Tencent Real-Time Communication

Service Level Agreement

제품 문서

목록:

Service Level Agreement
컴플라이언스 인증

최종 업데이트 날짜: : 2022-07-11 12:08:52

컴플라이언스는 Tencent Cloud TRTC 개발의 기초입니다. TRTC은 제공되는 서비스의 **안전성, 합법성, 가용성, 보안성** 및 **프라이버시를 보장**하며, 여러 국가 및 산업의 컴플라이언스 요구 사항을 준수합니다. 또한 TRTC 사용 고객에게 관련 지원을 제공하여 **기업 및 기업 고객의 여러 규정 준수 및 모니터링 요구 사항을 충족하고, 기업 및 기업 고객의 감사 작업에 대한 반복적 비용을 줄여 감사 및 관리 효율성을 향상시킵니다.**

TRTC는 SOC 감사 보고서(SOC 1, SOC 2, SOC 3 포함), 정보 보안 등급 보호 규정 2.0, ISO 인증 (ISO 9001, ISO 20000, ISO27001, ISO27017, ISO27018, ISO27701, ISO29151 포함), CSA STAR, NIST CSF, BS10012 및 K-ISMS 인증을 통과했습니다.

SOC 1 Type II 리포트

AICPA 감사 표준 SSAE No. 18의 AT-C section 320 을 참고하여 Tencent Cloud 클라우드 서비스 시스템의 제어 환경에 대해 제출한 리포트

SOC 2 Type II 리포트

AICPA 감사 표준 SSAE No. 18의 AT-C section 205 및 TSP section 100 2017 버전을 참고하여 클라우드 서비스 시스템의 보안성, 가용성 및 기밀성에 대해 제출한 리포트

SOC 3 Type II 리포트

Tencent Cloud 서비스 시스템의 보안성, 가용성 및 기밀성을 설명하는 일반 사용 리포트이며 AICPA SSAE No. 18의 AT-C section 205 및 TSP section 100(2017 버전)에 따라 수행

정보 보안 등급 보호 규정(Multi-Level Protection Scheme, MLPS) 2.0

Tencent의 핀테크 솔루션은 레벨 4 보호에 등록되어 있고, 퍼블릭 클라우드 서비스는 레벨 3 보호에 등록되어 있습니다

ISO 9001 품질 관리 시스템 인증

Tencent Cloud는 클라우드 컴퓨팅 분야에서 최초로 ISO 9001 CNAS 및 ANAB 인증을 획득한 중국 클라우드 컴퓨팅 서비스 제공 업체로서 효과적인 품질 관리 프로세스 딜리버리를 구현하여 고품질 클라우드 서비스를

ISO 20000 IT 서비스 관리 시스템 인증

Tencent Cloud는 최초로 ISO 20000-1:2018 표준 인증의 새 버전을 통과한 중국 클라우드 컴퓨팅 서비스 제공 업체이며 표준 IT 서비스 관리 프로세스를 수립하고 엄격하게 구현합니다.

ISO 27001 정보 보안 관리 시스템 인증

ISO/IEC 27001:2015는 ISO/IEC 27002:2013를 보완합니다. Tencent Cloud는 ISO 27001 지침 인증서를 통과하였으며, 이는 Tencent Cloud가 클라우드 컴퓨팅 정보 보안 제어의 효과적인 설계 및 구현을 실행했음을

클라우드 서비스의 정보 보안 제어를 위한 ISO 27017 구현 가이드

ISO/IEC 27017:2015는 ISO/IEC 27002:2013을 보완합니다. Tencent Cloud는 ISO 27017 지침 인증서를 통과하였으며, 이는 Tencent Cloud가 클라우드 컴퓨팅 정보 보안 제어의 효과적인 설계 및 구현을 실행했음을

ISO 27018 퍼블릭 클라우드 개인 정보 보호 인증

Tencent Cloud는 각 고객의 개인 정보를 보호하고 완전한 개인 정보 관리 시스템을 구축하며 다양한 기술적 수단을 사용하여 사용자의 개인 정보를 보호하기 위해 최선을 다하고 있습니다.

개인 정보 관리 시스템에 대한 ISO 27701 국제 표준

Tencent Cloud는 ISO/IEC 27701 인증을 통과한 세계 최초의 클라우드 서비스 제공 업체이며 개인 정보 관리 시스템을 구축 및 구현했으며 지속적으로 개선할 수 있는 능력을 갖추고 있습니다.

개인 식별 정보 보호를 위한 ISO 29151 가이드

Tencent Cloud는 개인 식별 정보 보호를 위한 적절한 정보 보안 리스크 관리 환경을 제공하는 동시에 업계 베스트 프랙티스를 충족하고 지속적으로 개선할 수 있는 능력을 갖추고 있습니다.

CSA STAR 클라우드 보안 관리 시스템 인증

CSA STAR는 클라우드 보안 특성에 대한 국제 인증입니다. Tencent Cloud는 STAR 인증을 골드 레벨로 통과하여 클라우드 보안 기술 관리 및 제어를 강화했습니다.

NIST 네트워크 보안 프레임워크

NIST CSF는 미국 국립 표준 기술 연구소에서 행정 명령(EO) 13636 '핵심 인프라 네트워크 보안 개선'에 따라 개발되었으며, 이 프레임워크는 비즈니스 주도형 네트워크 보안 이벤트 가이드에 중점을 두고 있습니다.

KISMS 인증

Tencent Cloud는 중국에서 최초로 KISMS 인증을 통과한 클라우드 컴퓨팅 서비스 제공 업체로서 Tencent Cloud가 구축한 정보 보안 관리 시스템 및 기능이 관련 한국 법률 및 표준의 컴플라이언스 요구 사항을 충족

BS 10012

British Standards Institute에서 발행한 개인 정보 관리 시스템 표준

보안 백서

최종 업데이트 날짜: : 2023-03-13 14:48:16

1. 개요

TRTC(Tencent Real-Time Communication)는 네트워크 및 오디오/비디오 기술에 대한 Tencent의 다년간의 경험을 활용하여 그룹 오디오/비디오 통화 및 저지연 인터랙티브 라이브 스트리밍 솔루션을 위한 통합되고 표준화된 API(Application Programming Interface)를 제공합니다. 또한 다양한 산업 및 시나리오를 위해 메인스트림 운영 체제 및 플랫폼과 호환되는 SDK(Software Development Kit) 솔루션을 제공합니다. TRTC를 사용하면 저비용, 저지연, 고품질 인터랙티브 오디오/비디오 솔루션을 빠르게 구축할 수 있습니다.
실시간 오디오/비디오 PaaS 클라우드 서비스의 업계 리더인 TRTC는 데이터 및 사용자 개인 정보 보안을 매우 중요하게 생각합니다. TRTC는 항상 데이터 및 사용자 개인 정보 보호에 최우선 순위를 두고 이를 일상적인 보안 기능 개발에 통합합니다. TRTC의 보안 보호 기능에 대한 이해를 돕기 위해 TRTC PaaS 서비스의 보안 개발 및 보안 컴플라이언스 감사에 대해 설명합니다.

2. 보안 컴플라이언스 및 개인 정보 보호

보안 컴플라이언스는 다양한 국가 및 산업의 컴플라이언스 요구 사항을 충족하는 TRTC 개발의 기초입니다. TRTC는 제공하는 서비스의 보안, 컴플라이언스, 가용성, 보안성 및 개인 정보 보호를 보장하는 것 외에도 귀사와 귀사 고객의 컴플라이언스 요구 사항을 충족하고, 감사 작업에 대한 중복 투자를 줄이고, 감사 및 관리 효율성을 개선할 수 있도록 관련 지원을 제공합니다.
TRTC는 SOC 1, SOC 2 및 SOC 3 감사를 통과했으며 중국의 사이버 보안 등급 보호 2.0 요구 사항을 충족하고 ISO 9001, ISO 20000, ISO27001, ISO27017, ISO27018, ISO27701, ISO29151, CSA STAR, NIST CSF, BS10012 및 K-ISMS 인증을 받았습니다.

보안 컴플라이언스 및 개인 정보 보호	설명
ISO/IEC 27001: 2013 정보 보안 관리 표준	ISO/IEC 27001: 2013은 국제적으로 인정된 정보 보안 관리 시스템에 대한 기본 인증을 받았으며, 이는 보안에 대한 기업의 노력을 나타내고, 기업 정보 보안 관리 시스템을 보유하고 있으며, 신뢰할 수 있는 정보 서비스를 제공할 수 있음 입증합
ISO/IEC 27017: 2015 클라우드 서비스 제공 및 사용에 적용되는 정보 보안 제어 가이드	ISO/IEC 27017: 2015는 클라우드 서비스 공급자 및 고객을 위한 특정 보안 제어 서비스의 정보 보안을 위한 실용적인 표준입니다. ISO 27017은 ISO 27002의 보 위한 클라우드 기반 개발, 운영 및 보안 규범을 제공하도록 설계되었습니다. TRT 한 정보 보안 관리 및 보호 기능을 입증하였습니다.
	ISO/IEC 27018: 2019는 퍼블릭 클라우드 개인 식별 정보 보호를 위한 실행 규범을 기반으로 퍼블릭 클라우드에서 개인 식별 정보 보호에 적용할 수 있는 보완 지

	위한 퍼블릭 클라우드 기능을 강화합니다. TRTC는 ISO 27018 인증을 통과했으 산, 문서 및 클라우드 IT 시스템의 보안을 보호하는 업계 모범 사례의 높은 표준에
CSA STAR 인증	국제 비영리단체인 CSA(Cloud Security Alliance)의 CCM(Cloud Control Matrix)를 Trust Assurance and Risk)는 클라우드 컴퓨팅 공급업체가 클라우드 컴퓨팅 보안 증하는 글로벌 클라우드 컴퓨팅 보안 인증입니다. 정보 보안 관리 시스템에 대한 라우드 보안 문제를 시각화하고 클라우드 벤더가 보안 관리 기능을 평가할 수 있 TRTC는 클라우드 서비스 보호 기능을 입증하는 CSA STAR 인증을 받았습니다
SOC 감사	SOC 리포트(System and Organization Controls Reports)는 AICPA(American Ins 해당 지침에 따라 전문적인 제 3자 회계 법인이 발행하는 서비스 조직의 내부 통 선도적인 클라우드 서비스 공급자인 Tencent Cloud는 2017년 SOC 감사에서 20 하여 2017년 버전을 따르는 중국 최초의 공급자가 되었습니다. 서비스 인증 보고 립하고 구현했으며 인증 보고서의 요구 사항을 준수하는지 확인하기 위해 정기적 증합니다.
사이버 보안 분류 보호 인증	CCP 2.0(Cybersecurity Classified Protection 2.0)은 2019년 12월 1일부터 시행되 아니라 보안 및 신뢰성, 동적 인식, 수동적 보호에서 이벤트 전, 중간 및 이벤트 후 사에 중점을 두고 있으며, 기존 정보 시스템, 기본 정보 네트워크, 클라우드 컴퓨 업 제어 시스템들을 완벽하게 다룹니다. CCP 2.0 및 해당 규정에 따라 Tencent C 비스 플랫폼은 CCP 레벨 3 컴플라이언스에 대해 등록 및 평가되었으며, 이는 클 니스에 종사하는 기업 사용자에게 CCP 컴플라이언스에 필요한 서비스를 제공한

3. 데이터 보안

데이터 보안은 TRTC의 주요 관심사 중 하나입니다. TRTC는 데이터 보안을 보장하기 위해 필요에 따라 합법적이고 규정을 준수하는 방식으로 데이터를 처리합니다. 이 섹션에서는 Tencent Cloud 및 TRTC의 데이터 보안 기술 제어 및 관리 정책에 대해 설명합니다.

3.1 데이터 보안 정책

TRTC는 데이터 보안 개발을 위한 전제 조건으로 기밀성, 무결성 및 고가용성에 중점을 두고 데이터 보안 관리 구축을 오디오/비디오 PaaS 서비스 구축 과정에 통합합니다. Tencent Cloud는 항상 다음과 같이 데이터의 가용성, 기밀성 및 무결성을 보장하기 위해 최선을 다할 것입니다.

가용성: Tencent Cloud의 사설망 전송 프로토콜을 통해 데이터의 고가용성을 보장합니다.

기밀성: 무단 액세스 및 도청을 방지합니다.

무결성: 데이터의 무결성을 보장하고 데이터가 위조되지 않도록 보호합니다.

TRTC는 모든 직원에게 데이터 보안, 개인 정보 컴플라이언스 및 데이터 암호화 보호에 대한 정기적인 교육을 제공하고 직원과 기밀 유지 계약을 체결하여 일상 운영 중의 데이터 가용성, 기밀성 및 무결성을 보장합니다.

3.2 높은 데이터 가용성

TRTC는 가용성이 높은 오디오/비디오 PaaS 데이터 서비스를 제공하기 위해 노력합니다.

전 세계적으로 분산된 IDC: TRTC에는 전 세계적으로 서비스를 제공하는 많은 IDC가 있습니다. 하나의 IDC에 대한 공격은 다른 IDC 또는 전체 서비스에 영향을 미칠 수 없으므로 격리 기반 보호를 구현합니다.
장애 격리 및 복구: IDC가 서비스 거부(DoS) 공격과 같이 방지하기 어려운 악의적인 공격을 받는 경우 TRTC는 장애가 있는 서버를 합리적으로 처리하여 전반적인 서비스 안정성과 가용성을 보장합니다.
DDoS 공격 방어: TRTC는 각 IDC에 DDoS 방지 방화벽을 배포했으며 DDoS 공격의 위험을 제어할 수 있는 충분한 기능과 리소스를 갖추고 있습니다.

3.3 데이터 수집

TRTC는 사용자의 동의가 있는 데이터 필드와 서비스에 필요한 데이터 필드만 최소한의 단위로 수집합니다. 애플리케이션 로그인 정보, ID, 비밀번호, 결제 정보, 이름 및 주소와 같이 개발자가 수집한 사용자 데이터는 TRTC 플랫폼이 아닌 개발자가 보관합니다.

3.4 데이터 마스킹

데이터 프라이버시를 보호하기 위해 TRTC는 콘솔의 기업 및 개인 정보를 마스킹한 후 표시합니다. 이 정책은 내부 관리 플랫폼, 로그 인쇄, 모니터링 및 알람 채널과 같은 TRTC의 내부 시스템 및 기타 제품에도 적용됩니다.

3.5 데이터 사용 및 저장

데이터의 컴플라이언스 및 보안을 보장하기 위해 개인 또는 기업 사용자 데이터, 최종 사용자 데이터, 음성/영상 통화 데이터, 시스템 운영 및 보안 데이터는 분류된 후에 저장됩니다.
개발, 테스트 및 프로덕션 환경은 TRTC 개발 중에 엄격하게 격리되어 실제 데이터가 개발 및 테스트에 직접 사용되지 않도록 합니다. 또한 비밀번호와 같은 개발자와 사용자의 기밀 정보는 암호화되어 저장됩니다.
온프레미스 서버의 녹화 SDK와 TRTC에서 제공하는 온클라우드 녹화 기능을 사용하는 개발자 및 사용자는 통화 내용의 전체 또는 일부를 녹화/녹음할 수 있으며, 모든 녹화본은 TRTC 서버가 아닌 개발자와 사용자가 제공하는 스토리지 서버에 직접 기록되어 저장됩니다.

4. TRTC PaaS 서비스 보안

저지연 고품질의 실시간 인터랙션 솔루션의 TRTC에 대한 요구 사항은 매우 까다롭습니다. TRTC 오디오/비디오 PaaS 서비스를 개발하는 과정에서 TRTC는 아키텍처에 대한 기술 및 보안 위험을 충분히 평가하고, 컴플라이언스 표준의 보안 위험 제어 시스템을 최대한 준수하며, 오디오/비디오 PaaS 서비스 개발 전반에 걸쳐 이를 구현하여 개발자 및 사용자를 위한 고품질의 안정적이고 안전한 오디오/비디오 PaaS 솔루션 세트를 제공합니다.

4.1 TRTC 전송 네트워크 보안

TRTC는 Tencent Cloud 프라이빗 전송 네트워크를 기반으로 초저지연, 고품질 전송을 특징으로 하고 수백만 명의 사용자 규모의 실시간 인터랙션을 지원하는 오디오/비디오 플랫폼을 개발했습니다. 프라이빗 전송 네트워크는 핵심 TRTC PaaS 서비스 중 하나입니다. TRTC 터미널에서 신호 연결, 인증, 실시간 스케줄링 및 오디오/비디오 데이터 실시간 전송을 위해 안전하고 규정을 준수하는 서비스 지원을 제공합니다. 또한 개발자와 사용자에게 안전하고 안정적

인 서비스를 제공하기 위해 현재 인터넷 환경이 직면한 보안 요소를 고려하여 Tencent Cloud 프라이빗 전송 네트워크의 아키텍처 설계는 다음 제어를 통합합니다.

전송 네트워크 보안 제어	설명
암호화 전송	TRTC는 전송 중 오디오/비디오 데이터의 기밀성을 보장하기 위해 전송 연결을 위한 제공합니다. 내장 암호화는 TRTC PaaS에 기본적으로 전역적으로 활성화되어 있으 터 전송의 암호화 보안을 보장합니다.
리소스 격리	TRTC는 각 TRTC 애플리케이션(SdkAppId)에 전용 리소스를 할당하여 다른 프로젝 소스의 안전하고 안정적인 보장을 제공합니다. 개발자와 사용자는 TRTC 콘솔에 등 업만 수행하면 TRTC 애플리케이션(SdkAppId)을 만들고 해당 리소스를 할당할 수
방 격리	TRTC는 각 유형의 오디오, 비디오 또는 메시지 데이터 전송을 위해 독립적인 격리 논리적으로 분리되어 있으며 사용자가 동일한 SdkAppid 및 동일한 방 이름으로 TR 사용자가 동일한 채널에 참여할 수 있습니다. 방은 세션이 시작되면 생성되고 세션이 종료됩니다. 이러한 방식으로 전송 격리가 방 레벨에서 구현됩니다.
실명 인증	사용자가 TRTC 애플리케이션을 사용하고 TRTC PaaS 서비스에 연결하면, TRTC는 증 정보를 사용하여 방 입장에 대한 인증을 수행하여 개발자와 사용자가 강력한 인증 와줍니다.

4.2 TRTC SDK 보안

TRTC는 필요에 따라 통합을 위해 iOS, Android, macOS, Windows, Web 및 미니 프로그램과 같은 다양한 플랫폼용 SDK를 제공합니다. 개발자와 사용자가 쉽게 통합할 수 있는 간단하고 안전하며 안정적인 오디오/비디오 SDK를 제공합니다.
TRTC는 개발자와 사용자의 데이터 및 정보 관련 컴플라이언스 및 보안 위협 대처 업무량을 줄이기 위해 규정을 준수하고 안전한 오디오/비디오 PaaS 서비스를 만들기 위해 최선을 다합니다.

SDK 보안 지원	설명
SDK 보안 및 컴플라이언스	TRTC SDK의 신뢰성과 보안은 TRTC 기능을 보장하는 기반 중 하나입니다. 의 컴플라이언스와 개인 정보 및 보안 위험 측면에서 기능 요구 사항의 합리성 개인 정보 보호 정책을 준수하도록 합니다. 기능 구현 중에 TRTC는 적절하고 필요한 품질 보안 테스트를 수행하고 타사 나 통합하는 보안 검사, 특히 컴플라이언스 확인을 수행합니다.
SDK 콘텐츠 암호화	TRTC SDK는 AES 128 대칭 키를 사용하여 데이터 수준에서 모든 오디오/비 할 수 있습니다. 암호화된 데이터는 Tencent Cloud 프라이빗 전송 프로토콜을 종적으로 수신 터미널에서 해독되어 렌더링됩니다. 전송 중 데이터 보안 및
개발자에 대한 SDK 보안 및 컴플라이언스의 이점	TRTC는 개발자를 위해 안전하고 합법적인 고품질 오디오/비디오 PaaS 서비 습니다. TRTC SDK에는 보안 암호화가 내장되어 있어 개발자와 사용자가 TR 이언스를 개선하고 고객의 보안 및 개인 정보 보호 요구 사항을 최대한 충족하 합니다.

4.3 TRTC 기본 컴퓨팅 리소스 보안

TRTC의 기본 컴퓨팅 리소스는 전 세계에 배포된 100개 이상의 분산 IDC와 Tencent Cloud CVM 인스턴스로 구성되어 TRTC의 기본 컴퓨팅 리소스 환경의 높은 확장성, 보안 및 가용성을 보장합니다.

컴퓨팅 리소스 보안	설명
IDC 장치 보안 관리	TRTC는 IDC에서 장치의 일상적인 관리를 위한 완전한 관리 규범을 제정했습니다 인 점검, 예외 모니터링 및 리포팅, IDC의 전력 리소스 지원에 완전히 반영되고 TR 개발 요구 사항을 충족하는 세부 관리 조치 및 서비스 구현 표준을 정의합니다.
서버, 데이터베이스, 미들웨어 등 컴퓨팅 리소스 보안	CPU, 메모리, 디스크 등 TRTC 운영에 필요한 리소스는 비즈니스 부하에 따라 합 TRTC는 실제 보안 운영에서 적절한 보안 기준 및 취약성 관리 지침을 개발하고 실 시나리오에서 기본 컴퓨팅 리소스의 부하 보안을 완벽하게 보장합니다.
DDoS 공격 방어	TRTC PaaS 서비스의 시스템 및 비즈니스 가용성에 대한 DDoS 공격의 중대한 영 Cloud 퍼블릭 클라우드 기능을 활용하여 핵심 서비스에 DDoS 공격 방지 스키마를 크 및 전송 레이어의 DDoS 공격을 실시간으로 탐지하고 방어할 수 있습니다. 실시 고, 공격이 감지되는 즉시 트래픽을 정리하고, TRTC를 몇 초 안에 보호할 수 있습

4.4 Web API 보안

개발자가 자신의 오디오/비디오 비즈니스를 효율적으로 개발하고 관리하기 쉽도록 TRTC는 개발자가 호출할 수 있는 RESTful API의 형태로 콘솔의 일부 기능을 제공합니다. RESTful API는 다음과 같은 보안 보장을 제공합니다.

보안 보호	설명
인증	TRTC RESTful API를 사용하기 전에 개발자는 먼저 Tencent Cloud 콘솔에 로그인하고 전용 Se 공급자 ID의 고유성을 보장해야 합니다.
입력 확인	개발자 요청 매개변수의 유효성은 TRTC 서버 백엔드에서 확인되어 유효하지 않은 매개변수를 방지합니다.
전송 보안	RESTful API는 SSL / TLS를 사용한 모든 API 통신의 암호화를 보장하기 위해 HTTPS 프로토콜 전송된 데이터를 보호하는 데 도움이 됩니다.
API 속도 제한	서버의 API 요청 속도에 제한이 있어 정상적인 사용자 요청에 대한 응답을 보장하면서 악의적인

5. 보안 운영

합리적인 보안 운영 정책을 고수하는 것은 TRTC의 고객 보안, 적법성 및 컴플라이언스 보장의 기반입니다. 비즈니스 특성에 따라 TRTC는 다음과 같은 방법으로 비즈니스 운영 보안을 보장합니다.

5.1 보안 비상 대응 메커니즘

TRTC는 자체 오디오/비디오 PaaS 비즈니스 특성을 기반으로, 다양한 보안 이벤트를 분류하는 기준을 개발하고 서비스를 분류하며, 보안 및 위협 레벨을 체계적으로 평가하여 완전하고 효율적인 프로세스에 따라 보안 예외 사항을 신속하고 효율적으로 처리합니다.
간단히 말해서, TRTC는 기능 보안 예외를 다음과 같이 처리합니다.

5.2 비즈니스 연속성 관리

저지연 고품질의 오디오/비디오 서비스를 개발자와 사용자에게 7×24시간 제공하기 위해, 전문적이고 효율적인 TRTC 개발 및 운영 팀이 오디오/비디오 서비스의 가용성 지원 및 관리를 담당합니다.

비상 대응 메커니즘	설명
비즈니스 모니터링 및 알람	TRTC는 비즈니스 서비스 및 시스템 운영 상태를 모니터링하기 위해 7×24시간 효 습니다. 애플리케이션, 미들웨어, 컴퓨팅 부하, 데이터베이스 및 네트워크 장치와 컴포넌트의 실행 상태 및 리소스 부하와 같은 메트릭에 대한 이벤트 모니터링 및 링 툴의 완전한 세트를 설정했습니다. 또한 봇을 활용하여 문제를 담당 직원에게 비스 복구 및 가용성을 보장할 수 있습니다.
재해 복구 및 중복성	TRTC는 다양한 극단적인 비즈니스 시나리오를 위한 인프라 레이어, 컴퓨팅 부하 재해 복구 보안을 고려하여 핵심 IDC의 중복 아키텍처 개발을 위한 솔루션을 개발 우드 서버는 예상치 못한 상황에서 TRTC의 기본 리소스 가용성을 추가로 보장하
연속성 시뮬레이션	TRTC는 중요한 비즈니스 시스템의 지속적이고 효율적인 운영을 보호하고 지속적 트워크, 미들웨어, 비즈니스 시스템에 대한 보안 비상 재해 복구 훈련을 정기적으 기반으로 검토를 수행하며, 기술 아키텍처, 운영 관리 프로세스 및 비상 계획을 개

5.3 보안 모니터링 및 침입 방지

TRTC 보안 팀은 PaaS 서비스에 대한 위협에 대처하기 위해, 심층 방어 구현 측면에서 보안 로그 분석을 위한 최소 권한 원칙에 따라 로그를 수집합니다. 기업에서 매일 생성되는 로그 데이터를 기반으로 식별된 보안 예외 사항에 대해 즉각적인 알람이 전송되며, 보안 운영 담당자는 연관성 및 추적 가능성 분석 검토를 추가로 수행합니다. 검증된 잠재적 위험은 비즈니스 시스템의 보안 및 안정성을 보장하기 위해 TRTC의 비상 대응 메커니즘에 의해 처리 및 추적됩니다.

6. 직원 보안

TRTC는 직원 관리 관점에서 일상적인 운영 및 관리 과정에서 데이터 및 정보 보안 원칙을 엄격히 준수합니다. TRTC는 전체 보안에 대한 직원 보안의 중요성을 충분히 인식하여, 채용, 입사, 교육 및 사직 프로세스에서 직원의 직업 윤

리 및 기본 자질이 Tencent Cloud의 가치관에 부합하고 보안 컴플라이언스 요구 사항 및 비즈니스 요구 사항을 충족하는지 충분히 고려합니다.

프로세스	설명
채용	직원 채용 프로세스의 초기 단계에서 TRTC는 전문 인사 전문가를 지정하여 지원자의 교육 및 업무
입사	신입 직원은 Tencent Cloud의 보안 컴플라이언스 인식 요구 사항을 충족하기 위해 직원 보안 정책을 한 각 직원과 적절한 수준의 기밀 유지 계약을 체결합니다. 중요한 데이터에 접근할 수 있는 위치에 참여하기 전에 보안 컴플라이언스 정책에 대한 엄격한 규범 학습을 완료하고 시험에 합격해야 합니
재직	직원은 정기적으로 보안 및 개인 정보 보호 교육에 참석하고 필수 시험에 합격해야 합니다. 또한 TR 동을 비정기적으로 진행하여 직원의 보안 의식을 지속적으로 고취하고 있습니다.
사직	직원은 팀을 떠나기 전에 설정된 사직 프로세스에 따라 인계를 완료한 후에 액세스 권한을 비활성화 시된 사전 통지 기간 동안 성과를 감사하고 직원에게 사직 후 정보 보안 및 기밀 유지 책임을 알립니 승인을 거쳐 사직할 수 있습니다.

7. 보안 책임 분담

TRTC는 실시간 인터랙티브 오디오/비디오 PaaS 클라우드 서비스 플랫폼으로서 플랫폼 및 SDK의 보안을 관리합니다. 서비스에 연결하는 개발자는 자신의 애플리케이션 및 시스템 환경의 보안을 관리하고 필요에 따라 TRTC의 보안 관리 기능을 합리적으로 사용하여 정보, 플랫폼, 시스템 및 네트워크를 보호해야 합니다.

8. 요약

고객에게 안전하고 규정을 준수하며 안정적인 오디오/비디오 PaaS 서비스를 제공하는 것은 TRTC의 주요 관심사 중 하나입니다. 정보 보안 계획의 구현을 체계적으로 추진하고, 규제 컴플라이언스 의무를 수행하며, 계획을 일상 업무 중에 제품 및 서비스 개발 지침으로 사용합니다. 또한 TRTC는 보다 효율적이고 안전하며 자동화된 보안 보호 조치를 구현하기 위해 새로운 기술을 적극적으로 연구합니다.
TRTC PaaS 서비스의 지속적인 고가용성을 보장하고 최종 사용자의 정당한 권리와 이익을 보호하기 위해, TRTC는 앞으로도 최선을 다해 안전하고 규정을 준수하는 실시간 인터랙티브 오디오/비디오 서비스를 만들어 나갈 것입니다.

정보 보안에 관한 참고 사항

최종 업데이트 날짜: : 2023-03-13 14:49:28

이 문서에 대해 다음과 같이 성명합니다.

1. 본문은 Tencent Real-Time Communication(TRTC)에 대한 Tencent Cloud의 보안 조치에 대한 개요를 제공하기 위한 것입니다. 정보 관리 방법과 고객과 최종 사용자 데이터의 보안을 보호하는 방법에 대해 설명합니다. 필수 요구 사항이 있는 경우 Tencent Cloud와 서비스 수준 계약(SLA)을 체결하는 것이 좋습니다. Tencent Cloud는 이 문서의 내용에 대한 어떠한 명시적 또는 묵시적 약속 및 보증도 부인합니다.
2. 본문은 광범위한 보안 기능 중 기술적 보안 기능의 '일부'만 포함합니다.
3. 본문은 국가 또는 산업별 정보 보안 표준 또는 요구 사항에 대한 참조 문서가 아닙니다.
4. 본문은 가독성을 위해 수정되었습니다. 모호하거나 부정확한 경우 제 1항목을 참조하십시오.
5. 이 문서의 해석 권한은 Tencent Cloud에게 있습니다.

1. 개요

Tencent Cloud TRTC는 다음 인증을 취득하였으며, 다음 인증의 보안 요구 사항을 충족합니다:
ISO 9001 인증
ISO 20000 인증
ISO 27001 인증
ISO 27017 인증
CSA STAR 인증
GDPR
자세한 내용은 컴플라이언스를 참고하십시오

2. 정보 보안 보호

TRTC의 관리 보안 및 기술 보안 요구 사항은 일반 데이터 보호 규정(GDPR)을 준수합니다.

2.1 정보 및 데이터 보안

사용자와 TRTC 서버 간의 통신은 Tencent Cloud의 개인 전송 프로토콜, TLS(전송 계층 보안) 및 WSS(Web Socket Secure)와 같은 프로토콜로 보호됩니다. 전송하는 동안 TRTC에는 전송된 정보를 해독할 수 있는 키가 없습니다. 통

화 내용은 터미널 장치(예: 클라이언트 app 또는 온프레미스 녹음 서버)의 인증 키로만 해독할 수 있습니다.

2.2 데이터 가용성

수많은 IDC: TRTC에는 전 세계적인 서비스를 제공하는 많은 IDC가 있습니다. 하나의 IDC에 대한 공격이 다른 IDC 또는 전체 서비스에 영향을 미칠 수 없도록 격리 기반 보호가 구현되어 있습니다.
장애 격리 및 복구: IDC가 서비스 거부(DoS) 공격과 같이 방지하기 어려운 악의적인 공격을 받는 경우 TRTC는 결함이 있는 서버를 합리적으로 처리하여 전반적인 서비스 안정성과 가용성을 보장합니다.
DDoS 완화: TRTC는 각 IDC에 DDoS 방지 방화벽을 배포했으며 DDoS 공격의 위험을 제어할 수 있는 충분한 기능과 리소스를 갖추고 있습니다.

2.3 데이터 분류 및 저장

개인 정보	용도	법적 근거
콘솔에 구성된 데이터: TRTC 애플리케이션 ID 및 이름, 기록 및 릴레이 푸시 활성화 여부, 선택한 과금 방식	당사는 과금을 위해 이 정보를 사용하여 해당 기능의 사용량을 결정합니다. 이러한 데이터는 Elasticsearch Service(ES) 기능에 저장됩니다.	당사는 귀하와 체결한 계약에 따라 해당 기능을 귀하에게 제공하기 위해 필요에 따라 이 정보를 처리합니다.
백엔드 로그 데이터: 라이브 스트리밍 이벤트 참가자의 사용자 ID, 방 ID, 클라이언트 IP, SDK 버전, OS 유형	이 정보를 사용하여 해당 기능이 필요에 따라 실행되는지 확인하고 문제 해결을 수행합니다. 이러한 데이터는 ES 기능에 저장됩니다.	당사는 귀하와 체결한 계약에 따라 해당 기능을 귀하에게 제공하기 위해 필요에 따라 이 정보를 처리합니다.
대시보드 정보: 통화 중 오디오/비디오 품질 정보: 최종 사용자의 APPID, 최종 사용자가 제어하는 기능에 대한 데이터(오디오 및 비디오 활성화/비활성화), 방 입장/퇴장, 방 ID, 음소거 기능, CPU 사용률, 메모리 사용량, 네트워크 딜레이, 데이터 패킷 손실, 해상도, 비트레이트, 프레임 레이트 및 볼륨 레벨	이 정보를 사용하여 해당 기능이 필요에 따라 실행되는지 확인하고 문제 해결을 수행합니다. 이러한 데이터는 ES 기능에 저장됩니다.	당사는 귀하와 체결한 계약에 따라 해당 기능을 귀하에게 제공하기 위해 필요에 따라 이 정보를 처리합니다.
(최종 사용자의) SDK 로그 데이터: 사용자 ID, 방 ID, 클라이언트	이 정보를 사용하	당사는 귀하와 체결

SDK 버전 번호, TRTC 방의 OS 유형	여 해당 기능이 필요에 따라 실행되는지 확인하고 문제 해결을 수행합니다. 이러한 데이터는 ES 기능에 저장됩니다.	한 계약에 따라 해당 기능을 귀하에게 제공하기 위해 필요에 따라 이 정보를 처리합니다.
UIN	당사는 과금을 위해 이 정보를 사용하여 해당 기능의 사용량을 결정합니다. 이러한 데이터는 ES 기능에 저장됩니다.	당사는 귀하와 체결한 계약에 따라 해당 기능을 귀하에게 제공하기 위해 필요에 따라 이 정보를 처리합니다.
SDK APPID (UIN을 사용하여 다양한 애플리케이션용으로 생성됨)	해당 기능의 일부로 이 정보를 사용하여 애플리케이션의 사용량을 결정합니다. 이러한 데이터는 ES 기능에 저장됩니다.	당사는 귀하와 체결한 계약에 따라 해당 기능을 귀하에게 제공하기 위해 필요에 따라 이 정보를 처리합니다.
문제 해결 데이터: 최종 사용자의 APPID, 최종 사용자가 제어하는 기능에 대한 데이터(오디오 및 비디오 활성화/비활성화), 방 입장/퇴장, 음소거 기능, 방 ID, CPU 사용률, 메모리 사용량, 네트워크 딜레이, 데이터 패킷 손실, 해상도, 비트레이트, 프레임 레이트 및 볼륨 레벨	이 정보를 사용하여 문제 해결을 위해 최종 사용자가 직면한 문제를 감지하고 찾습니다. 이러한 데이터는 ES 기능에 저장됩니다.	당사는 귀하와 체결한 계약에 따라 해당 기능을 귀하에게 제공하기 위해 필요에 따라 이 정보를 처리합니다.

TRTC는 통화 내용의 전체 또는 일부를 녹화할 수 있는 온프레미스 녹화 및 클라우드 녹화 기능을 제공합니다. 클라우드 녹화 기능을 사용하는 동안 모든 음성/영상 통화 녹음/녹화는 클라우드 스토리지 서비스에 저장되며 TRTC는 오디오/비디오 파일을 저장하지 않습니다.
TRTC는 Tencent Cloud 고객의 경우 중국 본토에, Tencent Cloud International 고객의 경우 싱가포르 IDC에 위의 데이터를 저장하여 데이터 보안 컴플라이언스를 위한 스토리지 요구 사항을 충족합니다.

2.4 액세스 승인

TRTC 방에 들어갈 때 최종 사용자는 악의적인 공격으로부터 Tencent Cloud 서비스 사용 권한을 보호하기 위해 동적 서명으로 인증해야 합니다. 자세한 내용은 UserSig를 참고하십시오.

2.5 액세스 제어

TRTC는 모든 내부 시스템에 대해 엄격한 액세스 제어 및 관리를 구현합니다. 모든 사용자는 독립적인 내부 계정 및 권한 부여 시스템을 가지며 2단계 인증을 통과해야 합니다. 모든 액세스는 기록됩니다.
사용자 데이터와 관련된 모든 서버는 엄격하게 감사되고 보호됩니다. TRTC는 필요할 때만 서버에 액세스합니다. 보안상의 이유로 TRTC가 서버에 액세스해야 하는 경우 먼저 임시 승인을 받습니다. 전체 프로세스가 기록되고 모든 작업 기록이 보관됩니다.

2.6 내부 보안 감사

당사는 아래에 설명된 대로 해당 기능과 관련하여 처리된 개인 데이터를 저장합니다.

개인 정보	보관 정책
임시 키 정보: SDK APPID, 사용자 이름 및 개인 키	해당 기능을 사용하는 동안 이 데이터를 보관합니다. 기능 사용이 종료되거나 계정이 삭제되면 7일 이내에 이 데이터를 삭제합니다.
애플리케이션 관련 고객 로그 데이터: SDK APPID, 애플리케이션 이름, 태그, 서비스 상태, 생성 시간, 작업	해당 기능을 사용하는 동안 이 데이터를 보관합니다. 기능 사용이 종료되거나 계정이 삭제되면 7일 이내에 이 데이터를 삭제합니다.

귀하는 DPSA에 따라 이러한 종류의 개인 데이터 삭제를 요청할 수 있습니다.

2.7 직원 보안 인식 교육

TRTC는 모든 직원에게 정보 보안 인식 및 보안 컴플라이언스에 대한 정기적인 교육을 제공합니다. 모든 직원은 매년 정기적으로 정보 기밀 유지에 대한 강의와 교육에 참가합니다.

2.8 위반 사항 처리

TRTC 직원은 기밀 유지 계약 및 내부 보안 정책을 준수해야 합니다. 직원이 상기 요구 사항을 위반한 경우 경중에 따라 교육 강화, 해고, 기타 법적 책임 추궁을 포함하되 이에 국한되지 않는 적절한 조치가 취해질 것입니다.

2.9 잠재적인 보안 취약점

TRTC 플랫폼에서 잠재적인 취약점을 발견하시면 티켓을 제출해주시기 바랍니다. 당사의 기술 전문가가 잠재적인 취약점에 즉시 응답하고 해결해 드릴 것입니다. 감사합니다.

취약점을 쉽게 찾고 확인할 수 있도록 다음 내용을 제출해 주시기 바랍니다.
연락처 정보
발견한 잠재적 취약점의 영향을 받는 기능에 대한 설명
잠재적인 취약점을 찾고 재현하는 데 필요한 단계와 방법.