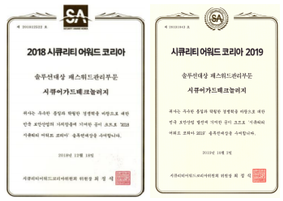
APPM

Automated Process Policy Management

2016년 APICTA 말레이시아
보안 부분 Winner



2018, 2019 시큐리티 어워드 코리아
Password 부분 대상 수상

미래창조과학부

글로벌 SW공모대전 대통령상 수상

√ 보안기능 확인서

전자정부법 제56조에 의거, 국가 · 공공기관이 도입하는 정보보호시스템 · 네트워크 장비 등 보안기능이 탑재된 IT 제품의 안정성을 검증하기 위해 선검증 대상 제품에 한하여 '보안기능 시험서' 제도를 운영
2017년 '보안기능 시험결과서' 제도를 시작으로 운영되었으며, 2020년부터 명칭이 '보안기능확인서'로 변경
'보안기능 시험결과서'의 경우 '신청기관 보관용' 및 '도입기관 제출용'으로 보안기능 시험결과서를 발급하였으나
'보안기능 확인서' 제도로 변경 후 현행 제도에서는 '보안기능 확인서'만 발급
승인 제품의 진위여부는 중앙행정기관 및 지자체 등 각급 기관에서 접근 가능한 '정보공유 시스템'에서 확인
[2020년 09월 18일 승인]

www.secureki.com
08594 서울특별시 금천구 가산디지털1로 5, 1922호 (가산동, 대륭테크노타운20차) TEL. 070-7490-3000 / FAX. 02-6442-7425
5, Gasan digital 1-ro, Geumcheon-gu, Seoul, 08594 Republic of Korea TEL. +82-70-7490-3000 / FAX. +82-2-6442-7425

SECUREKi

APPM SERIES

Automated Process Policy Management

APPM

APPM for Password

APPM은 최고 권한 계정(root, 관리자, 공용 계정)의 패스워드를 주기적, 일괄적으로 변경, 관리하고 워크플로우를 통하여 권한이 부여된 사용자에게 패스워드를 자동으로 생성/발급하는 통합 패스워드 관리 솔루션입니다.
패스워드의 통합관리기능을 통하여 패스워드와 관련된 보안 컴플라이언스에 대응 할 수 있으며, 스크립트 내에 저장된 패스워드 제거를 통하여 서비스의 보안성을 향상 시킬 수 있습니다. 또한 패스워드 변경 실패 작업에 대한 검증 프로세스와 논리적/물리적 장애 시에도 즉시 관리 시스템에서 보관중인 패스워드를 빠르고 안전하게 복원하여 사용할 수 있는 USB 3차 백업 기능은 APPM 만의 특화된 기능입니다. **특히, APPM은 제 26회 글로벌 SW공모대전 대통령상 수상제품으로 기술력과 안전성이 입증되었습니다.**

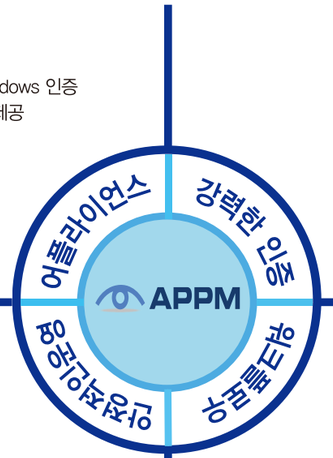
주요기능 및 특징

어플라이언스

- Agent-Less 방식으로 운영 및 관리 용이
  - Telnet, SSH 패스워드, SSH Key 로그인, Windows 인증
  - 웹 기반 솔루션에 대한 패스워드 변경 기능 제공
- 어플라이언스 형태로 제공
  - 설치 및 관리가 용이
  - 서버 자체 Health Check (CPU, Memory, Disk, 온도)기능 제공
- 하드코딩 된 소스코드 패스워드 제거
  - Push/Pull 기능 제공

강력한 인증

- 패스워드 재 사용 방지 기능
- 패스워드 일괄 변경 기능
- APPM 웹 접속에 대한 Mobile OTP 2차 인증 기능
- APPM자체 Incoming/Outgoing 방화벽
- 디스크 베이 잠금 장치 및 디스크 암호화
- 국내 유일 일방향 암호화 방식준수 특허 획득



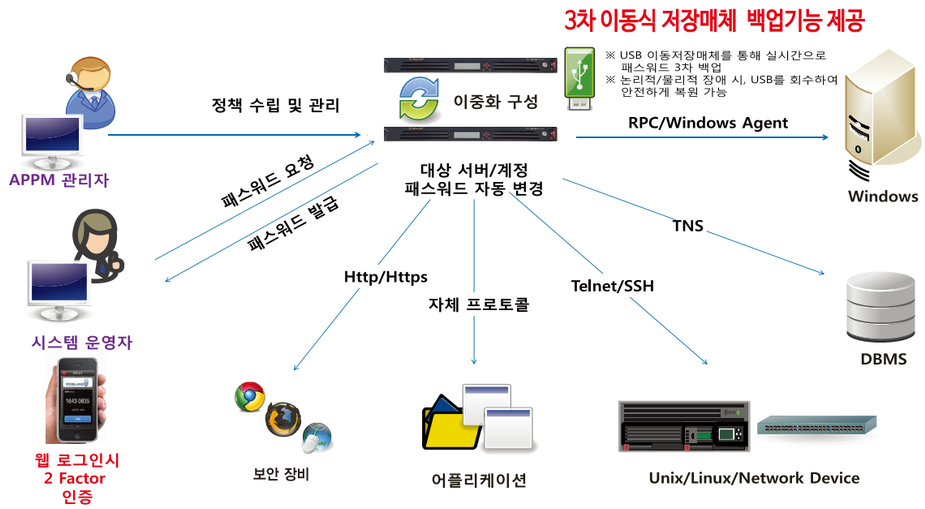
안정적인 운영

- 어플라이언스 이중화를 통한 장애 대비
  - Master/Slave, Active/Active 방식 제공
  - 주요 데이터 실시간 싱크
- 전원 장치 이중화 및 하드 디스크 이중화
- 3차 백업 기능 제공
- 패스워드 Verify 기능 제공
- **패스워드 관리 관련 특허 12 건 등록 및 출원** 특허청

워크플로우

- 계정 사용 권한 신청/승인 기능
- 대규모 고객사를 위한 관리자 권한 위임
- 일회성 패스워드 신청/승인 기능
- 사전/사후 승인 기능 지원
- 요청/승인/사용 이력에 대한 보고서

APPM 아키텍처



최고 권한 계정에 대한 효율적인 관리 방안

패스워드 통합 관리
- 다양한 운영 체제 및 플랫폼 지원(Unix/Windows/Database/Network Device/어플리케이션/보안 장비 등)
- 정기적인 패스워드 변경 및 변경 이력 관리
- 최고 권한 계정 사용 권한 부여에 대한 절차 확립(워크플로우 적용/2차 인증을 통한 패스워드 발급)

정책 수립 및 적용
- 요청변경 : 패스워드 발급, 사용후 자동 초기화
- 주기적 변경 : 패스워드 랜덤 변경 또는 규칙 변경
- 직접 변경 : 관리자가 일괄적으로 수동 변경 또는 계정 소유자가 주기적으로 변경

패스워드 보안 강화
- 외부 업체에 대한 패스워드 공유 방지
- 패스워드 재 사용 방지(사용된 패스워드 자동 초기화)
- 국내 유일 일방향 암호화 방식 준수 특허

하드 코딩된 패스워드 관리방안
- API 제공을 통해 스크립트 내에 패스워드 직접 코딩 방지
- 스크립트 내 패스워드에 대한 자동변경 및 사용

컴플라이언스 대응
- 계정/패스워드 사용 이력 관리
- 내/외부 보안 감사를 위한 권한 리포트 시스템 구축

안정성 및 장애대응
- 패스워드 Verify 기능(패스워드 변경 작업 검증)
- 서버 이중화 구성(자세 실시간 HA 구성 지원)
- 3차 USB백업 기능(논리적/물리적 장애 시 서비스 연속성 보장)

자체 보안성
- 물리적 보안 : 디스크 암호화, 디스크 Bay 잠금, 콘솔 로그인 제한, 2 Factor 인증
- 논리적 보안 : HTTPS 통신, AES/256, ARIA 암호화 적용, 서비스 프로세스 및 어댑터 Integrity 지원, 자체 감사 로깅

Reference

공 공

KDB산업은행, 고등과학원, 공무원연금공단, 공항철도, 국가핵융합연구소, 국립산림과학원, 국립암센터, 국립중앙도서관, 국립환경과학원, 국민건강보험, 국민건강보험 일산병원, 국민체육진흥공단, 금융결제원, 대한체육회, 문화체육관광부, 문화체육관광부 사이버센터, 문화체육관광부 한국문학번역원, 문화체육관광부 한국예술종합학교, 법무부, 부산광역시, 부산지방해양수산청, 사이버경찰청, 세종연구소, 용인시, 우체국물류지원단, 인재개발원, 인천광역시상수도사업본부, 인천국제공항, 질병관리본부, 창업진흥원, 한국교육학술정보원, 한국문화정보원, 한국공항공사 항로시설본부, 한국석유공사, 한국소비자원, 한국수출입은행, 한국양성평등교육진흥원, 한국정보인증, 한국주택금융공사, 한국중부발전, 한국환경공단, 한국환경산업기술원, 해양수산부, 행정중심복합도시건설청 . . . 등

금 융

AXA다이렉트, IBK캐피탈, KB국민카드, KEB외환은행, NH농협, NH농협생명, SBI저축은행, 하나은행, 수협은행, 삼성화재, 동양생명, 신영증권, 알리안츠생명, 여신금융협회, 금융감독원, 유안타증권, 전문건설공제조합, 하나카드, 하나캐피탈, 한국기업데이터, 현대해상화재보험, 카카오뱅크 . . . 등

서비스 / 제조 / 통신 / 기업

삼성, LG U+, KT ds, 딜라이브, 한국문화진흥, 한네트, SK telecom, CJ LION, DOUZONE, SK Infosec, 한화디펜스, 한일현대시멘트, 효성 동서석유화학주식회사, ADT 캡스, 한일홀딩스, GS건설 . . . 등

교육 / 병원

서울대학교, 숭실대학교, 한국과학기술원, 삼육대학교, 중앙대학교, 울산대학교, 한국산업기술대학교, 대구사이버대학교, 명지대학교 성신여자대학교, 한양대학교, 건국대학교병원, 창원경상대학교병원, 성균관대학교, 경남과학기술대학교, 대구보건대학교 . . . 등

국방 / CCTV / ORISS

대한민국 국방부, 국방과학연구소, 국군간호사관학교, 육군교육사령부, 육군헌병, 대한민국해군, 한국국방연구원, 방위사업청 / 동부화재, SK telink, 한국중부발전 / 부산광역시 동구, 양산시 . . . 등

APPM for CCTV

안전한 비밀번호 관리 방법으로 업무를 효율적으로!

APPM for CCTV는 "영상정보처리기기(CCTV)" 최고 권한 계정(root, 관리자, 공용 계정)의 패스워드를 주기적, 일괄적으로 변경, 관리하고 워크플로우를 통하여 권한이 부여된 사용자에게 패스워드를 자동으로 생성/발급하는 **통합패스워드관리 솔루션** 입니다.

현황

- "영상정보처리기기" 계정 비밀번호를 엑셀파일로 관리
- "영상정보처리기기" 계정 관리시스템의 부재로 비밀번호를 수작업으로 변경
- 공공기관에서 관리 중인 CCTV 영상이 해킹사이트에 실시간 게시되는 피해사례 발생
- "영상정보처리기기" 계정 비밀번호에 대한 보안적 이슈 대두

문제점

- 계정 비밀번호 변경에 다수 시간 소요되어, 부족한 인원과 업무효율성 감소
- "영상정보처리기기" 계정의 비밀번호가 저장된 엑셀 파일이 유출될 경우 모든 계정의 비밀번호를 알 수 있게 되어 보안의 치명적인 약점 발생
- 유지보수 용역 인원에게 부여한 비밀번호를 사용자가 암기하여 악용할 가능성 높음

주요기능

영상정보처리기기(CCTV)의 안전하고 체계적인 비밀번호 관리

- 실시간 접속 일회성 패스워드 주기적 발급 및 제공
- CCTV에 접속해 수행하는 모든 패스워드의 결과를 모니터링하고 실시간으로 패스워드를 기록
- 영상관제솔루션과 비밀번호 정보 자동 업데이트 제공
- 다양한 비밀번호 정책 설정 기능

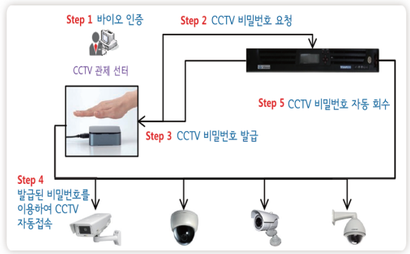
업무 효율성 보장 환경

- 다양한 비밀번호 정책을 설정 기능
- 허가받은 사용자에 대한 비밀번호 사용권한을 줄 수 있는 워크플로우 기능 제공
- CCTV 계정 관리 및 자산 기능 제공
- 비밀번호가 해킹의 위험으로부터 노출되지 않도록 쉽게 추측 할 수 없게 안전하게 설정

실시간 모니터링

- 다양한 비밀번호 정책을 설정 기능
- 중앙 관리 웹 콘솔에서 APPM for CCTV v1.4 서비스 프로세스의 상태 모니터링 제공

▲영상관제솔루션 자동 업데이트



▲바이오인증 본인 확인

특장점

1 3차 백업 지원(USB)
보안 USB 이동저장매체를 통해
실시간으로 비밀번호 일방향 3차 백업

2 보안 접속
관제센터에서 CCTV에 접속 시 비밀번호
노출 없이 바이오인증 방식을 통한 본인 확인 절차를 이용

도입 효과

1. 개인정보보호법 및 개인정보보호관리체계 준수

- 관련 근거에 적합한 개인정보에 대한 접근 권한의 제한 및 관리조치 준수
- 권한 없는 사용자의 최고 권한 계정의 접근을 차단하기 위한 시스템의 설치 및 조치 준수
- 영상관제솔루션과 비밀번호 정보 자동 업데이트 제공
- 다양한 비밀번호 정책 설정 기능

2. 정보자산 시스템 비인가 접근 및 사고위험 방지

- 정보자산 시스템 비인가 된 사용자의 최고 권한 계정으로의 접속을 완전 차단하여 사고 방지
- 정보자산 시스템의 내부자 최고 권한 계정에 대한 사용제어를 통하여 발생 가능한 위험 방지

3. 정보자산 시스템 접속작업 기록/감사/관리 및 장애대응

- 정보자산 시스템에 인가 된 사용자의 접속 작업 내역을 기록해 작업 내역 추적·감사를 통하여 신속한 장애 대응이 가능

비밀번호 컴플라이언스 및 감사 대응

CCTV 영상정보 안전한 관리를 위한 안정성 확보 조치 주요 내용

◆ 개인정보보호법 [제29조 안전조치 의무]
개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 안정성 확보에 필요한 관리적 · 기술적 및 물리적 조치 시행 의무

▶ 접근통제 및 접근 권한의 제한, 암호화 기술 적용 조치, 보안프로그램의 설치 및 갱신

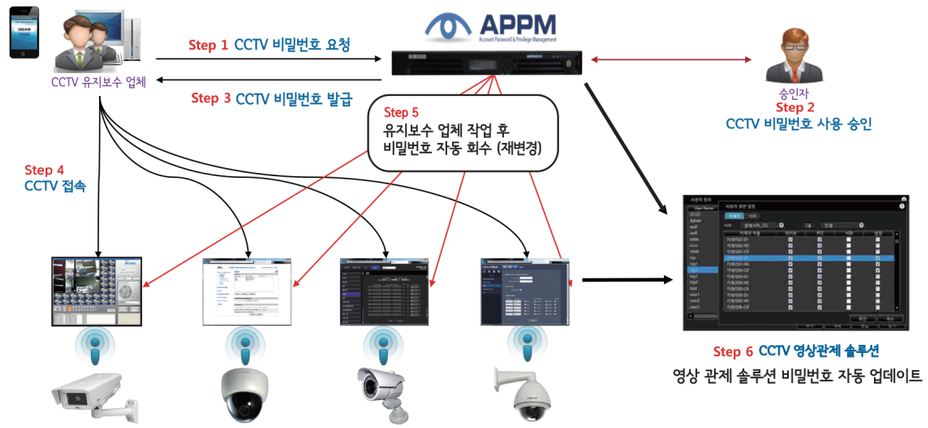
◆ 개인정보보호법 시행령 [제30조 개인정보의 안전성 확보 조치]
개인정보영상을 안전하게 저장, 전송할 수 있는 기술의 적용

▶ 네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치, 비밀번호 설정 및 갱신

◆ 개인정보의 안전성 확보조치 기준 [제5조 접근 권한의 관리]
개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용

◆ 정보통신망법 [제28조 개인정보의 보호조치] [시행령 제15조 개인정보의 보호조치]
비밀번호의 생성 방법 및 변경 주기 등의 기준 설정과 운영,
비밀번호의 일방향 암호화 저장 및 갱신

CCTV 아키텍처



APPM for CCTV 내부통제

CCTV 내부통제로 비밀번호와 오남용 감시를 동시에 관리!

APPM for CCTV 내부통제는 CCTV 및 VMS 기기의 비밀번호 관리 및 기기 운영 시 영상정보의 오남용을 감시•통제하며 권한이 부여된 사용자에게만 해당 기기로의 접근을 허용하는 **통합 내부통제시스템** 입니다.

주요기능

CCTV 및 VMS 접근 관리, 통제

- CCTV, VMS의 로그인, 설정변경, PTZ등의 이력 수집
- CCTV 자산정보, 장애일지, 해상도 조절
- CCTV, VMS 접근 권한 관리
- 관제업무 운영 PC의 로그인 생체 인증 제공

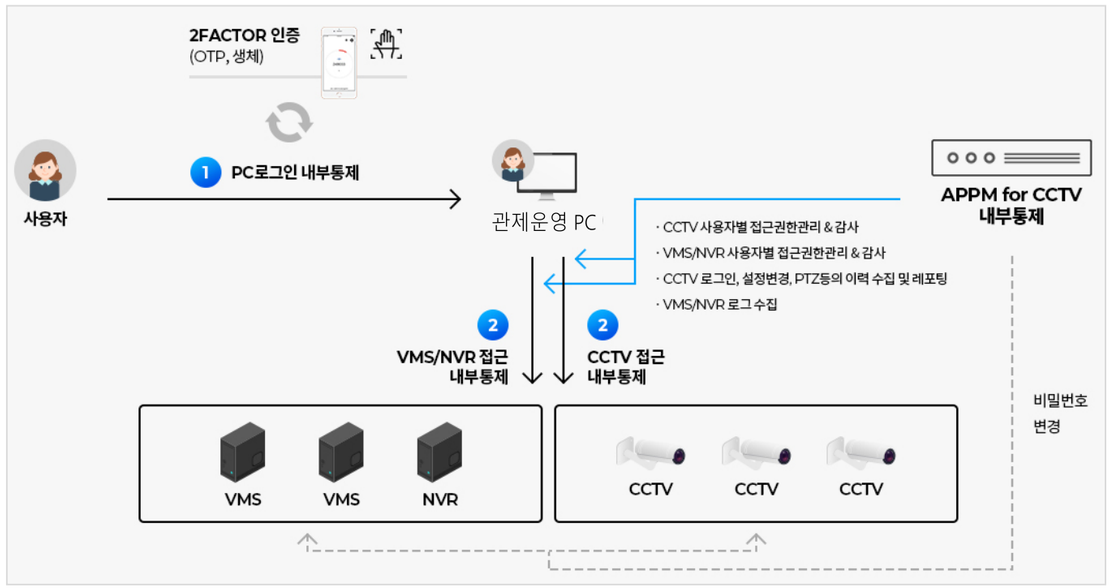
비밀번호 관리

- CCTV 비밀번호 관리 및 VMS 자동 업데이트
- 관제업무 운영 PC의 비밀번호 관리 기능 제공
- 다양한 비밀번호 정책 제공
- 워크플로우를 통한 비밀번호 발급 및 회수 기능 제공

실시간 오남용 감시 및 모니터링

- 영상정보처리기기 접속 및 오남용 행위 감시 기능 제공
- 관제업무 운영 PC의 로그인 이력 관리 기능 제공
- 사용자별 영상저보처리기기 접속에 대한 이력 제공
- 영상정보처리기기 및 VMS/NVR 작업 이력 실시간 감시 및 재현 기능 제공

아키텍처



도입 효과

1. 개인정보보호법 및 개인영상정보 보호원칙 준수

- 관련 근거에 적합한 개인정보에 대한 제한 및 관리조치 준수
- 관련 근거에 적합한 권한 없는 사용자의 접근차단으로 설치 및 운영에 관한 조치 준수

2. 영상정보 사용 오남용 행위 방지 및 대응

- 영상정보처리기기 접속에 대한 실시간 감시 및 오남용 행위 감시를 통한 컴플라이언스 준수
- CCTV 및 VMS 접근 시 2차 인증 수행으로 사용자 식별에 대한 안정성 확보 조치 준수

3. 영상정보처리기기 접속작업 기록/감사/관리 및 통제

- 영상정보처리기기의 사용자별 접속 및 작업이력 리포트 제공을 통한 컴플라이언스 준수
- 영상정보처리기기의 로그인, PTZ 이력 등을 기록 및 통계화하여 발생 가능한 위험 방지

컴플라이언스 및 감사대응

◆ **개인정보보호법 제31조 제2항 제4호**
◆ **공공기관 영상정보처리기기 설치.운영 가이드라인 제7조**

개인정보 유출 및 오용.남용 방지를 위한 내부통제시스템 구축

◆ **개인정보보호법 제24조 제3항, 제25조 제6항**

분실/도난/유출/위조.변조 또는 훼손방지 안정성확보 조치

◆ **서울특별시 영상정보처리기기설치 및 운영에 관한 조례 제4조(개인영상정보의 보호원칙)**

개인영상정보에 대한 접속기록 및 영상정보처리기기 조작행위 기록은 안전하게 보관•관리되어야 하며 주기적으로 점검 받아야 한다.

◆ **경기도 개인영상보호 및 영상정보처리기기 설치•운영 조례 제4조(개인영상정보의 보호원칙)**

영상정보처리기기 운영자는 개인영상정보 접속기록, 영상정보처리기기 조작행위 기록을 남기고 소명처리 하여야 한다.

특장점

1 통합내부통제시스템(ALL in One)

- PC, CCTV, VMS 접근 권한 통제 및 감시
- PC, CCTV, VMS 비밀번호 관리

2 보안 접속

- 관제센터에서 CCTV 및 VMS 접속 시 비밀번호 노출 없이 생체 인증 방식을 통한 본인 확인 절차 이용 가능

인증 및 자격

GS인증 획득 | 조달등록제품 | 특허 등록 | 국가용 보안요구사항

APPM for 간편로그인

APPM for 간편로그인은 기존 응용프로그램의 소스코드 수정이나 연동 작업 없이 다양한 어플리케이션을 패스워드 노출 없는 생체 인증을 통해 접속 할 수 있는 기능을 제공 합니다.

제품의 특징

- 업무 프로그램 접속 시 각기 다른 방법으로 접속
- 사용자가 개별적으로 패스워드 변경 관리
- 아이디/패스워드만으로 접속할 수 있기 때문에 대리 접속이 가능

해결방안

- **어플리케이션 사용자 계정 비밀번호 자동 관리 필요**
  - 각 어플리케이션 관리자 계정 비밀번호는 일회용으로 발급하고 사용 종료 시 자동 회수 필요
- **기본 아이디/패스워드 보다 강력한 인증 체계 필요**
  - 생체 인증을 통해 강력한 인증 체계 구축
  - 대리 접속 방지
- **업무 효율성 향상**
  - 비밀번호 분실 / 재설정으로 인한 업무 지연 및 장애리스크 제거
- **보안 향상 및 감사 대응**
  - 어플리케이션 접속 이력 로깅
  - 비인가 접속 방지

주요기능

- **사용자 어플리케이션 비밀번호 자동 관리**
  - 사용자는 더 이상 어플리케이션 비밀번호를 기록/기억 할 필요가 없음
- **생체 인증을 통한 안전한 어플리케이션 자동 접속**
  - 모든 어플리케이션 적용 가능
  - 웹 기반,C/S 기반,패키지 어플리케이션,서버 등
- **감사 추적**
  - 어플리케이션 접속 이력 로깅 / 비인가 접속 방지
- **업무 효율성 보장**
  - 빠른 어플리케이션 접속 · 자동 시작/자동 접속
  - 비밀번호 분실/초기화로 인한 업무 부담이 없음
- **보안 향상**
  - 어플리케이션 비밀번호 변경 규정 및 비밀번호 생성 규칙을 준수 / 비밀번호 미 노출로 대리 접속 방지

인증 방식의 진화

지식 기반 인증

- 사용자가 알고 있는 정보를 기반으로 인증 (ID & Password)

소지 기반 인증

- 사용자가 가지고 있는 소지품을 기반으로 인증(출입카드, OTP)

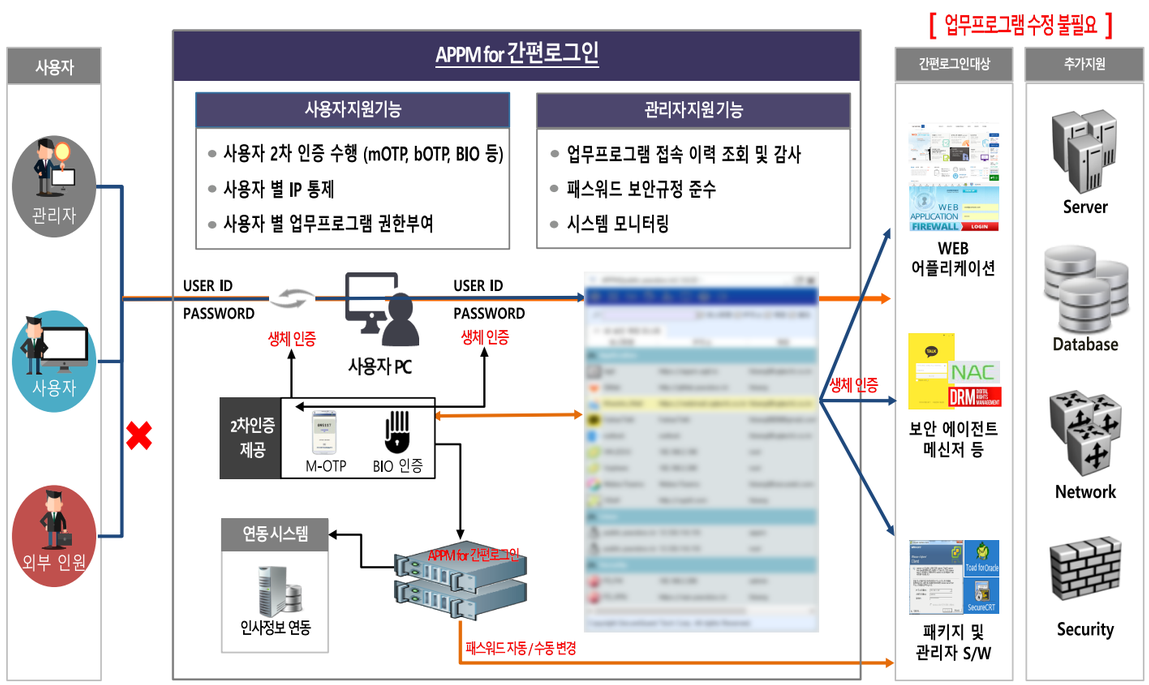
생체 기반 인증

- 사용자의 생리학적, 행동학적 특성을 기반으로 한 인증(홍채, 지문, 걸음걸이 등)

간편로그인 도입을 통한 『보안성이 강화된 어플리케이션 접속환경』

ID/PW 환경의 **보안성 강화**	사용자 PC, 업무프로그램, 상용프로그램 등 모든 사용자 접속환경에 2차 인증 적용을 통한 사용자 접속환경의 보안성을 강화합니다.
업무프로그램 계정에 대한 **패스워드 자동관리**	사용자 PC, WEB 기반, CS 콘솔 기반 등 모든 어플리케이션 계정의 패스워드를 실시간 자동 변경하여 패스워드 미변경으로 인한 취약점 제거 어플리케이션 소스코드 수정 없는 자동 로그인 기능 구현
FIDO기반 생체인식기술 **사용자 편의성 강화**	분실 및 불법사용의 여지가 있는 2차 인증 디바이스를 대체하여, FIDO 기반 생체인식 기술 적용으로 보다 편리하고 안전하게 개인인증을 수행합니다.

APPM for 간편로그인 아키텍처



APPM for IRASS

패스워드 관리 기반의 접근 통제 시스템

새로운 보안 계층 - 모든 권한 있는 엑세스 제어 및 감사

- 자동화되고 중앙 집중화된 패스워드 관리
- 중앙 집중식 인증
- 세션 기록 및 재현
- 접근 신청/승인 워크플로우
- 다단계 인증
- 지능적인 분석 및 이벤트 알림
- 세분화된 접근 통제
- 중앙 집중식 정책 관리
- 권한 기반 간편 로그인

주요 기능 및 특징

비밀번호 정책

- **요청변경**
  1회용 비밀번호 정책,
  패스워드 발급 후 자동 회수
- **주기적 변경**
  스케줄이나 규칙에 따라 변경
- **메뉴얼 변경**
  사용자가 원하는 암호로 직접 변경
- **즉시 변경**
  관리자가 즉시 패스워드 랜덤 변경

워크플로우

- 접근에 대한 신청/승인 가능
- 신청/승인에 대한 리포트
- 1회용 비밀 번호 요청 기능
- 권한 위임/대리 승인 기능

쉬운정책

- Agentless 기반의 운영
- TELNET, SSH, FTP, SFTP, RDP, Web, CS 접근 통제 및 실시간 감사 추적
- HTML5 기반 웹 SSH/웹 RDP 접속

어플라이언스 기반 및 가상화 기반 서버

- 쉬운 설치 및 관리
- 서버 Self-Health 체크- 서버 리소스, FAN, 파워 서플라이 등

하드코딩 패스워드 제거 기능

- Push / Pull 아키텍처

세션 리코딩 및 재현

- 감사 추적을 위한 실시간 세션 모니터링, 기록 및 재생 기능
- SSH, TELNET, FTP, SFTP, RDP, 웹, CS 어플리케이션에 대한 접속 통제 세션 모니터링, 기록 및 재생 기능

APPM for IRASS 접근 통제 시스템

패스워드 관리 솔루션과 완벽한 통합

- **다양한 운영 체제 및 플랫폼 지원**
  (유닉스 / 리눅스 / 윈도우 / 데이터베이스 / 네트워크장비 / Web, CS 어플리케이션 / 보안장비)
- 주기적인 암호 변경 및 요청 변경
- 워크플로우 기반 패스워드 제공 정책

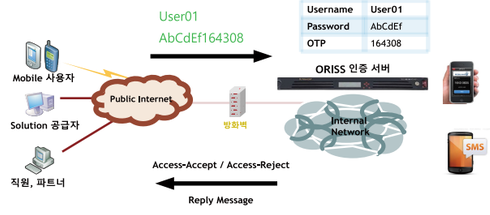
APPM for ORISS

APPM

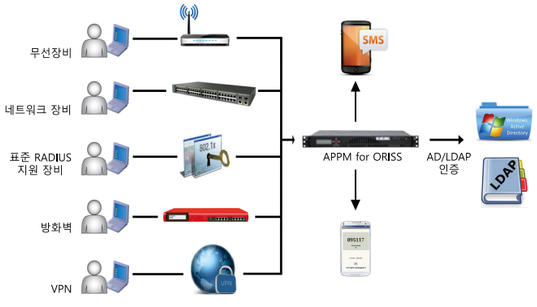
ORISS는 내/외부 접속에 대한 인증 강화가 요구됨에 따라 인증 강화 요건을 충족 시킬 수 있는 솔루션입니다. 현재 대부분의 로그인 방식이 ID/PW를 사용하고 있는데, 이경우 고정 Password를 보완할 TWO Factor 인증이 필요하게 됩니다. ORISS는 인증 필요시 재사용이 불가능한 OTP를 사용하고 본인의 Mobile 기기를 사용하므로 도용이 불가능합니다. 또한, 계정 및 패스워드 유출 시에도 완벽한 보안 기능을 제공합니다.

주요기능 및 특징

OTP 인증 서버와 RADIUS 인증 서버 일체형 어플라이언스,
표준 RADIUS 지원 장비에 대해 솔루션 수정 없이 2차 인증 기능,
OTP 및 SMS 2차 인증 기능 제공

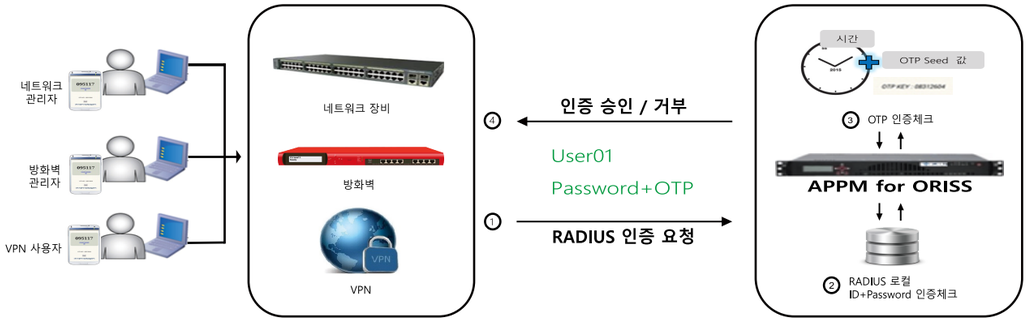


적용분야



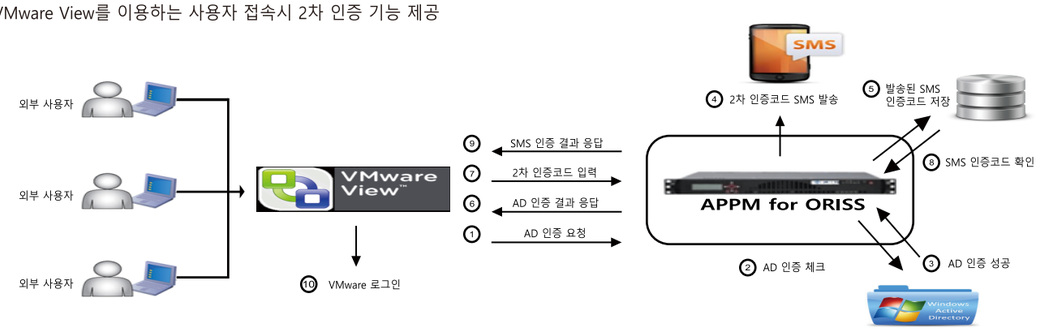
네트워크 및 보안장비 적용예

네트워크 디바이스 및 Firewall, VPN등과 같은 보안장비 2차 인증 기능 제공

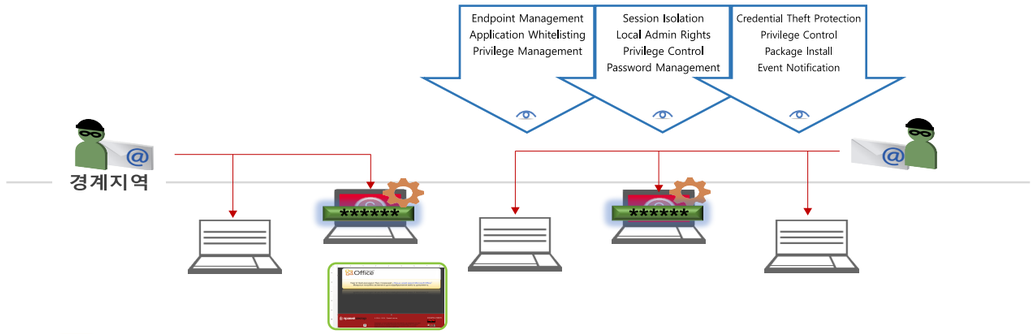


VMware View 적용예

VMware View를 이용하는 사용자 접속시 2차 인증 기능 제공



APPM for Defender



1 **스피어 피싱 캠페인**
대상 직원 선정

2 **Endpoints 감염**
이메일이나 다른 경로를 통한 악성 파일 첨부/실행

3 **공격자 접근 권한 획득**
RAT를 위한 백도어 설치

4 **정보 수집**
인증 정보 및 기타 정보 수집

도입 효과

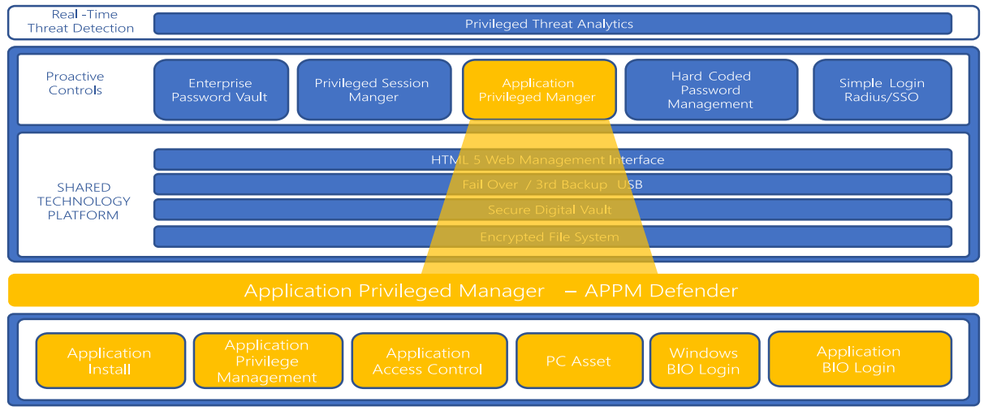
- 권한 있는 계정 사용에 대한 모니터링과 이상 징후 탐지
- 네트워크 전반에 대한 사전 예방적 인증 관리
- 관리자 권한 사용에 대한 요청 및 승인
- 모든 PC에 대한 단일 관리 기능 제공
- 워크플로우 기반의 윈도우 패키지 설치 지원
- 어플리케이션 통제를 통한 멀웨어 기반 공격 위험 감소

위험 분석 및 대응

수집
데이터 수집 및 분석
감지
의심스러운 활동 및 행동 식별
경보
자세한 사고 정보 전파
대응
신속한 대응 및 봉쇄

- 알려지지 않은 실행 프로그램 차단 및 경보
- Admin 권한 사용 모니터링
- 로컬 Admin 사용으로 도메인 보호
- Admin 권한 로그인 및 원격 로그인 감시
- 비 인가 소프트웨어 설치 감시
- 권한 기반의 RunAS 실행

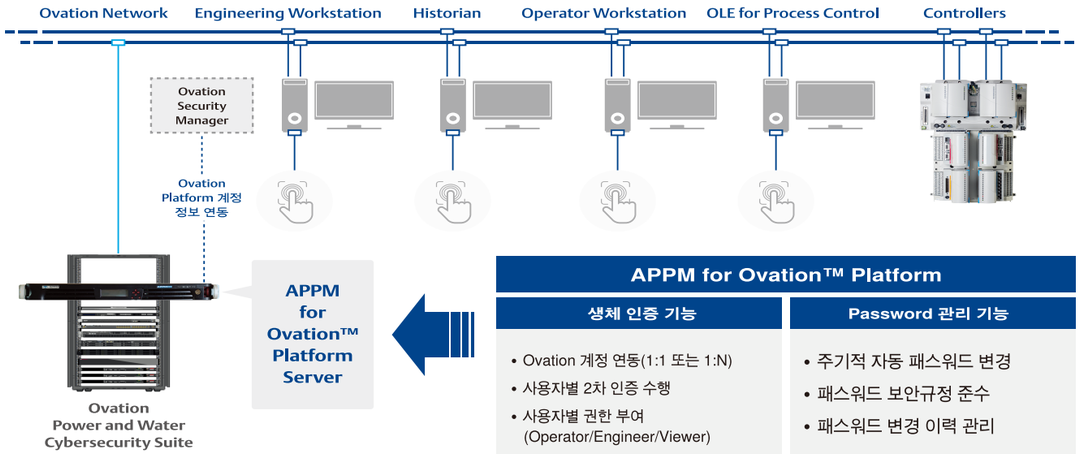
아키텍처



APPM for Ovation™ Platform

APPM for Ovation™ Platform은 생체 인식을 통하여 발전 및 수처리 통합제어시스템에 안전하고 강화된 보안 솔루션을 제공합니다.

구성도

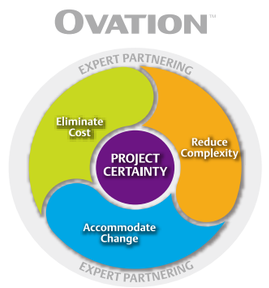


도입 효과

보안성
- 보안 위험 원천 차단
- 보안 취약점 보완 및 개선
- 계정 및 개인정보 관리 법규 충족

효율성
- 주기적 자동 패스워드 변경을 통한 체계적, 효율적 패스워드 관리 가능

통합제어시스템 (DCS)



편의성
- 감사 레포트 준비시 빠른 대응 가능
- 생체인증 기반의 간편 로그인 인증을 통한 보안성, 편의성 강화

안정성
- 시스템 안정성 증대

강화되는 보안 규정 1

산업통상자원 사이버안전센터 보안 상세 가이드(주요 통신기반시설 취약점 분석 평가)

법규	구분	항목	취약점 점검 항목	중요도	적용결과
제어시스템	계정관리	C-1	제어시스템 운영, 관리를 위한 계정이 타 사용자와 공유되지 않음	상	만족
	보안관리	C-18	비인가자 또는 인증과정이 없이 제어시스템, 제어기기에 대한 환경 설정이 가능하지 않도록 되어 있는가?	중	만족
관리분야	접근통제	A-50	외부에서의 사용자 접근에 대한 안전한 인증방식을 사용하고 있는가?	하	만족

강화되는 보안 규정 2

계정 및 개인정보관리 법규

법규	관련 조항	충족 여부
정보통신망법 제28조(개인정보의 보호조치)	3. 접속기록의 위조·변조 방지를 위한 조치	충족 - 위조 변조가 불가능한 개인 생체 정보를 통한 로그인 방식 채택
개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)	1. 개인정보처리자는 고유식별정보, 비밀번호, 바이오 정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.	충족 - 비밀번호 및 개인 생체 정보를 암호화하여 단방향 저장 관리
개인정보의 기술적·관리적 보호조치 기준 제4조(접근통제)	1. 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성 2. 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고 3. 비밀번호에 유효기간을 설정하여 반기 별 1회 이상 변경	충족 - 규정 이상의 패스워드 복잡도를 적용하여, 설정된 주기별로 패스워드 자동 생성

APPM for WinBio

당신의 패스워드는 안전하다고 생각하십니까?

해커는 당신이 변경하지 않고 사용중인 패스워드를 쉽게 탈취하고 사용 할 수 있습니다. 다른 방법들도 있습니다. 해커가 당신의 패스워드를 도용하는 것은 아주 쉬우며, 인증 자격을 도용할 수 있는 수백가지 방법을 알고 있습니다. 그리고 이 기술은 점점 더 정교 해지고 있습니다.

2016년 보고된 정보 유출 사고는 40% 증가하였고, Yahoo는 계정 정보 유출을 인정하였으며, 이는 10억개 이상의 계정에 영향을 주었습니다.

당신의 PC는 보호되고 있습니까?

패스워드만으로 당신의 PC를 보호하고 있다면 이것은 개인이나 기업에 엄청난 위험을 안겨 줄 수 있습니다. 개인 정보에 대한 침입과 해킹은 어디에서나 발생 할 수 있습니다.
자신의 PC를안전하게 보호하고 패스워드 관리 문제를 해결할 수 있는 방법 중 가장 먼저 할 수 있는 일은 2차 인증을 통한 보안 강화입니다.

일반적으로 2차 인증은 One-Time Password(OTP)를 이용하여 Windows 보안을 강화하는 방법 입니다.

그렇다면 2차 인증까지 결합하여 사용한다면 당신의 PC는 안전해 질까요? 여기에 당신만이 가진 조건을 추가할 수 있다면 당신의 PC는 더욱 안전하게 될것입니다. 이미 당신은 그것을 가지고 있고 그 자체로 훌륭한 인증 체계가 됩니다. 그것은 바로 당신의 생체 정보입니다.

생체 정보는 잃어 버릴 수가 없습니다.

생체 정보는 탈취할 수도, 도용할 수도 없습니다.

**당신만이 그것을 가지고 있고,
당신만이 그것을 사용할 수 있습니다**

Windows에서 2차 인증을 설정하고 사용함으로써 Windows PC에 대한 수준 높은 보호가 가능합니다.

모바일 지문, 정맥등을 이용한 다중 인증 솔루션이 바로 생체 인증 기술이 중심이 된 솔루션입니다.

사용자가 Windows OS 보안을 유지하면서 쉽게 컴퓨터에 로그인하는 방법은 무엇일까요?

모바일 생체 인식 이나 OTP를 통해 암호 없는 빠른 로그인 기능을 사용할 수 있습니다.

Windows 패스워드를 기억할 필요가 없고 패스워드 재 사용이 불가능하며 패스워드를 분실해서 재 설정 요청에 필요한 노력을 하실 필요가 없습니다.

암호를 생체 인증으로 대체하여 여전히 높은 수준의 보안을 제공합니다. 이렇게 하면 암호와 관련된 다양한 보안 위험을 사전에 예방할 수 있습니다

시간 동기화 방식의 모바일 OTP

모바일 지문 센서 혹은 정맥 센서

Offline 2차 인증

이 방법은 진정한 다중 인증을 제공하는데 필요한 세가지 요소 입니다.
또한 사용자를 위해 단순화 된 로그인 프로세스를 함께 제공하며,
패스워드 없는 로그인 방법을 지원합니다.

어떻게 동작할까요?

사용자가 PC를 로컬로 로그인하거나 도메인 자격 증명을 사용하여 로그인 할 경우 모바일 지문이나, 정맥 인증을 통하여 간편하게 로그인 할 수 있습니다. 이것은 별도의 인증 프로그램이나 응용 프로그램 수준이 아닌 네이티브 Windows 인증 수준에서 처리되어 강력한 보안성을 담보합니다.

사용자는 OTP번호를 입력하거나 생체 인식을 위해 모바일폰에 지문을 접촉하거나 정맥 인식을 선택할 수 있습니다.

인증된 사용자는 로컬 및 도메인에 대한 액세스 권한이 부여됩니다. 이것은 로그인을 안전하고 빠르게 할 수 있으며 매우 효율적입니다.

기능

Windows OS 보안

- 패스워드 도난 및 분실 방지
- 악성코드 또는 해커에 의한 로그인 자격 인증 탈취 방지
- Brute Force 공격 방지 및 예방

생체를 이용한 자동 로그인

- 모바일 지문 센서
- 정맥 센서

패스워드 초기화 기능

- 관리자 개입없이 패스워드를 스스로 초기화하고 잠긴 계정을 해제 할 수 있는 기능 제공

다양한 로그인 옵션

- 도메인 로그인 지원
- 패스워드를 이용한 로그인, 모바일 OTP, 생체 인증 등

모바일 OTP를 이용한 Offline 로그인 기능 제공