Workday 보안 및 데이터 보호

소개

비즈니스가 점차 디지털화되는 가운데 IT 리더의 최우선 과제는 고객 데이터, 직원 데이터, 지적 자산 데이터를 확실히 보호하는 것입니다. 또한 기업을 노리는 보안 위협이 갈수록 지능화되고 있으므로 서비스의 모든 영역에서 보안 및 데이터 보호에 최선을 다해야 합니다. 그렇다면 Workday는 어떻게 보안을 실현하고 데이터를 보호하는지 IT 전문가의 관점에서 살펴보겠습니다.

규정 준수 및 인증

Workday와 Workday 고객은 각종 국제 개인정보 보호 규정을 준수해야 합니다. 모든 지역에서 공통으로 시행되는 개인정보 보호 원칙에는 고지, 선택, 액세스, 사용, 공개, 보안에 관한 내용이 포함됩니다. Workday 어플리케이션에서는 차별화된 구성을 적용하여 국가별 법을 준수할 수 있습니다.

또한 Workday는 고객 데이터에 대한 무단 접근, 사용, 공개를 막는 기술 및 조직 차원의 안전장치가 포함된, 포괄적이고 문서화된 정보 보안 프로그램을 운영하면서 국제 개인정보 보호 규정을 준수합니다.

외부 감사: SOC1 및 SOC2 리포트

Workday의 운영, 정책, 절차에 대한 정기적인 감사를 통해 Workday가 서비스 제공자에게 요구되는 모든 기준을 충족하고 있음을 보장합니다. Workday는 SOC1(Service Organization Controls 1) Type II 리포트를 발행합니다. SAS 70의 후속 리포트인 SOC1은 SSAE 18(Statement on Standards for Attestation Engagements No. 18) 및 ISAE 3402 (International Standard on Assurance Engagements No. 3402)에 따라 발행됩니다.

이와 같이 2가지 표준의 요건을 이행하는 리포트를 통해 세계 각지의 기업들이 Workday와 같은 서비스 제공자가 적절한 통제를 수행하고 있음을 확신할 수 있습니다. 이 리포트는 (사베인스 옥슬리(Sarbanes Oxley)법에 의거하여) 고객의 재무제표에 영향을 미칠 아웃소싱된 중요 비즈니스 태스크에 대해 어떤 내부 통제가 이루어지고 있는지 알아야 하는 고객 또는 잠재고객을 위해 작성됩니다. SOC1의 범위는 Workday 프로덕션 시스템으로 제한되며, SOC1 감사는 독립적인 제3자 감사기관에 의해 6개월마다 시행됩니다. 감사 완료 후 고객 및 잠재고객에게 리포트가 제공됩니다.

Workday는 SOC2(Service Organization Controls 2) Type II 리포트도 발행합니다. Workday SOC2 리포트는 신뢰 서비스 원칙 및 조건(보안, 가용성, 기밀 유지, 처리 무결성, 개인정보 보호)을 모두 다룹니다. 고객이 Workday 서비스에 제출한 데이터를 포함하는 모든 Workday 시스템이 SOC2의 범위에 속합니다. 이 리포트는 Workday의 내부 보안 통제에 대해 알아야 하는 고객 또는 잠재고객을 위해 작성됩니다. SOC2 감사는 독립적인 제3자 감사기관에 의해 연 1회 시행되며, 감사 완료 후 고객 및 잠재고객에게 리포트가 제공됩니다.

SOC1 및 SOC2 감사 모두 Workday의 프로덕션 데이터 센터, 백업 및 복구 절차, 소프트웨어 개발 프로세스, 논리 보안 통제를 위한 물리적 및 환경적 안전장치를 검증합니다.

ISO 27001, 27017, 27018 인증

ISO 27001은 국제 표준화 기구(ISO) 및 국제전자기술위원회(IEC)가 2005년에 처음 발표한 정보 보안 표준입니다. 2013년 9월, ISO 27001:2013이 발표되어 최초의 2005년 표준을 대체했습니다. ISO 27001은 전 세계에서 인정받는 표준 기반 보안 접근 방식이며, 조직의 정보 보안 관리 시스템(ISMS)이 갖춰야 할 요건을 제시합니다.

2015년에 발표된 ISO 27017은 ISO 27001을 보완하는 표준입니다. 이 표준은 클라우드 서비스 프로비저닝 및 사용에 적용되는 정보 보안에 관한 통제 및 이행 지침을 제공합니다.

ISO 27018은 2014년에 ISO/IEC에서 발표한 보완 표준이며, 개인 데이터를 취급하는 클라우드 서비스 제공자에 적용되는 지침으로 구성됩니다.

Workday는 2010년 9월에 ISO 27001, 2015년 10월에 ISO 27018, 2017년 11월에 ISO 27017 인증을 각각 취득했습니다. 독립적인 평가를 통해 Workday가 ISO 표준을 준수하고 있음이 확인되면 인증이 부여됩니다. ISO 재인증은 3년마다 시행되지만, 매년 감독 감사를 받아야 인증이 유지됩니다. 이러한 ISO 인증은 Workday가 개인정보 보호와 보안에 최선을 다하고 있으며 Workday의 통제 기능이 제대로 실행되고 있음을 입증합니다. ISO 인증서 및 ISMS 적용성 보고서는 고객이 검토할 수 있습니다.

국가 간 데이터 전송

유럽 경제 지역(EEA)과 미국 간의 개인 데이터 전송에는 엄격한 데이터 보호 법률이 적용됩니다. EEA에서 영업 중인 고객이 이러한 요건을 이행할 수 있도록 Workday는 유럽위원회가 승인한 표준 계약 조항을 데이터 보호 협약에 수용하고 "모델 계약"이라는 명칭으로 참조합니다. 모델 계약에서는 EEA에서 제3국으로 개인 데이터를 전송할 때 적합성 요건을 충족할 수 있도록 계약 형태의 메커니즘을 제공합니다.

또한 Workday는 EU-미국 프라이버시 실드 및 스위스-미국 프라이버시 실드에 대한 자가 인증도 완료했습니다. 프라이버시 실드는 세이프 하버 프레임워크를 대체하며, 특히 유럽 사법재판소가 세이프 하버 프레임워크를 무효화한 판결에서 지적한 문제점의 해결을 목적으로 합니다. Workday는 프라이버시 실드에 참여하고 있습니다. TRUSTe는 Workday가 프라이버시 실드 프로그램에 사용하는 제3자 인증 방식입니다.

미국 상무부 프라이버시 실드 프로그램에 대한 자세한 내용은 http://www.privacyshield.gov에서, 표준계약조항에 대해서는 http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm에서 확인하실 수 있습니다.

고객 데이터를 안전하게 지키려는 Workday의 노력 및 Workday의 개인정보 보호 프로그램에 대한 자세한 내용은 Workday 개인정보 보호 프로그램 데이터시트를 참조하십시오.

유럽 일반 개인정보 보호법

유럽 일반 개인정보 보호법(General Data Protection Regulation, GDPR)은 유럽 연합(EU)에서 제정했으며, 기존 데이터 보호 지침(Data Protection Directive) 95/46/EC 및 회원국별 시행 규정을 폐지하고 대체합니다. 2018년 5월 25일자로 EU의 전체 28개 회원국에서 발효된 이 법은 모든 EU 회원국의 기존 데이터 보호법을 간소화하고 일치시킵니다. GDPR은 EU에 위치한 기업뿐만 아니라 그 소재지와 관계없이 EU 시민의 개인 정보를 처리하거나 저장하는 모든 기업에 적용됩니다.

Workday는 GDPR에서 정의하는 데이터 처리자에 해당합니다. Workday는 종합적으로 GDPR 요건을 평가하고 다양한 개인정보 보호 및 보안 방침을 이행하여 GDPR이 발효되는 즉시 데이터 처리자 요건을 준수했습니다. 이러한 방침에는 다음이 포함됩니다.

- 보안 및 개인정보 보호 방침에 관한 직원 교육
- 개인정보 보호 영향 평가 실행
- 고객에게 다양한 데이터 전송 방법 제공
- 처리 활동 기록 유지관리
- 고객에게 구성 가능한 개인정보 보호 및 규정 준수 기능 제공

Workday 서비스는 개인정보 보호를 고려한 설계 및 기본적인 개인정보 보호를 중요하게 생각합니다. Workday는 GDPR 준수가 전 세계의 Workday 고객에게 매우 중요한 비즈니스 우선 과제임을 잘 알고 있습니다. 따라서 EU 감독 기관에서 발표하는 GDPR 관련 지침을 계속 모니터링하면서 Workday 규정 준수 프로그램을 최신 버전으로 유지합니다.

데이터 보안

물리적 보안

Workday는 완전히 이중화된 서브시스템 및 상호 격리된 보안 구역을 갖추고 미션 크리티컬 컴퓨터 시스템을 호스팅하도록 설계된 첨단 데이터 센터에 프로덕션 시스템을 코로케이션하여 운영합니다. Workday 데이터 센터는 가장 엄격한 물리적 보안 조치를 취합니다.

- 서버 영역에 액세스하려면 다중 인증을 거쳐야 합니다.
- 중요 구역에 액세스하려면 2중 생체 인식 인증이 필요합니다.
- 카메라 감시 시스템이 내부 및 외부의 주요 진입 지점에 설치되어 있습니다.
- 보안팀이 연중무휴 24시간 데이터 센터를 모니터링합니다.
- 무단 액세스 시도는 데이터 센터 보안팀에 의해 기록되고 모니터링됩니다.

데이터 센터에 대한 모든 물리적 액세스는 엄격히 제한되고 규제됩니다. Workday는 여러 보안 모범 사례, 즉 "최소 액세스" 강화 서버, 정기 유지보수 기간 등을 적용하면서 데이터를 다룹니다.

데이터 분리

Workday는 다중 테넌트 SaaS 어플리케이션입니다.

Workday의 핵심 기능인 다중 테넌시는 여러 고객이 Workday 시스템의 단일 물리적 인스턴스를 공유할 수 있게 하면서 각 고객 테넌트의 어플리케이션 데이터를 격리합니다. Workday는 이를 위해 Workday 개체 관리 서버(OMS)를 사용합니다. 모든 사용자 ID는 정확히 하나의 테넌트와 연결되고, 이를 통해 Workday 어플리케이션에 액세스하게 됩니다.

어플리케이션 개체(조직, 근무자 등)의 모든 인스턴스는 테넌트 기반입니다. 따라서 새 개체가 생성되면 역시 해당 사용자의 테넌트에 연결되고, 이 연결은 취소할 수 없습니다. Workday 시스템은 이러한 연결을 자동으로 유지관리하고, 사용자 ID 및 테넌트를 기준으로 삼아 모든 개체에 대한 액세스를 제한합니다. 사용자가 데이터를 요청하면 시스템에서 자동으로 테넌시 필터를 적용하여 사용자의 테넌트에 해당하는 정보만 불러옵니다.

저장된 데이터의 암호화(데이터베이스 보안)

Workday는 어플리케이션에 포함된 고객 데이터의 모든 속성을 암호화한 다음 데이터베이스에 저장합니다. 이는 Workday 기술의 기본적인 설계 특성입니다. Workday는 AES(Advanced Encryption Standard) 알고리즘과 256비트 키를 사용합니다. 이러한 암호화가 가능한 이유는 Workday가 디스크 기반 RDBMS 어플리케이션이 아닌 인메모리 개체 지향 어플리케이션이기 때문입니다. 특히 Workday의 메타데이터는 Workday OMS에 의해 해석되며 메모리에 저장됩니다. 모든 데이터 입력, 업데이트, 삭제는 MySQL 데이터베이스의 영구 저장소에 커밋됩니다. 이런 특별한 아키텍처 덕분에 Workday는 10여 개의 데이터베이스 테이블만 사용하면 됩니다. 그와 달리 RDBMS 기반 어플리케이션은 수만 개의 테이블이 필요하며, 따라서 성능 문제로 전체 데이터베이스 암호화가 불가능합니다.

전송 중 데이터 암호화(네트워크 보안)

사용자는 인터넷에서 TLS(Transport Layer Security)의 보호를 받으면서 Workday에 액세스합니다. 이 기술은 수동적인 도청, 적극적인 변조, 메시지 위조의 위험으로부터 네트워크 트래픽을 보호합니다.

Workday는 경계 방어, 네트워크 침입 차단 시스템 등 선제적인 보안 절차도 구현했습니다. 또한 Workday 자체 리소스 및 외부 제3자 벤더가 정기적으로 Workday 네트워크 인프라에 대한 취약성 평가 및 침입 테스트를 수행합니다.

데이터 백업

Workday 마스터 프로덕션 데이터베이스는 외부 데이터 센터에서 유지관리되는 슬레이브 데이터베이스에 실시간으로 복제됩니다. 매일 이 슬레이브 데이터베이스로부터 전체 백업을 수행합니다. Workday 데이터베이스 백업 정책에 따라 데이터베이스 백업 및 트랜잭션 로그를 수집해야 합니다. 그러면 상업적으로 합당한 범위에서 트랜잭션 손실을 최소화하면서 데이터베이스를 복구할 수 있습니다. 트랜잭션 로그는 트랜잭션 로그에 마지막으로 입력한 후 데이터 백업을 2차례 할 때까지 보존됩니다. 인터페이스를 구현하는 시스템의 데이터베이스 백업은 인터페이스 시스템을 지원하는 데 필요한 기간에 사용 가능해야 합니다. 이 기간은 시스템별로 다릅니다. 데이터베이스 및 트랜잭션 로그의 백업은 고객 데이터가 포함된 모든 데이터베이스에 대해 암호화됩니다.

재해 복구

Workday는 Workday 표준 서비스 수준 협정(SLA)에 따라 서비스를 보장합니다. SLA에는 Workday 프로덕션 서비스에 대한 재해 복구(DR) 계획이 포함되어 있는데, 복구 시간 목표(RTO)가 12시간, 복구 시점 목표(RPO)는 1시간입니다. RTO는 Workday 프로덕션 서비스를 사용할 수 없게 된 시점부터 다시 사용 가능해지는 시점까지로 측정합니다. RPO는 첫 트랜잭션이 소실된 시점부터 Workday 프로덕션 서비스를 사용할 수 없게 된 시점까지로 측정합니다.

Workday는 이러한 SLA 약정을 지키고자 프로덕션 환경을 완벽하게 복제한 DR 환경을 유지관리합니다. 뜻하지 않게 정전이 발생하고 사전 정의된 기간보다 길어질 것 같으면 Workday는 DR 계획을 실행합니다. DR 계획은 최소 6개월마다 테스트를 거칩니다.

단일 보안 모델

기존 ERP 시스템과 달리 Workday는 단일 보안 모델을 운영합니다. 여기에는 사용자 액세스, 시스템 통합, 보고, 모바일 기기 및 IT 액세스가 포함됩니다. 모든 사용자는 Workday 보안 모델을 통해 로그인하고 허가를 받아야 합니다. 반면에 기존 ERP 시스템은 대개 어플리케이션 계층의 보안을 사용하므로, IT 및 DBA 직원이 우회하여 데이터베이스 레벨에서 직접 데이터에 액세스할 수 있습니다. Workday에서는 이것이 불가능합니다. Workday는 암호화된 영구 데이터 저장 기능을 갖춘 개체 지향 인메모리 시스템입니다. 따라서 액세스 이벤트 및 변경사항은 추적 및 감사 대상이 됩니다. 이 특별히 견고한 보안 모델과, 효과적으로 모든 데이터 업데이트의 날짜를 기록하고 감사하는 자동 기능을 연계함으로써 거버넌스 및 규정 준수에 드는 시간과 비용을 절감하고 전반적인 보안 위험을 낮출 수 있습니다.

인증

Workday 보안 액세스는 역할을 기반으로 하며, 사용자 및 웹 서비스 통합에 싱글 사인온(SSO) 및 x509 인증을 사용하도록 SAML을 지원합니다. Workday에서는 고객이 다양한 사용자 집단별로 인증 요건을 다르게 설정할 수 있습니다.

또한 지리적 차이점 또는 조직 차원의 차이점 때문에 복수의 사용자 인증 유형이 필요한 경우에는 사용자가 인증 유형을 선택할 수 있게 합니다.

싱글 사인온 지원

LDAP가 통합 사용자 이름/비밀번호 솔루션을 지원한다면, SAML은 더 나아가 전사적 SSO 환경을 구현할 수 있게 합니다. SAML을 사용하면 고객의 자체 ID 및 액세스 관리(IAM) 솔루션과 Workday의 사이에서 끊김없는 SSO 경험을 구현할 수 있습니다.

Workday 기본 로그인

기본 로그인을 사용하려는 고객을 위해 Workday는 고객의 Workday 비밀번호를 그대로 저장하지 않고 보안 해시 형식으로만 저장합니다. 로그인 시도 실패와 성공한 로그인/로그아웃 활동은 감사를 위해 기록됩니다. 비활성 사용자 세션은 일정 시간이 지나면 자동으로 만료되는데, 이 시간은 고객이 구성할 수 있습니다. 고객이 구성할 수 있는 비밀번호 규칙에는 길이, 복잡성, 만료일이 포함됩니다.

다중 인증

Workday는 다중 인증(MFA)을 제공하며 고객에게 이 기능의 사용을 권장합니다. Workday에서는 고객이 TOTP(Time-Based One-Time Passcode) 알고리즘을 기반으로 한 인증 어플리케이션을 제공할 수 있습니다. 고객은 이 설정을 통해 MFA 제공자와 Workday 기본 로그인을 쉽게 통합할 수 있습니다. 또한 Workday는 이메일-SMS 게이트웨이 메커니즘을 통해 고객의 최종 사용자가 일회성 비밀번호를 받을 수 있게 합니다. 마지막으로, Workday는 사용자의 신원을 증명하는 추가 메커니즘으로 힌트 질문(challenge question)을 지원합니다.

신뢰할 수 있는 기기

Workday 고객과 최종 사용자는 Workday 테넌트 액세스에 사용할, 신뢰할 수 있는 기기를 등록할 수 있습니다. 최종 사용자는 미확인 기기에서 계정 액세스를 시도하면 알림을 받습니다. 신뢰하지 않는 기기는 제거할 수 있습니다. 관리자에게는 신뢰할 수 있는 기기의 목록이 모니터링 용도로 제공됩니다. 이 기능을 구성하려면, 관리자가 해당 테넌트에 대해 기능을 사용하도록 설정하고 최종 사용자가 브라우저 쿠키를 통한 기기 추적에 동의해야 합니다.

단계별 인증

Workday는 중요 리소스에 대한 액세스에는 더욱 강력한 인증 메커니즘인 단계별 인증을 제공합니다. SAML 인증 유형을 사용하는 곳이라면, Workday에서 중요 항목으로 분류된 리소스에 대한 무단 액세스를 더 확실하게 차단할 수 있습니다. 즉 고객이 2차 인증을 강제로 시행하여 사용자가 반드시 인증 정보를 입력해야 액세스가 가능해집니다.

권한 부여

Workday 어플리케이션은 권한 부여를 위해 그룹 정책 기반 보안을 적용합니다. 어떠한 사용자도 프로덕션 데이터베이스에 직접 액세스하지 못합니다. Workday가 제공하고 고객이 생성하는 시큐리티그룹과 사전 정의된 보안 정책을 연계하여 기능, 비즈니스 프로세스, 리포트, 데이터에 대한 사용자 액세스를 허가하거나 제한합니다. 이는 온라인 액세스 및 웹서비스를 통한 액세스에 모두 적용됩니다.

고객이 구성할 수 있는 시큐리티그룹은 사용자, 역할, 직무, 조직, 위치 계층, 사업장을 기준으로 합니다. 이 그룹은 다른 그룹을 논리적으로 포함하거나 제외하는 새로운 시큐리티그룹과 연계하여 사용할 수 있습니다. 시스템 대 시스템 액세스는 통합 시스템 시큐리티그룹에 의해 정의됩니다. 고객은 각자의 필요에 따라 이러한 그룹 및 정책을 맞춤 구성할 수 있습니다. 즉 필요한 만큼 세부적으로 액세스를 조정하여 글로벌 구현과 같은 복잡한 구성도 지원할 수 있습니다.

Workday는 채용, 계약 종료와 같은 비즈니스 프로세스를 기반으로 자동 업데이트되는 시큐리티그룹도 제공합니다. Workday가 제공하는 이 그룹은 독립적으로 사용하거나, 다른 Workday 제공 시큐리티그룹 또는 고객이 생성한 시큐리티그룹과 연계하여 사용하면서 보안 정책을 통해 액세스를 결정할 수 있습니다.

퍼블릭 클라우드

Workday는 AWS(Amazon Web Services) 퍼블릭 클라우드 서비스를 사용하여 Workday Media Cloud에 콘텐츠를 저장하고 처리합니다. 고객 콘텐츠는 다른 고객의 콘텐츠와 논리적으로 격리되며, 모든 Workday Media Cloud 콘텐츠는 저장될 때 AWS 서버 측 암호화를 사용하여 안전하게 암호화됩니다. Workday가 AWS에 저장하는 각 개체는 고유한 256비트 암호화 키를 사용하여 AES 암호화됩니다.

Workday는 AWS 클라우드에서 논리적으로 격리된 섹션인 Amazon VPC(Amazon Virtual Private Cloud)를 사용합니다. 최종 사용자와 Workday 데이터 센터 및 Workday Amazon VPC 서비스 간의 모든 통신은 전송 계층에서 암호화됩니다. 또한 Workday Amazon VPC 서비스와 Workday 데이터 센터의 모든 통신도 암호화됩니다. Workday는 TLS 프로토콜에 따라 보안 암호만을 사용하여 모든 트래픽을 암호화합니다.

상시 감사

Workday는 비즈니스 데이터에 대한 모든 변경사항을 어플리케이션 레벨에서 추적합니다. 이러한 어플리케이션 감사 정보는 Workday 시스템의 전반에서 제공되는 감사 및 규정 준수 리포트의 기반이 됩니다. Workday는 성공한 사용자 로그인/로그아웃 활동과 실패한 로그인 시도를 기록했다가 Workday 감사 리포트에서 이 정보를 제공합니다. Workday는 비파괴성 업데이트, 즉 데이터를 덮어쓰지 않고 테넌트 수명 주기 동안 유지하는 방법을 사용합니다. 그러면 고객은 모든 값에 대해 완전한 감사 이력을 확보할 수 있습니다. Workday 감사 기능은 감사자가 비즈니스 개체 또는 트랜잭션의 변경 이력을 추적하는 데 필요한 정보를 제공합니다.

Workday 소개

Workday는 기업의 HR 및 재무 관리를 위한 엔터프라이즈 클라우드 어플리케이션을 제공하는 선두 주자입니다.

2005년에 설립된 Workday의 재무 관리, HCM, 분석 어플리케이션은 세계 최대 규모의 기업, 교육 기관, 정부 기관을 효과적으로 지원할 수 있도록 설계되었습니다. 중견기업부터 포춘 50대 기업까지 다양한 조직에서 Workday를 선택했습니다.

워크데이 코리아 유한회사 | 서울특별시 강남구 영동대로 517, 30층(삼성동, 아셈타워)
수신자 부담 전화번호 080 822 1409 | www.workday.com/ko-kr