

계정/권한 및 패스워드 관리와 감사 접근제어 통합 솔루션

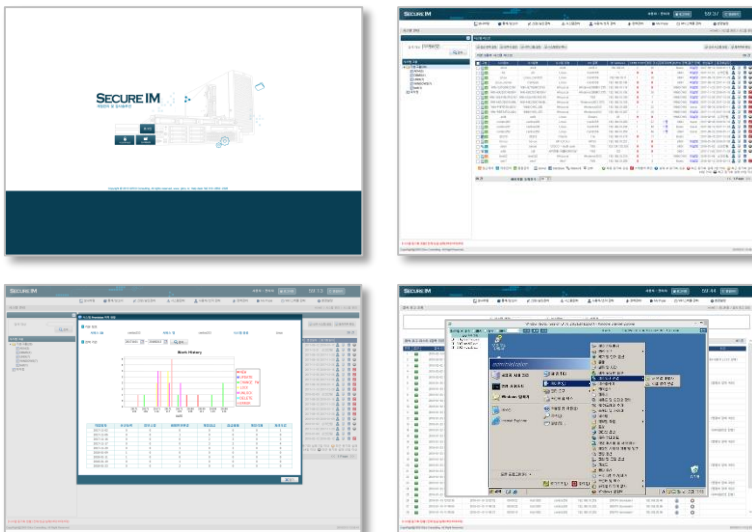
Secure IM은 계정/권한 및 패스워드 관리와 감사/접근제어를 지원하는 통합 솔루션입니다.

계정 라이프사이클 관리를 자동화하고, Workflow 기반의 전자결재를 통해 접근권한을 제어함으로써, 사용자 환경의 편의성 제공 및 전사 IT 시스템에 일관된 정책을 적용할 수 있는 통합계정관리 인프라를 제공합니다.

또한, 시스템계정 레벨의 권한 제어를 통한 특화된 접근제어 기능을 제공하여, 내부 보안 고도화 및 강화되는 Compliance 이슈에 능동적으로 대응할 수 있도록 지원합니다.

❖ 특징점

- 계정/권한 및 패스워드 관리와 시스템 접근제어/감사까지 통합 지원으로 별도의 연동 구축이 불필요
- 서버, 네트워크, 보안장비 등의 시스템 계정관리는 물론 DBMS와 Application 계정의 통합관리 가능
- 전사적, 서비스 별 계정 및 비밀번호에 대한 생성 규칙, 운영 규칙 등의 정책의 일관되고 체계적인 관리 기능 제공
- 시스템의 로컬 정책설정 정보의 관리 및 프로비저닝 가능
- 블록체인 기술을 통한 인증 정보 연동 가능
- 클라우드 환경 지원



관리대상시스템



❖ 주요 기능



계정/권한 관리

- 계정 Life-Cycle 관리 자동화
- 웹 기반의 인터페이스를 통한 조직관리
- 사용자별 직무(관리자/승인자/감사자)에 따른 권한부여
- ID/PW 관리 정책 표준화
- 휴면/잠금/삭제/Ghost&Broken 계정 관리
- 계정/권한 신청 및 승인 프로세스 제공
- 서버, Network, DBMS, 보안장비, Application 계정/권한까지 통합 관리
- 전자결재 및 계정 생성 시 신청자/승인자에게 통보 기능
- 계정/패스워드 정책 프로비저닝 지원

- 정책에 따른 주요 계정의 패스워드 자동 변경 관리 (랜덤 패스워드)
- 관리대상 계정 정보를 수동 입력하지 않고 자동 등록 기능 제공
- 패스워드 복잡성, 변경주기 등 정책의 적용
- 권한을 취득한 계정에 대한 패스워드 확인 프로세스 제공
- 중요 계정의 실제 패스워드 알림없이 사용 권한 부여 프로세스 제공
- 패스워드 정책 설정의 대상시스템 프로비저닝 자동화 지원
(변경 주기, 영숫자/특수문자 포함, 변경 규칙에 대한 정책을 대상시스템에 적용)
- 다수의 패스워드 변경에 대한 일괄 작업 기능으로 관리자 업무 경감
- 패스워드 변경 이력 및 관련 보고서 제공
- 계정 유형 관리 및 유형에 따른 패스워드 변경 예외 설정 가능



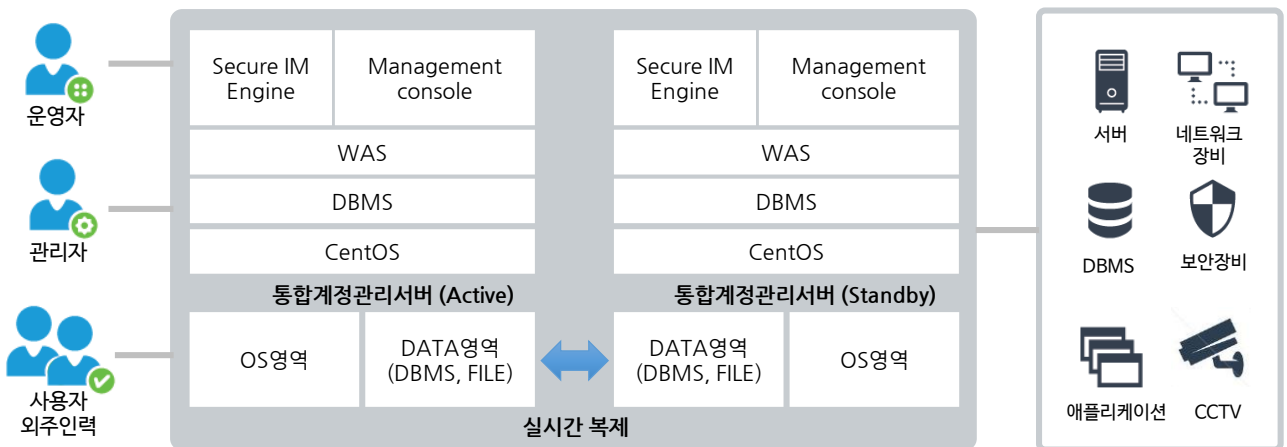
패스워드 관리



감사/접근제어

- 다양한 프로토콜 지원 (SSH, SFTP, FTP, Telnet, RDP 등)
- 다양한 클라이언트 프로그램 지원 (Putty, SecureCRT, Xshell, Filezilla 등)
- Workflow / 정책 기반의 시스템계정 단위의 접근권한 제어
- 접속 세션 별 사용자의 실시간 감사 및 작업이력 감사데이터 제공
- 다양한 조건으로 대상시스템 접근 및 사용 통제 (프로토콜, 요일, 시간, 명령어, IP 등)
- 패스워드 외 추가 인증 지원 (SMS, OTP, 모바일2채널, 바이오인증, 전화인증 등 연동)
- 방향키 사용 히스토리 명령어 실행을 통한 금지명령어 실행 통제
- 웹 스크립트 내의 금지명령어 사용을 N-depth 까지 통제
- 정책 위반 시 관리자 통보 연동 기능 (SMS, Email, Messenger 등)

❖ 구성도



Secure PM은 '계정관리장치 및 방법' 알고리즘의 특허 기술 기반으로 개발된 패스워드 관리 솔루션입니다. 패스워드 관리 강화를 통한 보안성 향상을 효과를 얻을 수 있으며, 관리 업무의 효율화로 관리자의 업무 부하를 경감할 수 있습니다.

❖ 패스워드 관리 솔루션 비교

SECURE PM

기존의 패스워드 관리시스템

- 패스워드 정책 적용(영,숫자,특수문자)
- 패스워드 변경이력 관리
- 패스워드 주기적 변경
- 패스워드 랜덤/일괄 변경기능
- 계정 사용 권한 신청/승인
- 관리대상 계정등록/삭제 수작업

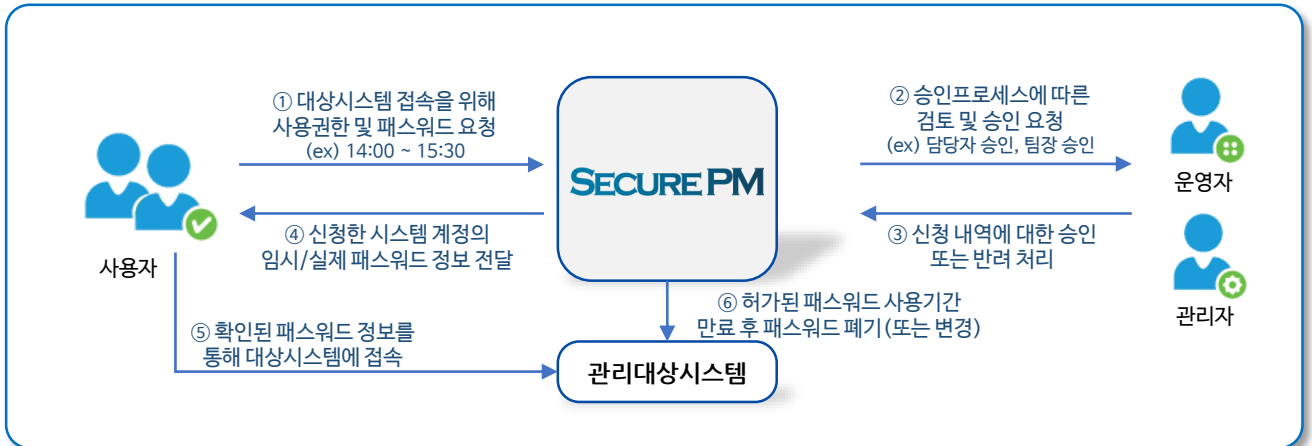
+α

패스워드 관리를 위한 Secure PM만의 추가 기능

- 임의 생성된 Ghost 계정 탐지
- 초기 패스워드로 초기화 된 시스템 탐지 (CCTV, 보안장비)
- 클라우드 환경 지원
- 관리대상 계정등록/삭제 자동화

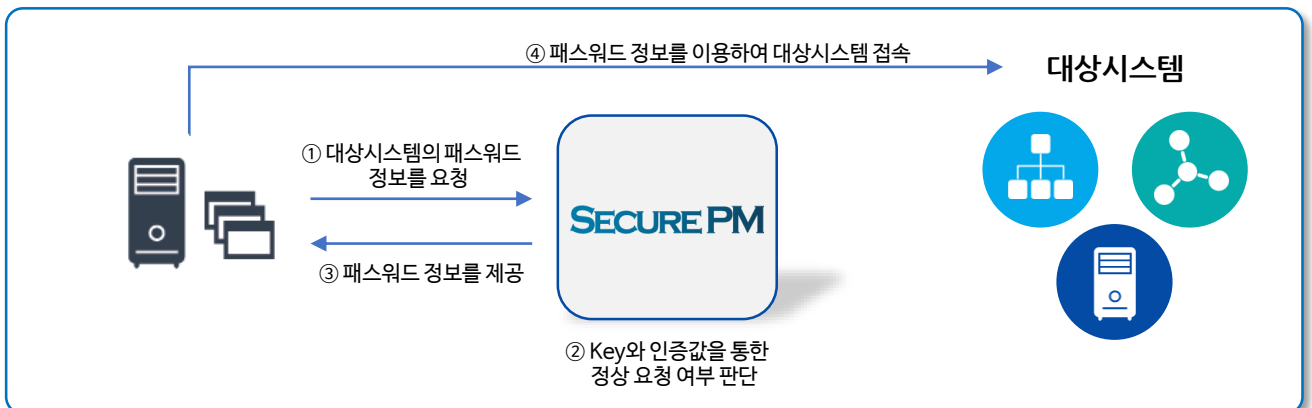
SPECIAL OFFER

❖ 업무 프로세스



❖ 하드코딩 된 계정/패스워드 변경 가능 API 제공

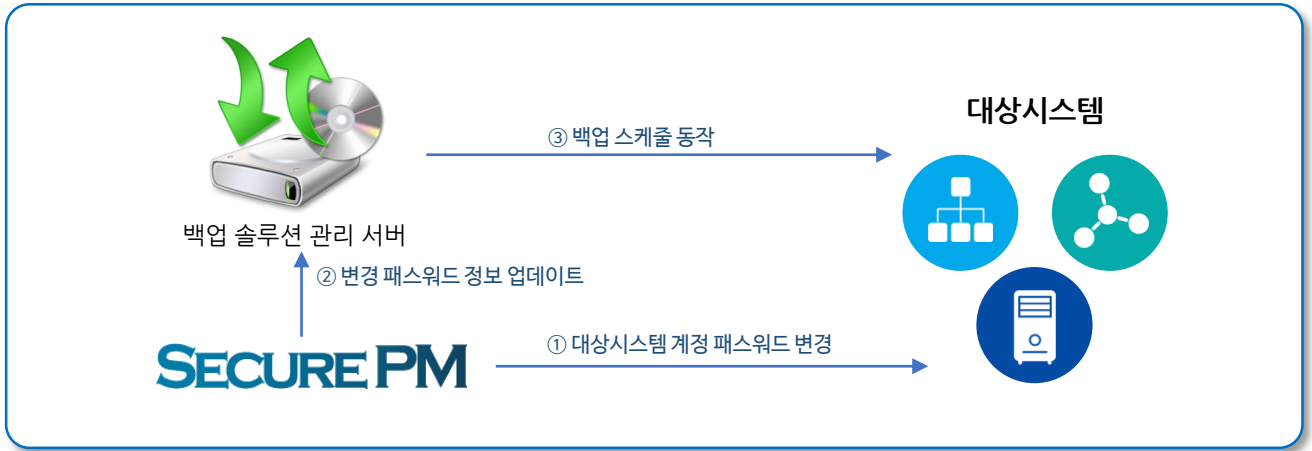
업무시스템 내에 계정 패스워드가 하드코딩 되어 있는 경우, 보안에 취약하며 이를 변경할 시 운영서비스에 영향을 줄 수 있습니다. Secure PM은 패스워드를 변경하여 사용할 수 있는 API를 제공하여 이러한 하드코딩 된 패스워드에 대한 보안을 강화할 수 있습니다.



❖ 패스워드 변경에 대한 백업 솔루션 연계 지원

시스템 계정 랜덤 패스워드 변경에 대한 정보를 백업 솔루션에 반영하여, 패스워드 변경이 백업 솔루션의 동작에 영향을 주지 않도록 구현이 가능합니다.

(ex) CA Backup, 넷볼트 등



❖ 패스워드 관리시스템 비교표

구분	Secure PM	S사 PM	S사 A제품	D사 T제품
다국어 지원	지원	X	X	한글 미지원
구성 방식	Agentless (일부 Agent방식)	Agentless	Agentless	Agent방식 (일부 Agentless)
이중화 지원	지원	지원	지원	지원
계정관리, 접근통제 연동 기능	지원	지원	지원	X
워크플로우 커스터마이징	지원	△	△	X
신규장비 연동 지원	원활	?	?	어려움
국산 보안장비 지원	지원	지원	지원	X
임의 계정 생성/삭제 탐지	지원	X	X	X
관리대상 계정 정보 등록/삭제	자동화	수작업	수작업	자동화
권한별 대상서버 관리 지원	지원	?	?	?
승인자 부재시 비상결재 지원	지원	?	?	?
패스워드 변경 기한 만료시 자동 잠금	지원	X	X	?
보안장비의 패스워드 초기화 자동탐지	지원	X	X	?
Application 하드코딩 패스워드 연동API	지원	지원	지원	?
백업 솔루션 패스워드 연계	지원	X	X	X



CCTV의 안전한 패스워드 관리

SecurePM for CCTV는 다수의 CCTV의 계정에 대해 안전한 패스워드 관리를 지원하는 솔루션입니다.

패스워드를 주기적으로 일괄 변경하고 관리할 수 있는 보안 및 감사 관리 기능을 제공하며, 관리를 위한 정책을 설정하고 적용할 수 있습니다.

SecurePM for CCTV를 통한 관리 시스템 구성을 통해 체계적이고 효율적인 업무 프로세스와 함께 패스워드 관리 부재로 인한 보안 사고나 불법적인 개인 정보 노출 등을 예방할 수 있습니다.

CCTV 패스워드 관리의 필요성

개인정보보호법 및 컴플라이언스 대응

- CCTV 안전조치 의무 [개인정보보호법 제 29조]
- CCTV 영상 정보의 안전한 관리 [제 25조, 제 29조]
 - 관리적, 기술적, 물리적 조치 시행 의무 규정
- 개인정보의 안정성 확보 조치 [제 5조]
 - 접근 권한 관리 및 안전한 비밀번호 설정
- 안전한 비밀번호 관리 기준 [정보통신망법 제 28조]

보안사고 및 영상정보 무단 누출 방지

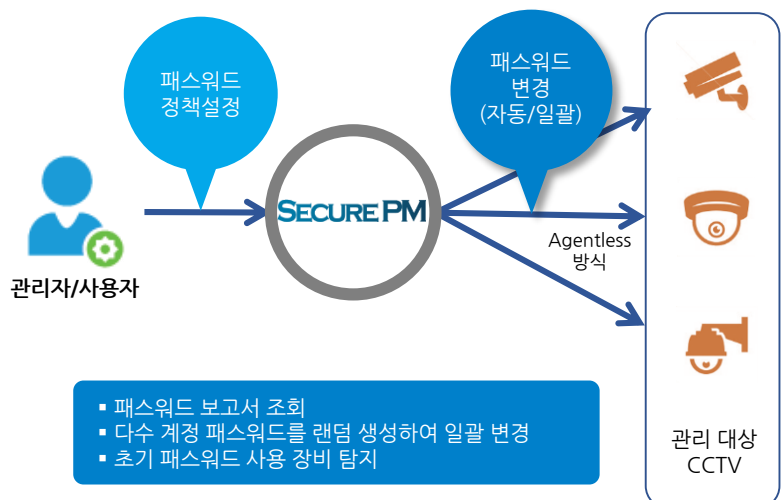
- 익명으로 개설한 웹사이트에 국내 CCTV 및 IP 카메라 6000여개 무방비 노출 사례
- 패스워드 미변경 및 외부노출 또는 '1234'와 같이 간단한 패스워드 사용으로, 불법 접속 가능



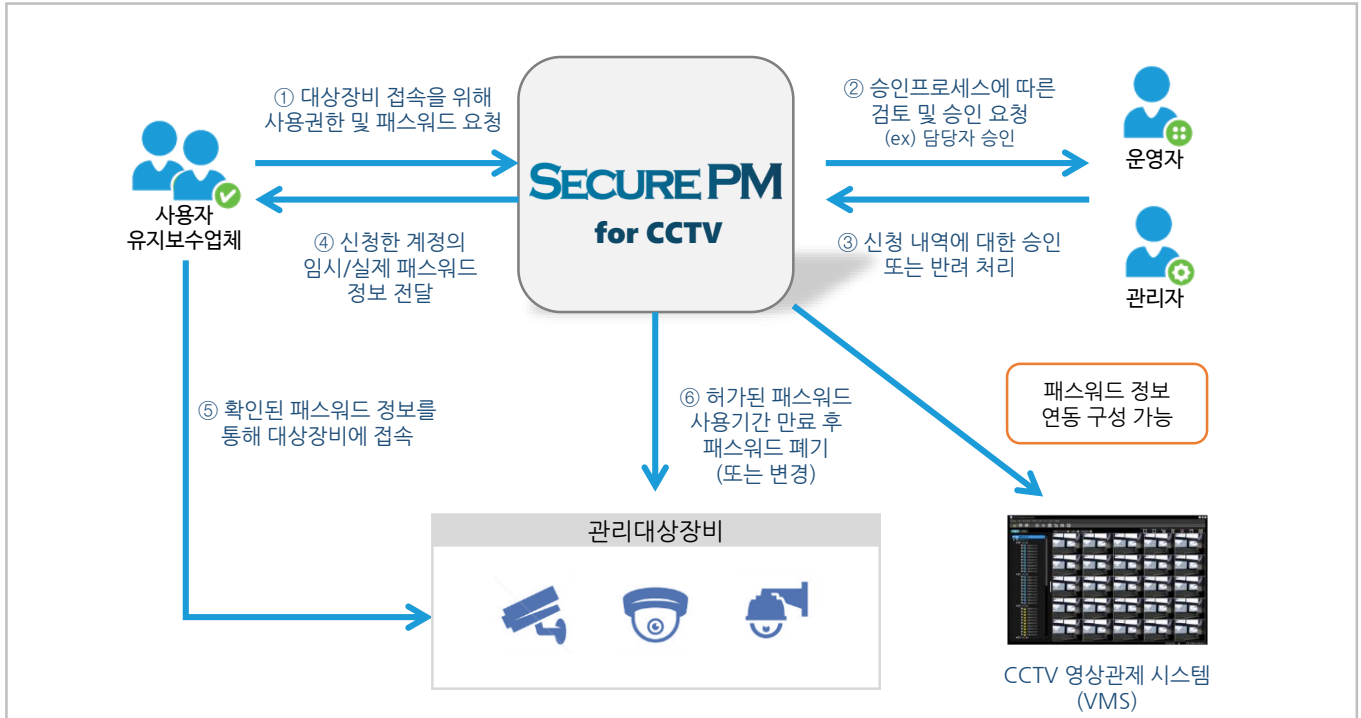
주요 기능 및 특징

SECURE PM

- 다수 CCTV 장비에 대한 패스워드의 체계적인 관리
- 변경 주기, 복잡도, 길이 등에 대한 다양한 패스워드 정책 설정이 가능
- 패스워드 변경/미변경 현황에 대한 정확한 정보 확인
- 자동 및 일괄 변경 기능 지원으로 패스워드 변경 업무의 효율성 제공
- 패스워드 열람에 대한 신청/승인 워크플로우 제공 및 감사로깅 기능
- 초기 패스워드를 사용하고 있는 장비에 대한 탐지



업무 프로세스



강력한 보안 기능 및 편의성 / 확장성 제공



- OTP, 바이오인증 등의 사용자 2Factor 인증 연동 가능
- 다양한 형태의 경고 및 알림 기능
- 관리 및 사용이 편리한 웹 인터페이스 제공
- 웹 전자결제를 통한 패스워드 사용 요청 및 승인과 승인프로세스의 유연한 관리 기능 제공
- 계정관리가 가능한 장비의 경우, 계정 라이프사이클 관리가 가능하도록 확장성 제공
- 관리대상 장비의 모든 계정 정보를 Scanning 엔진으로 수집 관리 가능
- 패스워드 정보를 지정된 위치에 암호화된 형태로 저장하여 비상시 관리자 확인 가능
- 패스워드 정보는 암호화 모듈을 통해 관리하여, 유출로 인한 2차 피해 방지
- 고가용성 보장을 위한 이중화 구성 가능