

클라우드에서의 Tableau Online 보안

목차

운영 보안.....	4
시스템 유지 관리.....	4
데이터 보안 및 개인 정보 보호.....	4
프라이버시 쉴드.....	4
백업 및 복구.....	5
재해 복구.....	5
데이터 거버넌스.....	5
사용자 및 데이터 원본 필터.....	6
사용자 보안.....	7
액세스 및 인증.....	7
역할 및 사용 권한.....	8
전송(네트워크) 보안.....	9
암호화.....	9
애플리케이션 보안.....	9
멀티 테넌트 아키텍처.....	10
관리 대시보드.....	10
결론.....	10

소개

데이터의 보안과 개인 정보 보호는 조직의 성공에 필수적입니다. 바로 이러한 이유로 Tableau는 이를 첫 번째 우선순위에 두고 있습니다. 이 백서는 Tableau가 Tableau Online에서 고객 데이터의 보안과 가용성을 위해 얼마나 노력하고 있는지 알려드리는 소개서입니다.

Tableau Online에 게시된 데이터는 다음과 같은 엔터프라이즈 보안 기능으로 보호됩니다.

- 물리적인 보안
- 운영 보안
- 데이터 보안 및 개인 정보 보호
- 계정 보안
- 전송 중인 데이터의 보안
- 애플리케이션 보안

이 모든 요소의 기반에는 가용성, 성능, 용량 및 보안을 지속적으로 모니터링하는 인프라가 있습니다. 이러한 모니터링의 결과는 데이터의 기밀성, 무결성 및 가용성을 지속적으로 보장하도록 개선하는 데 사용됩니다.

Tableau는 알려진 위험 요소 및 즉각적인 위협에 대해 광범위하고 효율적인 보호를 제공하도록 설계된 다중 보안 모델을 구현했습니다. Tableau의 사고 대응 프로토콜의 일부로서, 보안 위반은 Trust 웹 사이트 (<https://trust.tableausoftware.com>)를 통하여 보고되거나 문제가 발생한 고객에게 직접 보고될 것입니다. 사고 보고서에는 범위, 심각도 및 해결 방안이 포함됩니다.

Tableau는 고객 데이터가 안전하다고 확신할 수 있도록 세계적인 수준의 보안 호스팅 서비스를 제공하기 위해 최선을 다하고 있습니다.

운영 보안

SOC 2 및 ISAE 3402

매년, Tableau는 공인 회계 법인을 통해 Tableau Online에 대한 관리 목적 및 활동에 대한 심도 있는 감사를 수행합니다. Tableau는 Tableau Online 서비스에 대한 관리 절차가 SSAE 16(Statement on Standards for Attestation Engagements No. 16)과 ISAE(International Standard on Assurance Engagements) 3402에 의거하여 마련된 SOC 2 Type II 보고서에 의해 인증되었음을 알려드립니다. Tableau Online SSAE 16 보고서는 요청하면 받아보실 수 있습니다.

데이터 센터

Tableau Online 서비스는 모든 중요 서비스에 대해 중복성이 기본 제공되는, 독립적으로 감사가 진행되는 엔터프라이즈급 데이터 센터에서 호스팅됩니다. 데이터 센터에는 화재 진압 시설은 물론, 환경 문제를 감지하여 서비스가 정지되기 전에 대응하도록 설계된 추가 모니터링 시스템이 갖추어져 있습니다. 그뿐만 아니라, 호스팅 서비스 업체는 정전이 지속되는 상황에서도 운영을 보장하도록 관련 공급 업체와 계약을 맺고 있습니다.

기밀 유지 협약에 따라, Tableau는 요청 시에 데이터 센터 제공업체에 대한 감사 보고서를 공유할 수 있습니다. 자세한 내용은 Tableau 계정 담당자에게 문의하십시오.

시스템 유지 관리

Tableau Online 인프라를 유지 관리하는 전담 팀이 시스템 안정성, 보안, 성능을 보장하기 위해 정기적인 점검을 수행하며, 예정된 유지 관리 시간은 Tableau Trust 사이트에 최소 2일 전에 게시됩니다. 또한, 사이트 관리자는 예정된 작업에 대한 이메일 공지를 받으며, 사용자는 Tableau Online 사이트에 로그인할 때 공지를 보게 됩니다.

데이터 보안 및 개인 정보 보호

프라이버시 쉴드

Tableau는 EEA(유럽 경제 지역) 거주자와 관련된 개인 데이터에 대해 **프라이버시 쉴드 프레임워크**에 의거하여 인증된 **활발한 참여자**이며, 연방 무역 위원회 수사권 및 집행권의 적용을 받습니다.

백업 및 복구

백업을 구성하는 모든 요소는 중요하게 다뤄집니다. 백업 매체는 암호화되며, 항상 보안이 확실한 시설에서 유지 관리됩니다. 디스크 기반의 백업은 보안이 철저한 데이터 센터 시설에 저장됩니다. 외부 백업 제공 업체가 수행하는 백업은 암호화되어 전송 및 저장됩니다. 승인된 시스템 관리자만이 백업에 액세스할 수 있습니다.

Tableau Online 백업 정책에 따라 일별 백업은 31일 동안 보유됩니다.

이 백업을 통하여 Tableau는 Tableau Online 시스템 전체를 복원할 수 있습니다. 현재의 백업 방법으로 단일 고객 사이트의 복구는 가능하지 않습니다. 즉, Tableau는 시스템 오류가 아닌 다른 문제로 인한 개별 고객의 통합 문서 또는 데이터 손실을 복원할 수 없다는 뜻입니다.

재해 복구

Tableau Online 서비스의 각 인스턴스는 여러 지리적 위치에 있는 주 데이터 센터 및 백업 데이터 센터에서 운영됩니다. 주 데이터 센터의 서비스가 중지되면, 시스템은 백업 사이트로 전환되어 운영 서비스를 제공하도록 재구성됩니다. 그런 다음 데이터가 최근 백업에서 복구됩니다.

읽기 전용 애플리케이션인 Tableau Online은 통상 고객이 관리하는 데이터 원본에서 데이터를 가져오므로, 정보를 원본에서 직접 가져오거나 백업에서 복원하는 방식으로 비주얼라이제이션을 다시 게시하는 것이 가능합니다. 이를 통해 복구 목표 시간을 크게 줄일 수 있습니다.

데이터 거버넌스

데이터는 Tableau Online에 저장되어 있는 경우에도 고객이 소유하게 됩니다. 권한이 부여된 사람만이 사이트에 저장된 데이터 또는 통합 문서에 액세스하게 되며, Tableau 직원과 다른 고객은 고객 데이터에 액세스할 수 없습니다. 단, 서비스 운영을 담당하는 아주 소수의 신뢰할 수 있는 시스템 관리자는 데이터에 액세스할 수 있습니다. 액세스 권한 및 모든 관리자 권한에 대한 사용자 승인 절차는 분기별로 검토 및 승인되어 문서화됩니다.

한 가지 기억하실 점은 대부분의 고객 데이터가 자체 데이터 원본에 안전하게 저장된다는 것입니다. 단지 통합 문서, 데이터 추출 및 캐시된 데이터만 Tableau Online에 저장됩니다.

Tableau는 시스템 사용 정보, 계정 상태 및 성능 메트릭에 액세스하고 모니터링할 뿐입니다. 메트릭에는 다음과 같은 사항이 포함됩니다.

- 계정별 및 사용자별 저장공간 사용량
- 계정별 및 사용자별 대역폭 사용량
- 계정별 및 사용자별 통합 문서 및 뷰 수
- 사용자별 액세스(로그인) 날짜 및 시간
- 계정별 및 사용자별 데이터 원본의 수 및 유형(SQL Server, Salesforce.com 등)
- 계정별 및 사용자별 데이터 새로 고침 날짜 및 시간
- 사이트 성능 메트릭

Tableau Online에는 다음 4가지 방식 중 하나로 데이터가 입력됩니다.

1. 데이터가 포함된 통합 문서를 게시합니다.
2. 온프레미스 원본 데이터에서 Tableau 데이터 추출로 내보냅니다. 이 방식은 항상 실시간 연결이 아니라 데이터 추출을 만들기 때문에 가상 사설 통신망(VPN)이나 보안 터널을 구축할 필요가 없습니다. Tableau Online에서 직접 액세스할 수 없는 데이터 원본은 데이터 추출을 게시하여 Tableau Online 동기화 클라이언트를 통해 자동 새로 고침을 예약하면 됩니다.
3. 애플리케이션 프로그래밍 인터페이스(API)를 통해 웹 서비스에 연결합니다. Salesforce.com, Google Analytics 등 대부분의 클라우드 데이터 원본에는 API 연결을 통해 데이터 추출을 생성하고, 정기적으로 업데이트되도록 예약합니다.
4. 클라우드 플랫폼에 호스팅된 데이터에 직접 연결합니다. Tableau Online은 이러한 **데이터 원본**에 대해 실시간 라이브 연결이나 추출을 만들 수 있습니다.

사용자 및 데이터 원본 필터

통합 문서 및 데이터 원본에 사용자 및 데이터 원본 필터를 추가함으로써 추가적인 보안을 지정할 수 있습니다. 사용자 필터링은 게시된 뷰에서 누구나 볼 수 있는 데이터를 제한할 수 있는 특별한 유형의 필터입니다. 예를 들어, 지역 관리자들이 공유하는 매출 보고서에서 서부 관리자는 서부 매출만을, 동부 관리자는 동부 매출만을 볼 수 있게 하려고 합니다. 이런 경우에는 각 관리자마다 별도의 뷰를 만드는 대신, 각 관리자가 특정 지역의 데이터만 보도록 사용자 필터를 정의할 수 있습니다.

사용자 필터는 개별 필드에 정의됩니다. 사용자나 그룹에는 해당 필드에 있는 멤버의 하위 집합만 보도록 권한이 주어집니다. 위의 매출 보고서의 경우에는 사용자 필터가 지역 필드에 정의되고, 각 관리자에게 해당 지역을 보는 권한이 주어지는 것입니다.

데이터 원본 필터는 사용자 필터와 비슷한 방식으로 작동하는데, 전체에 적용되는 게시된 데이터 원본에 필터를 설정할 수 있게 해줍니다. 데이터 원본 필터는 통합 문서나 데이터 원본을 게시할 때 사용자가 볼 수 있는 데이터를 제한하는 데 유용하게 사용될 수 있습니다. 데이터 원본을 Tableau Online에 게시할 때, 데이터 원본 및 모든 관련 파일 또는 추출은 서버에 전송됩니다. 데이터 원본을 게시할 때, 데이터 원본의 다운로드나 수정에 대한 액세스 권한을 정의하고, Tableau Online을 통해 해당 데이터 원본에 원격으로 쿼리할 수 있는 사용자 및 그룹도 선택할 수 있습니다. 쿼리 권한만 부여하고 다운로드 권한은 부여하지 않는 경우, 계산된 필드, 별칭, 그룹, 집합 등을 포함하는 다양한 데이터 모델을 쿼리용으로만 공유할 수 있습니다.

게다가, 이 데이터 원본에 쿼리하는 사용자는 원래 게시된 데이터 원본에 있는 데이터 원본 필터를 보지도 수정하지도 못하며, 모든 사용자 쿼리에 이 데이터 원본 필터가 적용됩니다. 이는 사용자 데이터의 제한된 하위 집합에 액세스를 부여하는 좋은 방법입니다.

사용자 보안

액세스 및 인증

사이트에 명시적으로 추가된 사용자만 콘텐츠 및 통합 문서에 액세스할 수 있습니다. 지정된 관리자가 사용자 추가 및 삭제와 권한 지정을 포함하는 모든 계정 관리 기능에 대한 책임을 집니다. 계정 관리가 완벽하게 제어됩니다. 사이트 액세스가 더 이상 허용되지 않는 사용자가 있는 경우, 단순히 그 사용자 계정을 삭제하면 해당 사용자는 Tableau Online에 저장된 콘텐츠에 더 이상 액세스할 수 없게 됩니다.

Tableau Online에서 사용할 수 있는 인증에는 두 가지 방법이 있으며, 그 중 한 가지 또는 둘 다를 사용하도록 유연하게 사이트를 구성할 수 있습니다.

1. Tableau 계정

Tableau 계정이 기본으로 사용되며, Tableau가 관리하는 ID 저장소에 안전하게 저장됩니다. 이 방식의 인증을 통해 사이트 관리자는 별도의 ID 공급자와 통합할 필요 없이 사용자를 신속히 구성할 수 있습니다. 이 계정은 고객이 관리하며 보안 인증을 통해 Tableau Online에 연결됩니다. Tableau 계정은 또한 Tableau 웹 사이트, Tableau 고객/파트너 포털 및 Tableau 포럼과 같은 다른 Tableau 서비스 및 리소스에 액세스하는 데도 쓰입니다.

사용자는 사용자 ID(이메일 주소)와 사용자 선택 비밀번호를 통해 인증됩니다. 관리자가 사이트에 사용자를 추가하면, 비밀번호 설정 방법에 대한 안내가 포함된 이메일이 사용자에게 전송됩니다. 관리자는 사용자 암호를 설정하거나 저장된 암호를 검색할 수 없습니다. 암호는 강력한 해싱 알고리즘을 사용하여 보호됩니다.

10번의 잘못된 암호 시도가 있으면 10분 동안 계정이 잠기고, 계정이 연속해서 잠길 경우에는 잠김 시간이 배로 증가합니다. 사용자는 동시에 5개의 세션까지 열 수 있으며, 8시간이 지나면 시간 초과로 종료됩니다.

암호는 최소 8자로 이루어져야 하며 문자와 숫자를 포함해야 합니다.

2. SAML

SAML을 사용하면 관리자가 SAML 2.0 지원 ID 공급자(IdP)를 통해 사이트에 싱글 사인온(SSO) 기능을 구성할 수 있습니다. 자세한 내용은 [온라인 제품 가이드](#)의 사이트 인증 섹션을 참조하십시오.

참고: SAML 및 싱글 사인온(SSO) 관련 기능은 현재 요청 시에만 사용할 수 있습니다. 이 기능을 사용하시려면 Tableau 지원팀에 문의하십시오.

Tableau Online에서 2시간 동안 활동이 없는 세션은 자동 종료됩니다.

역할 및 사용 권한

Tableau Online 내의 액세스는 사이트 역할 및 사용 권한의 조합으로 제어됩니다. Tableau Online에 추가된 모든 사용자는 하나의 관련 사이트 역할을 갖게 됩니다. 사이트 역할은 관리자에 의해 지정되며, 사용자가 게시할 수 있는지, Tableau Online에 게시된 콘텐츠를 볼 수만 있는지 또는 상호 작용할 수 있는지 등을 포함하는 허용 권한 수준을 결정합니다. 사이트 역할에 대한 자세한 내용은 [여기에서 확인](#)할 수 있습니다. 사용 권한은 콘텐츠(프로젝트, 통합 문서, 뷰 및 데이터 원본)에 지정되며, 개별 사용자 또는 그룹에도 지정될 수 있습니다. 사용 권한을 지정할 때는 규칙에 따라 해당 콘텐츠로 작업할 수 있는 사용자를 지정합니다.

사용 권한은 작성, 보기, 수정 및 삭제와 같은 권한을 부여하는 데 사용됩니다. 프로젝트에 지정된

사용 권한은 그 프로젝트에 게시된 모든 통합 문서와 뷰의 기본 액세스 수준을 제어합니다. 또한 관리자는 '재무 사용자'와 같은 그룹을 만들어 사용 권한을 보다 용이하게 관리할 수 있습니다.



사용 권한 창

개체 보안 관리에 활용할 수 있는 매개 변수가 포함된 맞춤 설정은 20여 가지가 넘습니다. 자세한 내용은 온라인 문서의 [사용 권한 관리](#) 섹션을 참조하십시오.

전송(네트워크) 보안

암호화

클라이언트(Tableau Desktop 또는 지원되는 브라우저)와 Tableau Online 간의 모든 통신은 전송 중인 데이터를 보호하는 TLS를 사용하여 암호화됩니다.

데이터 원본 연결은 데이터 원본의 암호화 기능에 따라 암호화될 수도 안 될 수도 있습니다. 고객은 사용하려는 데이터 원본에 사용할 수 있는 암호화 옵션에 대해 잘 알고 있어야 합니다.

뿐만 아니라, Tableau 제품에는 스푸핑, 하이재킹 및 SQL 삽입 공격을 방지하는 다양한 보안 메커니즘이 내장되어 있습니다. Tableau는 또한 정기적인 업데이트마다 새로운 위협에 대비하기 위해 제품에 취약점은 없는지 적극적으로 테스트합니다.

구독 이메일과 같이 이메일을 사용하는 기능은 SMTP를 사용하여 전송되며, 이는 업계 표준에 따라 암호화되지 않음을 알려드립니다.

애플리케이션 보안

애플리케이션 보안은 보안 요구 사항, 위협 모델링, 코드 검토를 포함하는 보안 설계 사례와 보안 테스트가 조합되어 구현됩니다. 자동화 및 수동 취약성 테스트는 개발 프로세스의 일부로서 진행되며, 주 버전 출시에 앞서 애플리케이션 모의 해킹은 타사 보안 업체에서 시행합니다. Tableau는 타사 보안 전문가와 긴밀히 협력하여 보안 문제를 테스트, 발견, 검증 및 해결하기 위해 최선을 다하고 있습니다.

또한, Tableau는 외부 보안 업체의 취약성 검사 서비스를 구현하여 Tableau Online을 포함한 회사의 인터넷 관련 리소스 및 서비스를 지속적으로 검사하고 있습니다. 취약점이 발견되면 심각도와 영향을 평가하여 분류 기준에 따라 알림이 생성됩니다. 이 평가 결과에 따라 개선 우선순위가 정해집니다.

멀티 테넌트 아키텍처

멀티 테넌트 솔루션인 Tableau Online은 개별 고객에게 별도의 전용 환경을 제공하지 않습니다. 이 애플리케이션은 사용자, 데이터, 메타데이터를 사이트별로 논리적으로 분할함으로써 고객 영역을 분리합니다. 서비스에 업로드되거나 링크된 모든 데이터는 해당 데이터 소유 고객에게 프로그래밍 방식으로 연결되며, 이러한 제어 방식으로 한 고객이 다른 고객의 데이터에 액세스할 수 없게 됩니다.

관리 대시보드

Tableau Online은 고객 사이트에 대한 사용 통계를 제공하는 다양한 기본 대시보드를 게시합니다. 제공되는 통계 정보에는 사용자 활동, 뷰 수 및 데이터 원본 사용이 포함됩니다. 관리자는 이러한 기본 대시보드를 사용하여 사이트가 어떻게 이용되는지 알아볼 수 있습니다.

이러한 대시보드 사용에 대한 자세한 내용은 온라인 제품 가이드의 [관리 뷰](#) 섹션을 참조하십시오.

결론

Tableau Online 서비스는 업계 모범 사례에 따라 구축되고 타사 보안 전문가가 검증한 강력한 보안 모델에 기반하여 운영되고 있습니다. Tableau는 고객의 데이터가 얼마나 중요한지 잘 알고 있으며, 이를 보호하기 위해 최선을 다하고 있습니다.

Tableau 정보

Tableau를 사용하면 데이터를 비즈니스를 개선할 수 있는 실행 가능한 인사이트로 전환할 수 있습니다. 데이터가 저장된 위치나 형식에 상관없이 손쉽게 연결하고, 애드혹 분석을 빠르게 수행하여 숨겨진 기회를 발견하게 됩니다. 드래그 앤 드롭으로 고급 시각적 분석 기능을 갖춘 대화형 대시보드를 작성하여 조직 전체에서 공유하고, 팀원들이 데이터에 대한 고유한 관점을 탐색하도록 도와줍니다. 글로벌 기업부터 신생 기업 및 소규모 비즈니스에 이르기까지 전 세계 모든 사람들이 Tableau의 분석 플랫폼을 사용하여 데이터를 보고 이해하고 있습니다.

리소스

[무료 평가판 다운로드](#)

[클라우드에서의 비즈니스 분석 사용 이유](#)

[효율적인 캠페인 대시보드 생성을 위한 5가지 우수 사례](#)

[모든 백서 보기](#)

