

CJIS 규정 준수를 위한 강력한 인증 기능

RSA 공공 부문 솔루션

CJIS(Criminal Justice Information Service)는 FBI의 가장 큰 부서이며 자동차, 범죄 이력, 총기 추적, 지문 기록 등 매우 민감한 데이터를 저장하는 국가 중앙 형사 사법 데이터베이스를 운영하고 있습니다. CJIS 시스템은 사법, 안보 및 정보 기관 파트너에게 미국과 국민을 보호하는 데 필요한 정보를 제공합니다. CJIS는 보안이 보장되지 않는 장소에서 CJIS 시스템에 액세스하는 모든 사용자에게 고급 인증을 요구하는 정책을 시행하고 있습니다.

누가 영향을 받습니까?

다음에 해당하는 모든 조직:

- 연방 기관, 정부, 지자체 및 허가받은 민간 계약업체 등 CJIS 정보 시스템에 액세스하는 조직

어떤 위험이 있습니까?

- CJIS 규정 표준을 준수해야 합니까?
- 모바일 데이터 터미널 또는 핸드헬드 디바이스에서 CJIS 시스템에 액세스하는 직원이 있습니까?
- 노트북 및 모바일 디바이스로부터 CJIS에 대한 원격 사용자 액세스를 보호하기 위해 어떤 방법을 사용합니까?
- 조직에서 원격 사용자 액세스를 위한 강력한 인증인 MFA(Multi-Factor Authentication)를 활용하고 있습니까?
- 사용자의 최소 권한 액세스를 감사, 관리 및 지원할 수 있습니까?

CJIS 액세스 요구 사항 충족

- [FBI의 CJIS\(Criminal Justice Information Service\) 보안 정책 버전 5.8\(2019\)¹, 5.6.2.2.1항](#)
- 이 정책을 준수하면 사용자가 데이터 보안 및 암호화를 일관된 수준으로 유지하여 시스템의 중요한 형사 사법 정보를 지속적으로 보호할 수 있습니다.

RSA SECURID® SUITE

운영 환경 내부, 클라우드 및 모바일 환경에 대한 완벽한 액세스 솔루션

ID 보장

컨텍스트를 고려한 위험 기반의 인증을 통해 뛰어난 보안 및 편의성 제공

옵션 제공

다양한 MFA(Multi-Factor Authentication) 방식을 통해 갈수록 다양해지는 사용자 및 활용 사례 지원

분산된 ID 통합 관리

클라우드, 모바일, 온프레미스 애플리케이션 전반에 일관된 가시성을 제공하고 액세스 정책 및 인증 정책 적용

액세스 보장

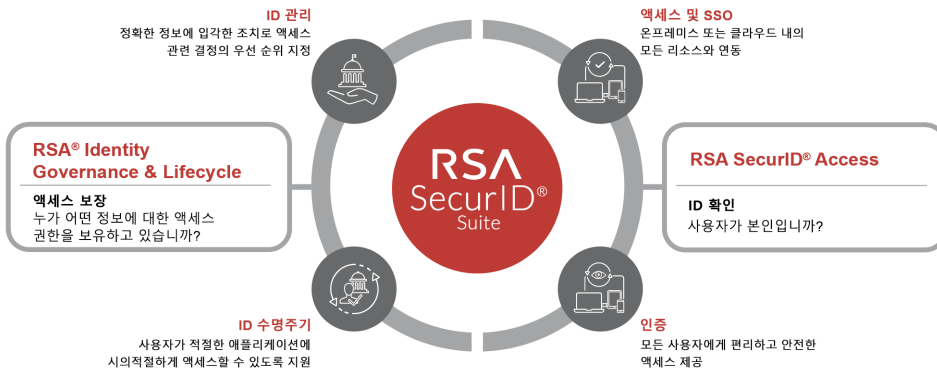
액세스 권한 소유자를 파악하고, 해당 액세스 권한이 적절하고 정책 및 규정을 준수하는지 확인

최소 권한 액세스 관리

사용자가 필요한 자산에만 액세스할 수 있도록 최소 권한 액세스 및 소유 권한 관리

[Rsa.com/trysecurid](https://rsa.com/trysecurid)에서 무료 평가판 신청

- 또한 **CJIS 보안 정책** 5.5.2.1항을 참조해 액세스 권한을 제어하고 감사하여 최소 권한 액세스 제어가 제대로 이루어질 수 있도록 해야 합니다.
- 지속적으로 CJIS 액세스 권한 소유자를 모니터링하고, 변경 내역 감사 추적을 제공하고, 퇴직하거나 더 이상 액세스 권한이 필요하지 않은 사용자의 권한을 해제하려면 ID 거버넌스 및 수명주기 관리가 필요합니다.
- 규정 미준수는 CJIS 데이터베이스에 대한 액세스 권한 상실, 고용 손실 및 고발로 이어질 수 있습니다.



공공 및 계약업체의 ID 및 액세스 보장

제공

업계를 선도하는 다단계 인증

보호 현황

- 25,000여 조직
- 5,500만 사용자

모든 주요 활용

사례로 보안 적용 범위 확장

- 클라우드
- 모바일
- BYOD
- 웹 포털
- 기존 VPN
- 기타...

액세스 제어

- 해당 상황의 컨텍스트 또는 위험 기반
- 액세스 검토 및 사용 권한 감사를 자동화하여 복잡성과 수작업 최소화

자세한 정보

rsa.com/ko-kr/accessthesolution

RSA SecurID Suite는 공공 및 민간 부문 조직에 액세스 권한 및 ID를 제공하여 누가 어디에 대한 액세스 권한을 보유했는지, 액세스 권한이 적절하고 규정을 준수하는지 파악할 뿐만 아니라 사용자가 액세스를 시도할 때 해당 사용자가 본인인지 확실하게 확인할 수 있습니다.

RSA SecurID Suite는 CJIS에 대한 주요 액세스 보안 요구 사항을 지원하는 솔루션입니다.

RSA의 안전한 액세스 솔루션

RSA SECURID ACCESS:

- CJIS가 요구하는 2FA 또는 MFA 제공
- CJIS에서 인용된 “고급 인증” 방식 포함
- 여러 활용 사례에 정책 중심의 위험 기반 MFA 적용
 - 모바일 푸시 및 생체 인식 인증 기능
 - 하드웨어, 소프트웨어 및 모바일에 최적화된 인증기 및 위험 기반 인증
- 자격 증명을 보호하고 권한이 부여된 사용자에게만 액세스 부여

RSA IDENTITY GOVERNANCE AND LIFECYCLE:

- CJIS 시스템에 대한 최소 권한 액세스 관리
- 역할 및 정책에 기반한 액세스 권한 부여 및 권한 해제, 감사 추적 유지
- 적절한 업무 분장이 이루어지도록 지원

가장 광범위한 리소스 세트와의 상호 운용성으로 임무 지원

RSA SECURID ACCESS는 다음을 제공:

- 모든 활용 사례를 지원하는 인증기를 비롯한 업계 최고 수준의 다단계 인증
- 테스트, 문서화, 인증을 완벽하게 지원하는 500곳 이상의 기술 파트너와의 상호 운용성 및 수천 곳 이상의 기술 파트너와의 표준 기반 상호 운용성 제공
-가장 일반적인 CJIS 통합 중 하나인 NetMotion의 상호 운용성 포함
- 전체 통합 목록: rsa.com/ko-kr/partner/rsa-ready-program

RSA SECURID SUITE 정보

RSA SecurID® Suite는 무단 액세스를 차단하면서 디지털 환경에서 리소스에 편리하고 원활하게 액세스할 수 있는 현대적인 업무 환경을 제공합니다. 이 제품군은 비즈니스 중심의 보안 솔루션으로 꾸러진 RSA 포트폴리오의 일부로서 통합된 가시성, 자동화된 분석 정보 및 조율된 작업에 따라 디지털 위험을 관리하는 통합된 접근 방식을 제공합니다. RSA는 전 세계 수백만 명의 사용자를 보호하고, Fortune지 선정 500대 기업의 90%가 넘는 기업이 성장하고 혁신 변화에 지속적으로 적응할 수 있도록 지원합니다. 자세한 내용은 rsa.com/ko-kr을 참조하시기 바랍니다.

1. <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>