TeamViewer

원격 IT
보안 체크리스트

올바른 원격 기술에 투자하는 데는 시간이 걸립니다. 이 체크리스트에는
안전한 원격 IT 지원을 제공하기 위한 필수 항목이 담겨 있습니다. 모든 항목을 갖추고 있는지 지금 확인해 보세요.

엄격한 비밀번호 규칙 구현
단일 로그인(SSO)으로 직원 안전 프로토콜을 정의하세요.
SSO를 사용하면 직원들은 하나의 비밀번호로 안전하게 로그인할 수 있습니다.
그 결과, 여러 개의 취약한 비밀번호를 생성하고 (또 잊어버리는) 번거로움이 사라집니다.

여러 층의 신원 확인 절차 구축
다단계 인증(MFA)으로 무단 액세스를 방지하세요.
사용자에게 계정, 장치 및 시스템에 대한 액세스 권한을 부여하기 전에,
여러 형태의 신분증을 제공할 수 있는지 확인하세요.

원격 입력 비활성화
원격 입력을 비활성화하여
안전하고 중단 없는 원격 세션을 진행하세요. 지원을 받는 사용자가
흐름을 방해하지 않을 것이란 확신을 갖고 원격으로 연결하세요.

다른 사람들이 화면을 보지 못하도록 방지
블랙 스크린 기능 없이는 보안 원격 지원 솔루션이
완성되지 않습니다. 원격 장치에 액세스하면
원격 장치의 화면이 검게 변하도록 설정할 수 있습니다.

보안 표준의 지속적 준수
BYOC(Bring Your Own Certificate) 정책을 사용하면
디지털 인증서를 통해 클라우드 서비스 및 애플리케이션을 보호할 수 있습니다.
즉, 보안 표준 및 규정 준수에 대해 더 강력하게 제어할 수 있다는 의미입니다.

(원하는 대로) 액세스 권한 부여, 제한, 취소
규칙에 기반한 조건부 액세스 기능을 사용하면
사용자 자격 증명, 위치, 시간, 장치 등의 기준을 기반으로
조치를 취할 수 있어 원격 보안을 대폭 강화합니다.

액세스 권한을 부여할 때는 까다로워지세요
세분화된 액세스 제어를 사용하면 누가 조직의 특정 장치에 액세스할 수
있는지 완벽하게 제어할 수 있습니다. 팀, 개인 및 장치 별로
특별 권한, 라이선스 및 정책을 적용하세요.

더욱 든든해진 안전한 IT
지원을 제공하고 싶으십니까?

자세히 알아보기