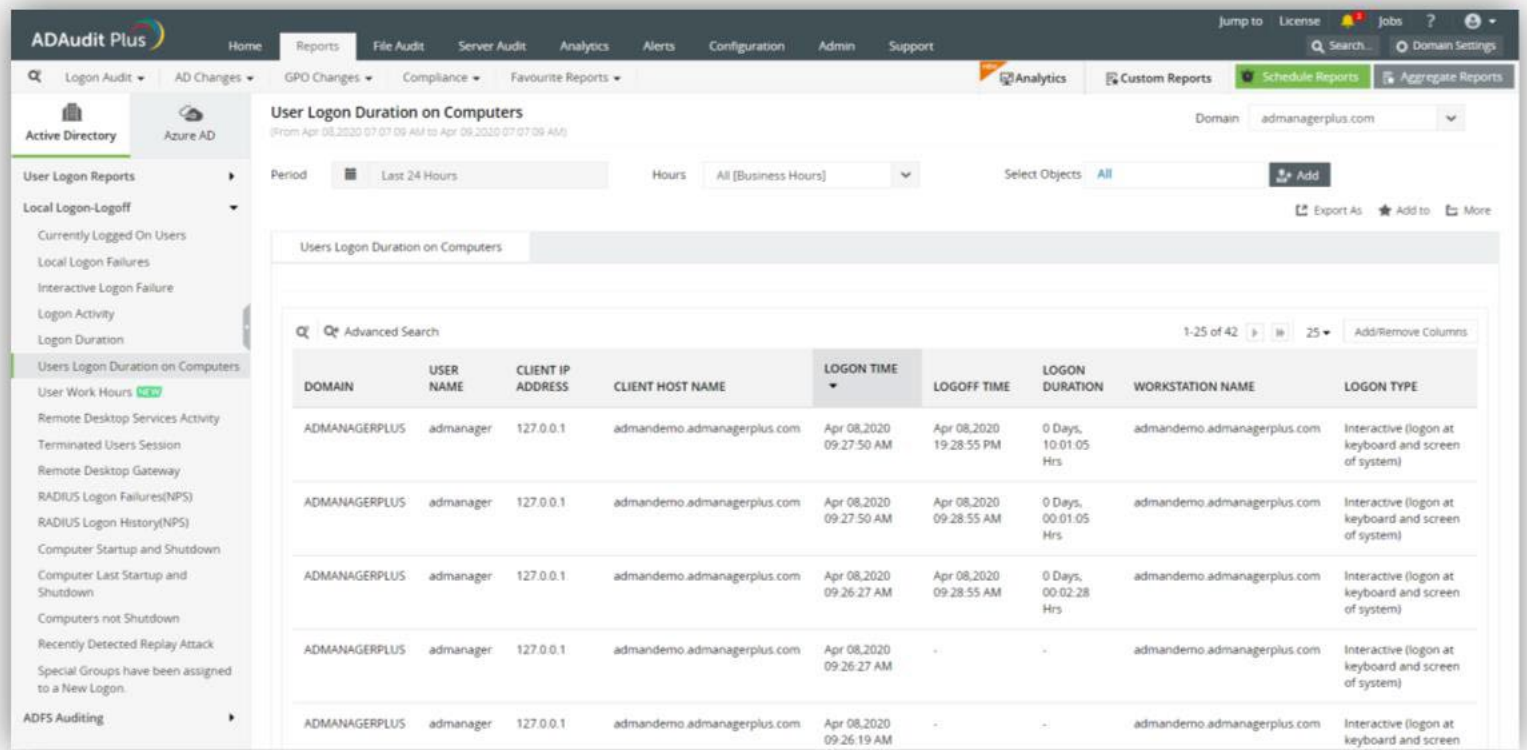
- 사용자 작업 시간 모니터링: 사용자 환경 내에서 컴퓨터를 사용하는 직원의 출근, 활동 시간, 유휴 시간 및 생산 시간을 추적합니다.



- **내부자 위협 탐지**: 악의적인 로그인, 권한 남용, 측면 이동, 데이터 잘못 취급 등과 같은 내부자 위협 지표를 즉시 탐지합니다.



- **로그온/로그오프 추적**: 로그온 및 로그오프 작업에 대한 사용자별 정보 가져오기, 여러 컴퓨터에 로그온한 사용자 확인, IP 주소 및 로그온 시간 보기



ADAudit Plus를 고객이 좋아 하는 이유

- 즉각적인 알림: 중요한 사용자의 중요한 이벤트 또는 활동에 대한 즉각적인 이메일 통지
- 위협 탐지 및 대응: UBA 엔진은 권한 남용, 내부자 공격, 멀웨어 및 기타 위협을 신속하게 탐지하고 맞춤형 대응을 실행 및 기타 위협, 맞춤형 대응 실행
- 250개 이상의 보고서: 감사 준비 보고서를 통해 PCI DSS, HIPAA, SOX, GDPR, GLBA, ISO 27001등을 포함한 여러 규정 준수 간소화
- 로그 보관 및 포렌식 분석: 사용자 정의 위치에 감사 데이터를 보관하고 필요할 때 이를 기반으로 보고서를 생성.
- 기술 지원 팀: 효율적인 지원 팀은 이메일, 전화 통화 또는 채팅으로 지원.

지원되는 플랫폼

DC 및 멤버 서버 감사	파일 감사	기타 구성 요소
Windows 서버 버전: 2003/2003 R2	Windows 파일 서버 감사: 서버 2003이상	AD FS 감사: AD FS 2.0이상
2008/2008 R2	EMC 감사: VNX, VNXe, Celerra, Unity, Isilon	워크스테이션 감사: Window 11, 10, 8, 7, 비스타, 그리고 XP
2012/2012 R2	Synology 감사: DSM 5.0 이상	PowerShell 감사: PowerShell 버전 4.0, 5.0
2016/2016 R2	NetApp Filer 감사: Data ONTAP 7.2 이상	
2019	NetApp Cluster 감사: Data ONTAP 8.2.1이상	

제품 에디션 종류

Standard	Professional
아래의 라이선스된 장치에서 수집된 이벤트 로그 데이터에 대한 보고 및 경고: Domain controllers Azure AD tenant Windows servers Workstation Windows file servers Synology NAS servers NetApp filers Huawei file storage Hitachi NAS storage	Standard 기능 모두 포함 아래 추가 기능 제공: 그룹 정책 설정 변경 추적 계정 잠금 분석 AD 권한 변경 감사 DNS 변경 추적 AD 개체/속성 값 변경 전후 AD 스키마 및 구성 변경 추적 등

라이선스 세부정보

Active Directory Auditing 구성 요소에 대한 ADAudit Plus의 라이선스는 도메인 컨트롤러의 수를 기반으로 합니다.

기타 추가 기능은 다음 수를 기반으로 합니다.

- Azure AD tenant 수
- 파일 서버 수
- EMC 파일 서버/NetApp 파일러/Synology NAS 서버/ Huawei NAS/ Hitachi NAS 서버 수
- 멤버 서버 수
- Workstation 수

Fortune 100대 기업 10 개 기업 중 9개 기업이 사용 중입니다.

ManageEngine
ADAudit Plus

ManageEngine

감사합니다

텔리맨트 주식회사
https://www.tmn.co.kr
02) 588-7350

기술 질문: inforeq@tmn.co.kr
견적 요청: sales-info@tmn.co.kr