nurit

정보자산의 보안강화를 위하여 다계층 인증을 위한

BaroPAM 솔루션 적용 모습

2025. 5.

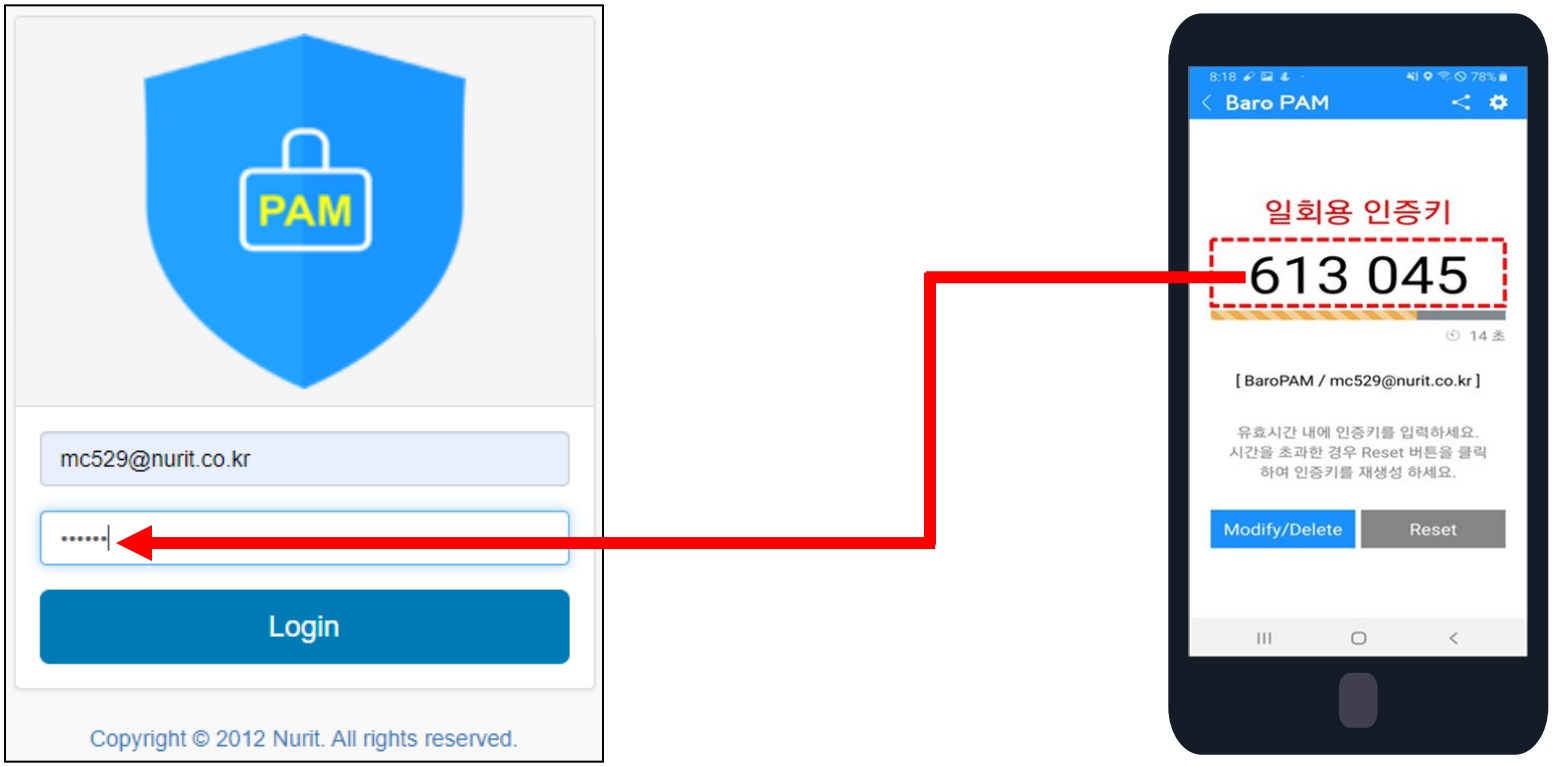
PAM

1등급 GOOD Software

별첨. 적용 모습

1. 애플리케이션 로그인

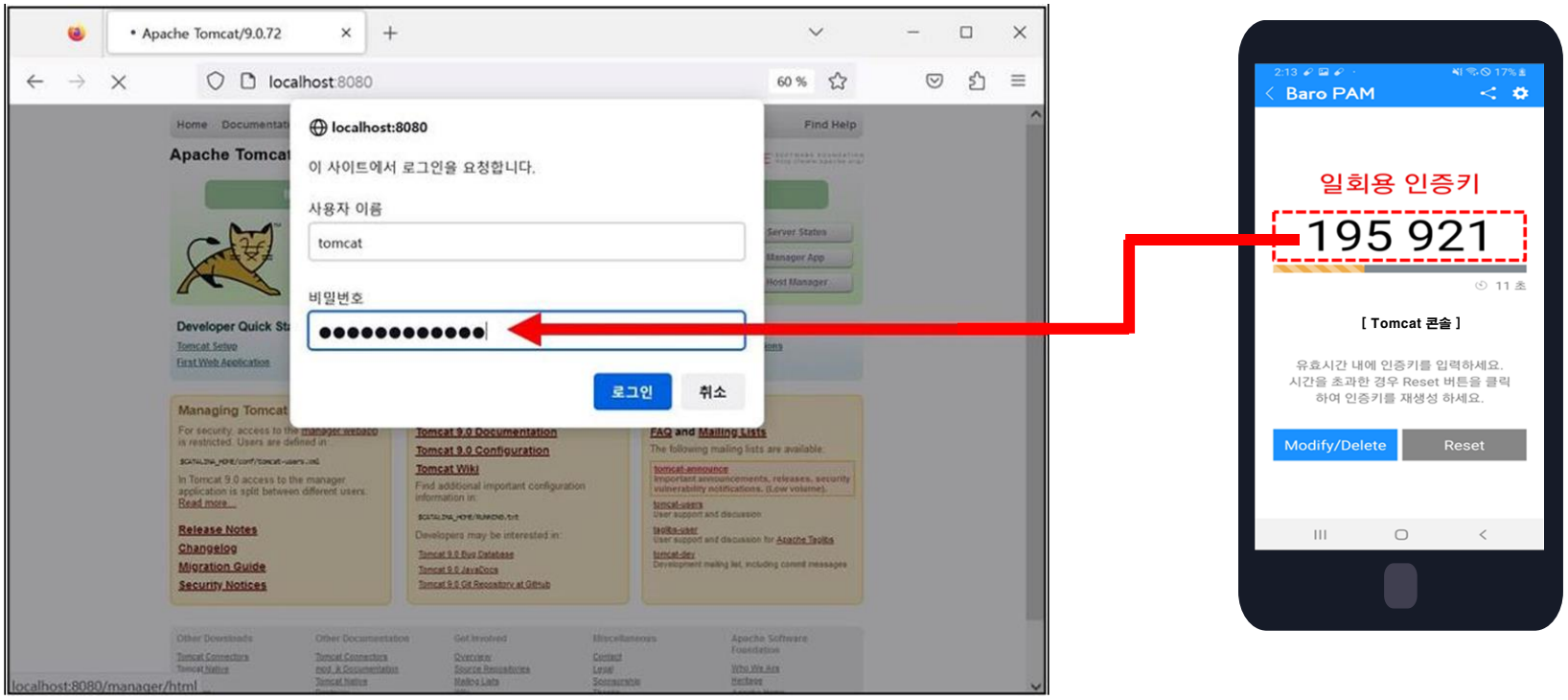
ERP/그룹웨어/전자결재/포탈 등의 애플리케이션 로그인 시 보안 강화를 위한 사용자 식별.인증을 위하여 로그인-ID를 입력한 후 BaroPAM 앱에서 일회용 인증키를 생성합니다. 생성한 일회용 인증키를 입력한 후 로그인 버튼을 클릭하여 애플리케이션에 로그인 합니다.



별첨. 적용 모습

2. WAS 콘솔 로그인

Weblogic, JEUS, Tomcat 등과 같은 WAS(Web Application Server) 콘솔의 로그인 시 보안의 취약점을 개선하기 위한 사용자 식별 · 인증을 위하여 BaroPAM을 적용하여 보안을 강화 합니다.

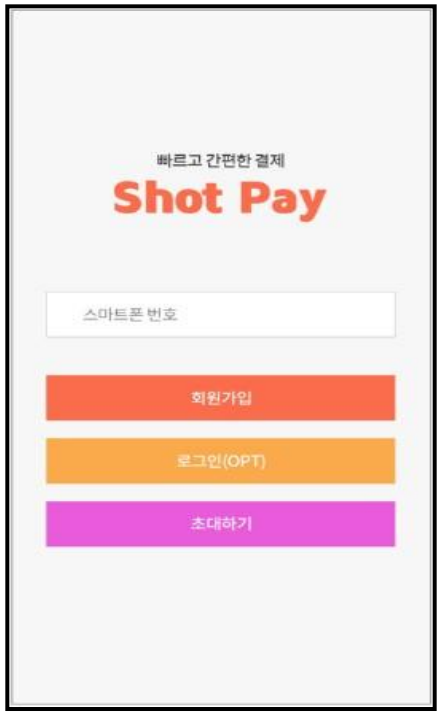


WAS 콘솔 로그인 화면에서 암호를 먼저 입력하고 공백 없이 이어서 일회용 인증키를 입력하면 됩니다. 예를 들어, 암호가 "tomcat" 이고, 일회용 인증키가 "195921" 이라면 "tomcat195921"으로 입력하면 됩니다.

별첨. 적용 모습

3. 간편결제 / 계좌이체 인증 (핀테크)

간편결제 및 계좌이체 시 앱에서 **OTP번호생성** 버튼을 클릭합니다. 생성한 **OTP번호**는 앱에 표시되며 결제버튼을 클릭하여 결제하여 보안을 강화 합니다.



카드결제 시 OTP 생성 규칙 = 카드번호 + 결제금액 + 고유번호
계좌이체 시 OTP 생성 규칙 = 계좌번호 + 이체금액 + 고유번호

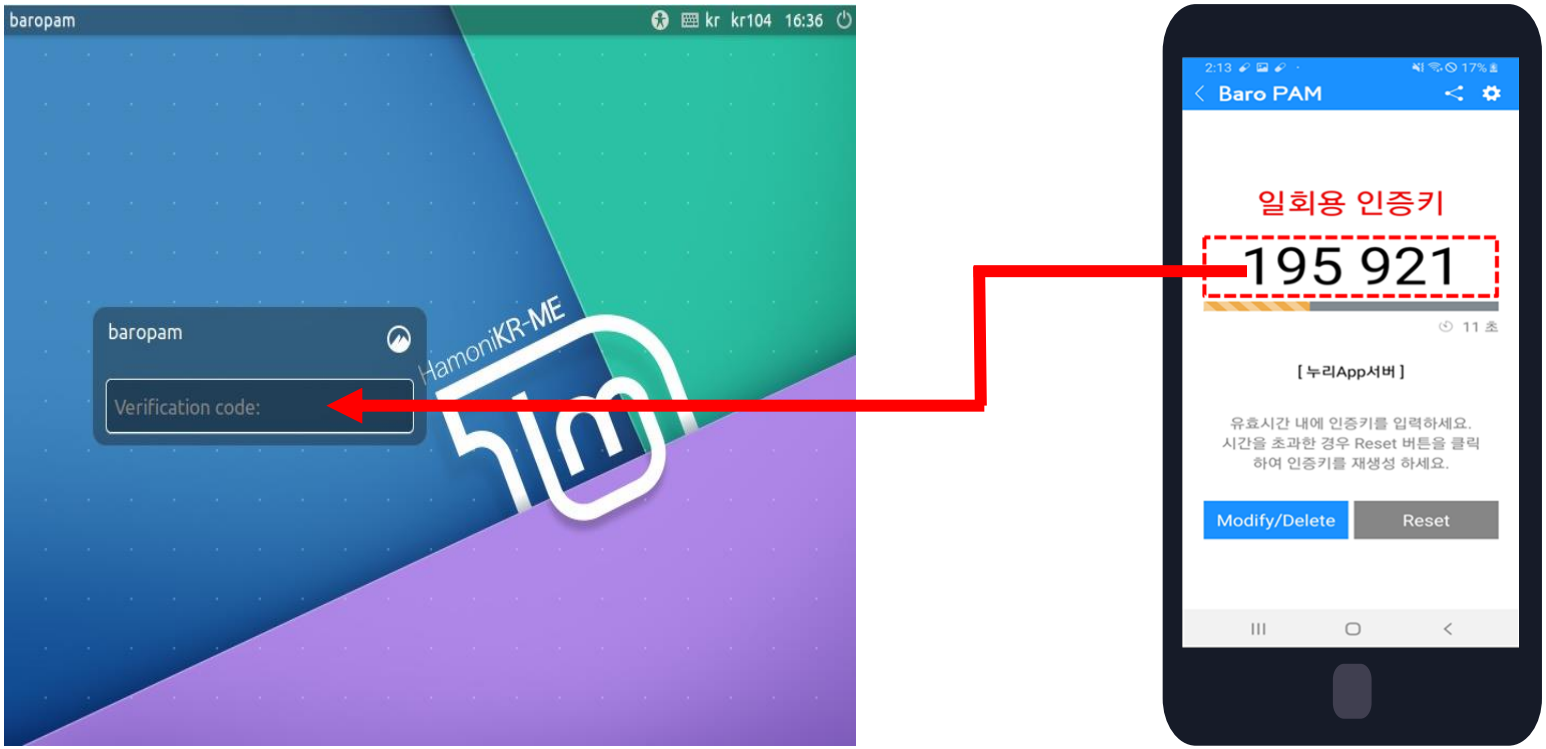
→ 서버에서 OTP 검증을 통해서 결제/이체 정보의 위변조 여부를 확인.

nurit

별첨. 적용 모습

4. 개방형OS 로그인 (하모니카OS / 구름OS)

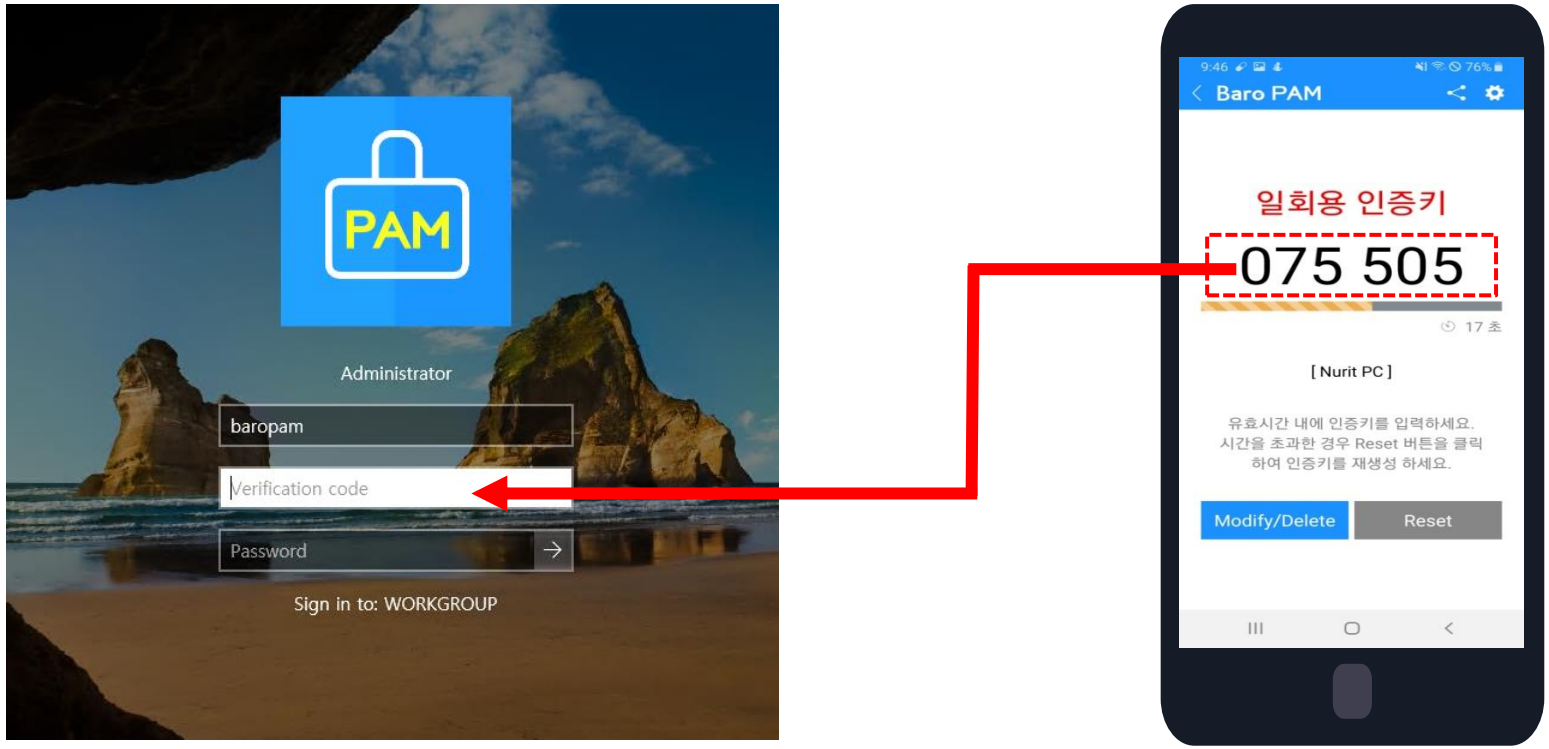
Windows 환경을 대체 및 보안에 강한 국산 OS인 개방형OS에 로그인 시 보안 강화를 위한 사용자 식별.인증을 위하여 로그인-ID를 입력한 후 BaroPAM 앱에서 일회용 인증키를 생성합니다. 생성한 일회용 인증키를 입력한 후 로그인 버튼을 클릭하여 로그인 합니다.



별첨. 적용 모습

5. Windows 로그온

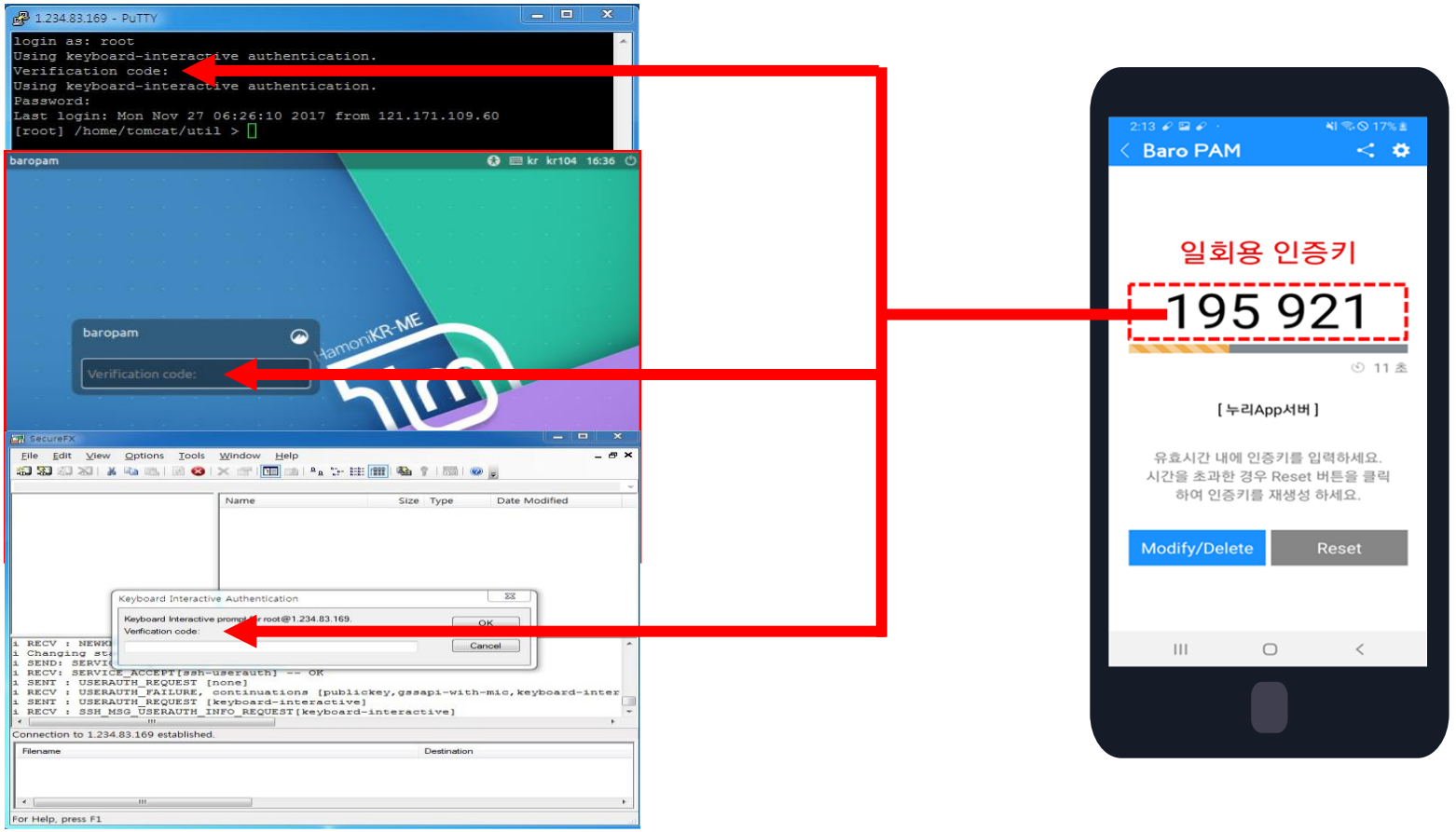
Windows 로그온 시 보안 강화를 위한 사용자 식별.인증을 위하여 BaroPAM 앱에서 일회용 인증키를 생성합니다.
생성한 일회용 인증키와 비밀번호를 입력한 후 로그온 버튼을 클릭하여 Windows에 로그온하여 보안을 강화 합니다.



별첨. 적용 모습

6. Linux / Unix 로그인

Linux / Unix 환경에 로그인 시 보안 강화를 위한 사용자 식별.인증을 위하여 로그인-ID를 입력한 후 BaroPAM 앱에서 일회용 인증키를 생성합니다. 생성한 일회용 인증키를 입력한 후 로그인 버튼을 클릭하여 로그인 함으로써 보안을 강화 합니다.

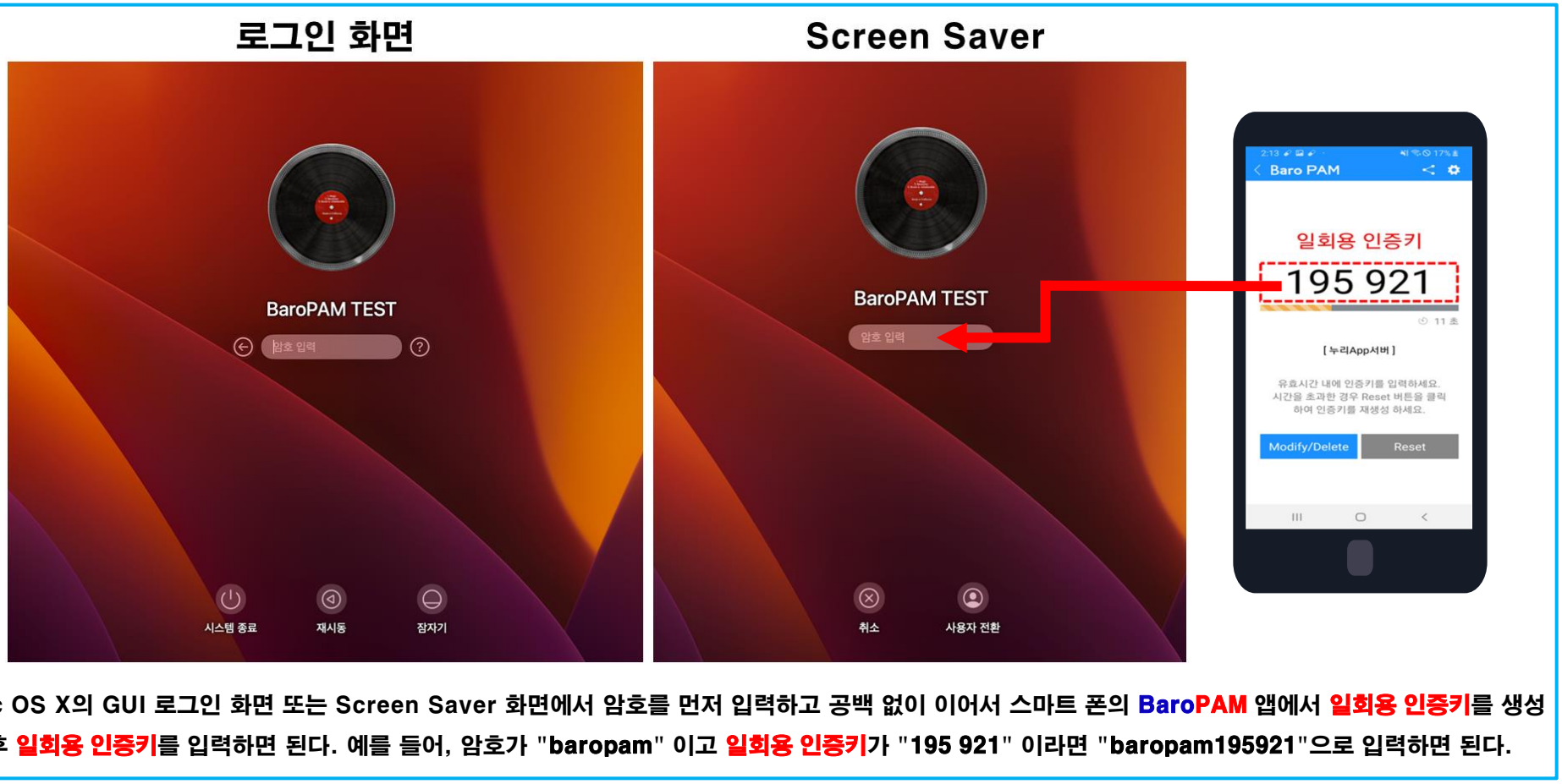


nurit

별첨. 적용 모습

7. MacOS 로그인

MacOS 환경에 로그인 시 보안 강화를 위한 사용자 식별.인증을 위하여 로그인-ID를 입력한 후 BaroPAM 앱에서 일회용 인증키를 생성합니다. 생성한 일회용 인증키를 입력한 후 로그인 버튼을 클릭하여 로그인 함으로써 보안을 강화 합니다.

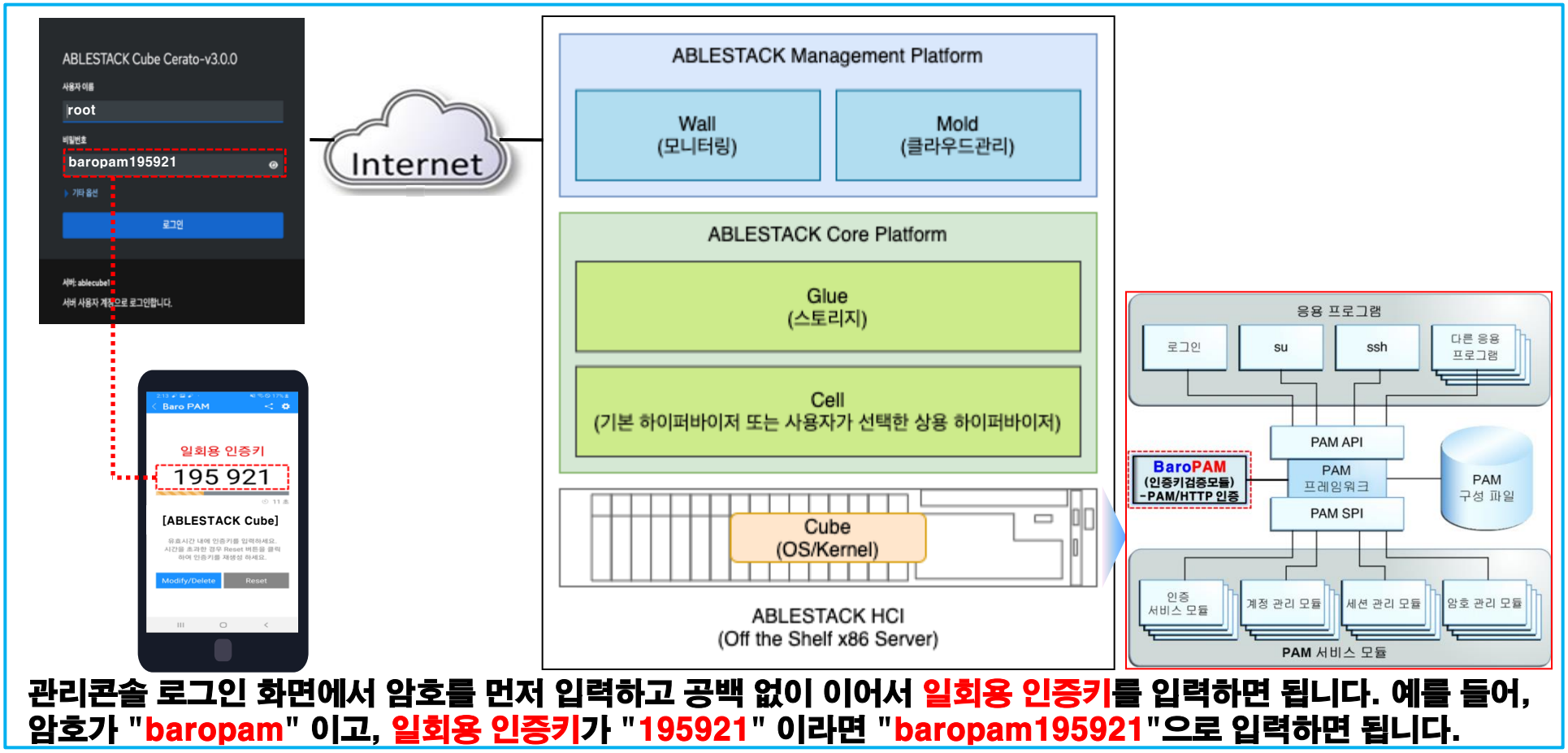


Mac OS X의 GUI 로그인 화면 또는 Screen Saver 화면에서 암호를 먼저 입력하고 공백 없이 이어서 스마트 폰의 BaroPAM 앱에서 일회용 인증키를 생성한 후 일회용 인증키를 입력하면 된다. 예를 들어, 암호가 "baropam" 이고 일회용 인증키가 "195 921" 이라면 "baropam195921"으로 입력하면 된다.

별첨. 적용 모습

8. ABLESTACK Cube 관리콘솔 로그인

ABLESTACK Cube 관리콘솔의 로그인 시 보안의 취약점을 개선하기 위한 사용자 식별 · 인증을 위하여 BaroPAM을 적용하여 보안을 강화 합니다. (Cube는 엔터프라이즈 환경에서 안정적인 운영 환경을 제공하기 위해 Enterprise Linux OS의 다운스트림인 CentOS를 기반으로 BaroPAM 손쉽게 적용 가능)

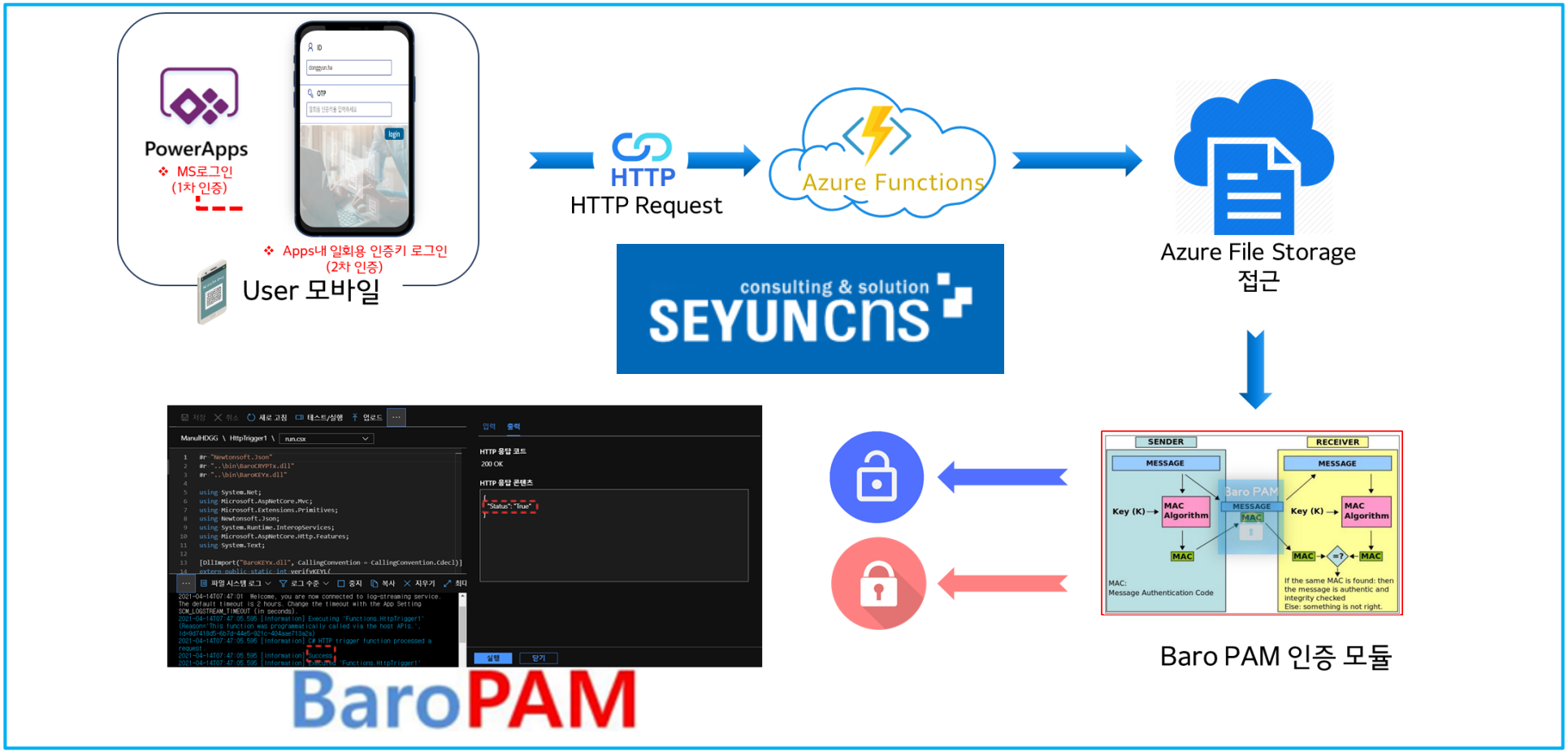


관리콘솔 로그인 화면에서 암호를 먼저 입력하고 공백 없이 이어서 일회용 인증키를 입력하면 됩니다. 예를 들어, 암호가 "baropam" 이고, 일회용 인증키가 "195921" 이라면 "baropam195921"으로 입력하면 됩니다.

별첨. 적용 모습

9. MS Azure 환경과 융합

MS Azure(Function, File Storage) 환경을 활용해 User 모바일 환경에서 Power Apps 를 활용하여 보안 강화를 위한 사용자 식별.인증을 위하여 2차 인증까지 진행한 내용을 HTTP Request 를 통해 Azure 환경에 접근해 BaroPAM 인증을 진행하여 보안을 강화 합니다.

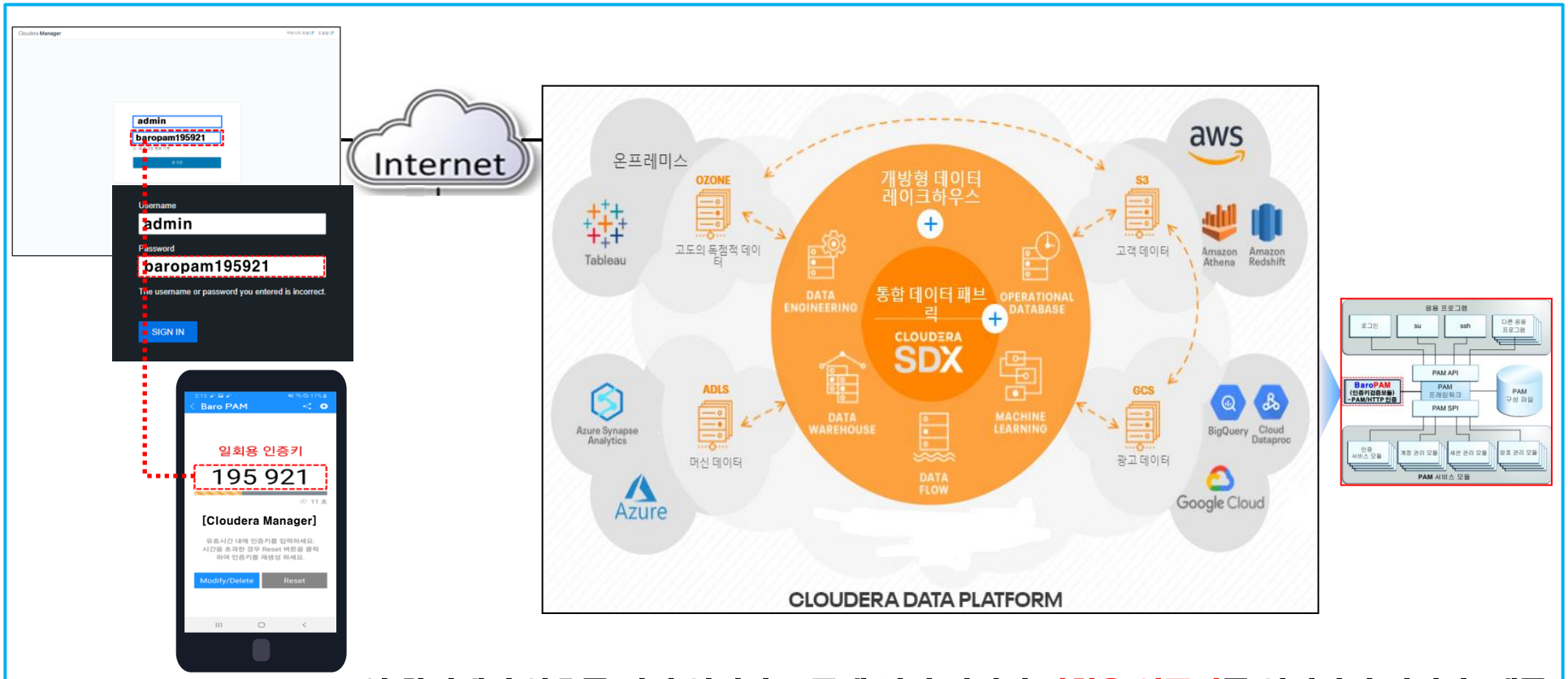


nurit

별첨. 적용 모습

10. Cloudera Data Platform의 Cloudera Manager 로그인

CDP(Cloudera Data Platform)는 데이터의 위치에 관계없이 데이터 센터와 여러 데이터 클라우드 간에 데이터, 애플리케이션, 사용자를 양방향으로 안전하게 이동할 수 있는 자유를 제공하는 솔루션으로, Cloudera Manager로 그인 시 보안의 취약점을 개선하기 위한 **사용자 식별 · 인증**을 위하여 **BaroPAM**을 적용하여 보안을 강화 합니다.



Cloudera Manager 로그인 화면에서 암호를 먼저 입력하고 공백 없이 이어서 **일회용 인증키**를 입력하면 됩니다. 예를 들어, 암호가 "**baropam**" 이고, **일회용 인증키**가 "**195921**" 이라면 "**baropam195921**"으로 입력하면 됩니다.

nurit

별첨. 적용 모습

11. SSO(Single Sign On) 솔루션과 융합

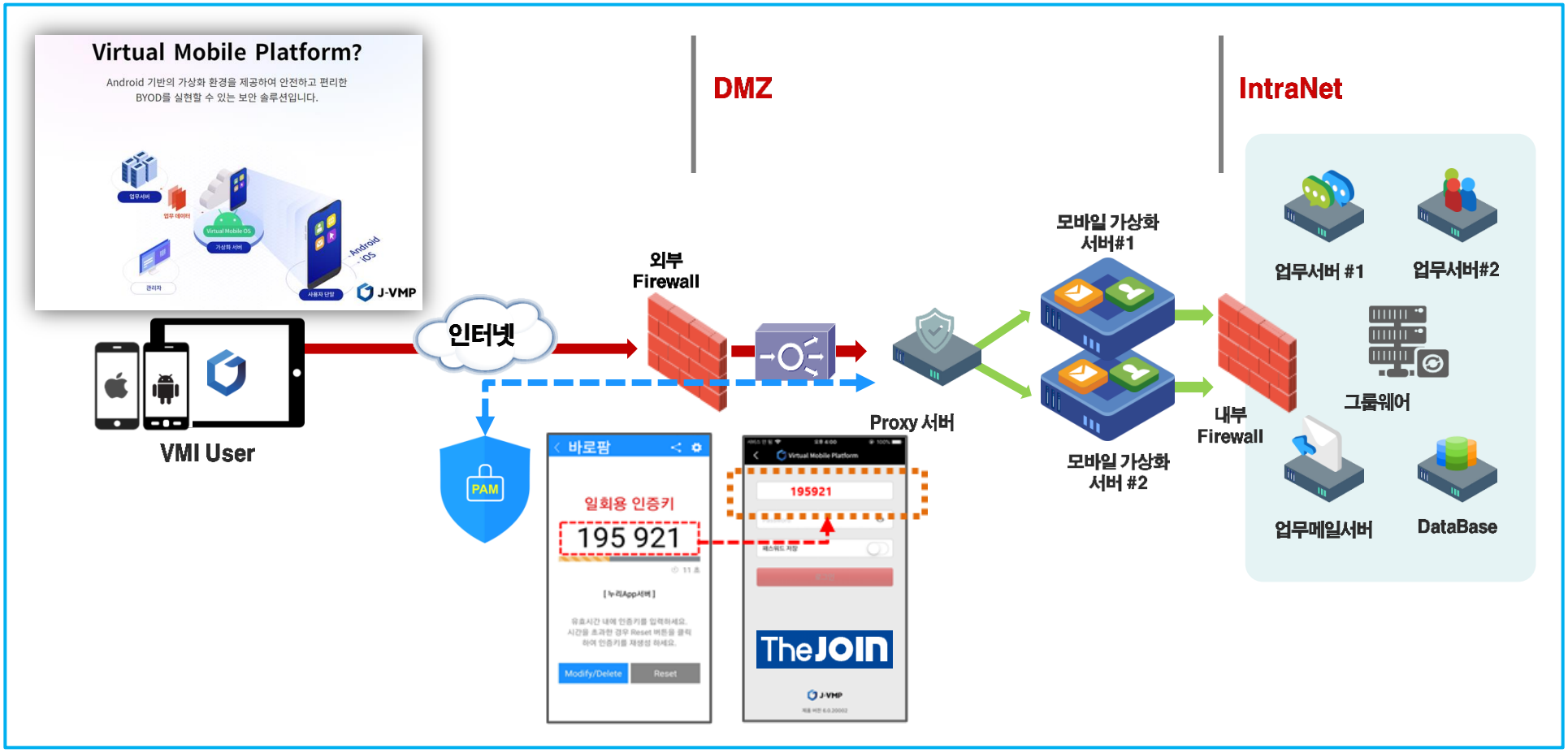
SSO(Single Sign On)는 1회 인증으로 여러 시스템을 이용할 수 있는 통합인증 기능으로 단일화된 ID로 SSO로그인시 각 업무시스템을 별도의 인증절차 없이 권한에 따라 차등적, 선별적으로 각 시스템에 접근할 수 있는 환경을 제공하는 솔루션에 **사용자 식별 · 인증**을 위하여 **BaroPAM**을 적용하여 보안을 강화 합니다.

nurit

별첨. 적용 모습

12. VMI(Virtual Mobile Infrastructure : 모바일 가상화) 솔루션 적용

모바일 가상화 플랫폼(VMI)은 서버에 있는 모바일 가상(개인사용자)영역에 접근하여, 개인 모바일 영역과 물리적으로 완전히 분리된 모바일 업무환경을 제공하는 플랫폼으로 보안 강화를 위한 사용자 식별 · 인증을 위하여 BaroPAM을 적용하여 보안을 강화 합니다.

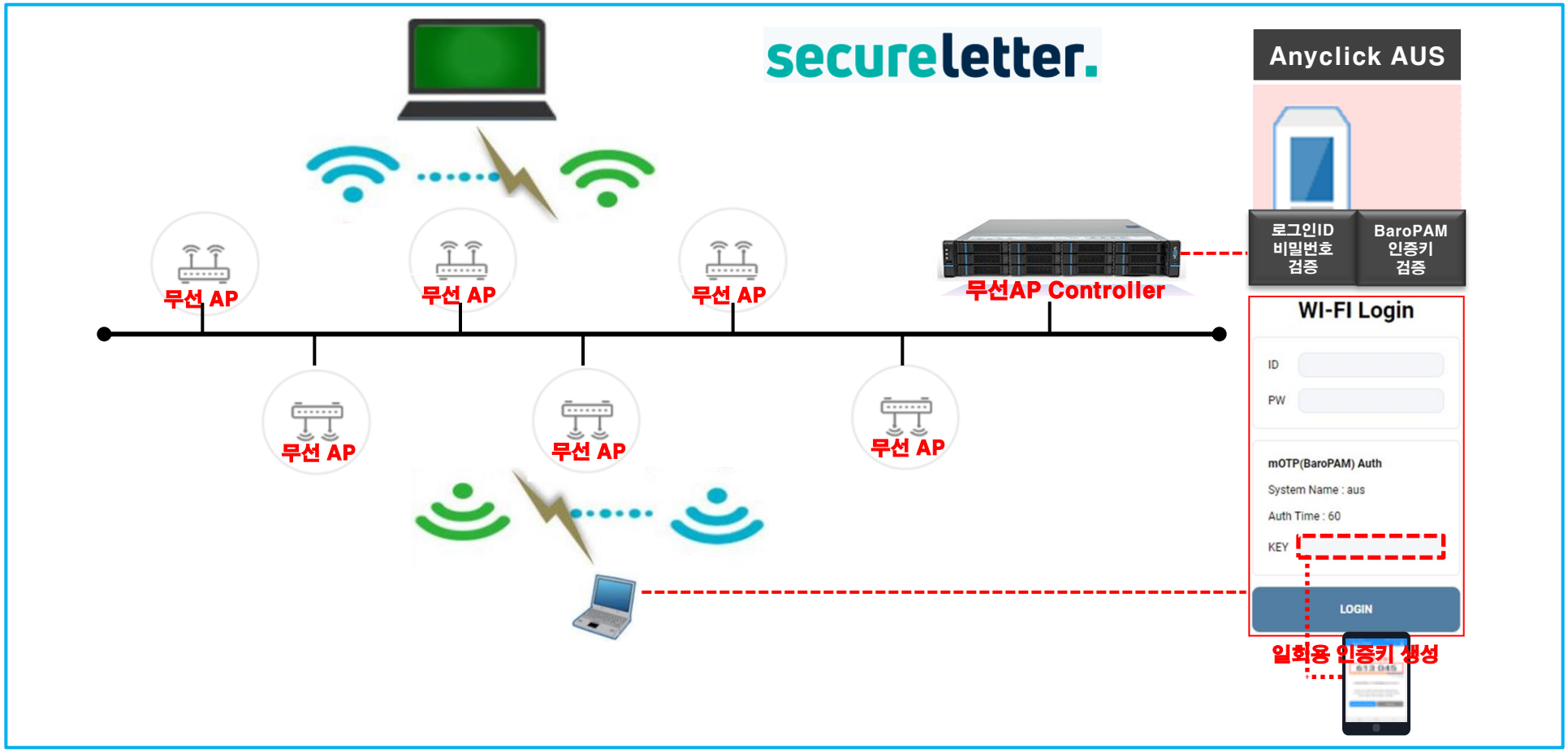


nurit

별첨. 적용 모습

13. 무선AP 솔루션과 융합

무선 액세스 포인트(WAP)는 일명 무선AP라 불리며, 컴퓨터 네트워크에서 와이파이를 이용한 관련 표준을 이용하여 무선 장치들을 유선 장치에 연결할 수 있게 하는 장치로 유선 LAN 기반의 업무환경을 5G 기반 모바일 환경으로 전환하기 위해서는 보안 강화를 위한 무선 사용자 식별 · 인증을 위하여 BaroPAM을 적용하여 보안을 강화 합니다.

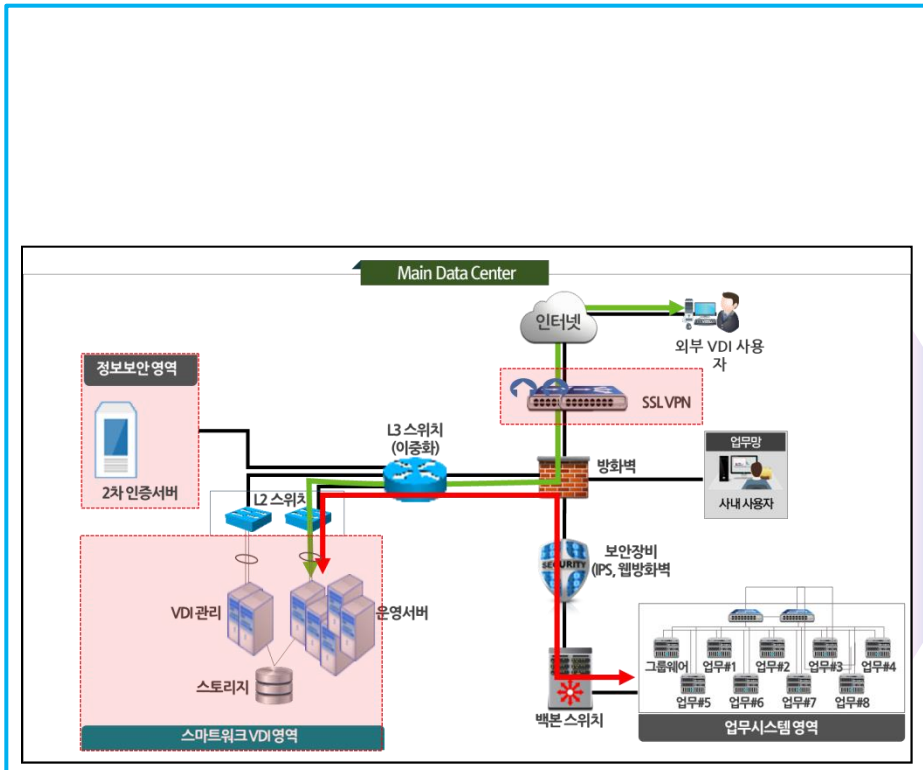


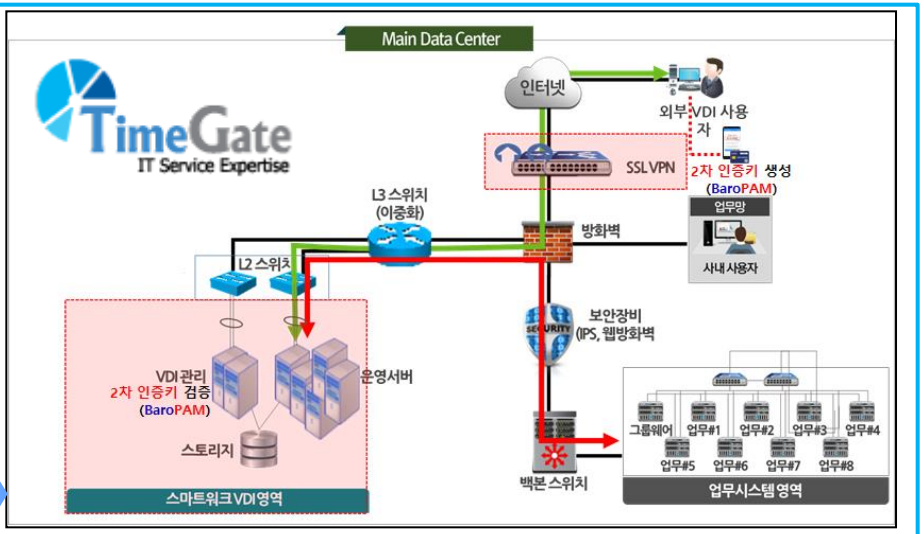
nurit

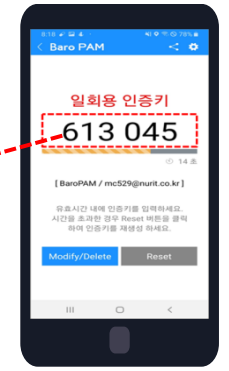
별첨. 적용 모습

14. VDI(Virtual Desktop Infrastructure) 솔루션과 융합

VDI(Virtual Desktop Infrastructure)는 소프트웨어를 이용해 데스크탑을 가상화하고 , 이를 중앙에서 사용자 환경으로 제공하는 솔루션에 보안 강화를 위한 사용자 식별 · 인증을 위하여 BaroPAM을 적용하여 보안을 강화 합니다.





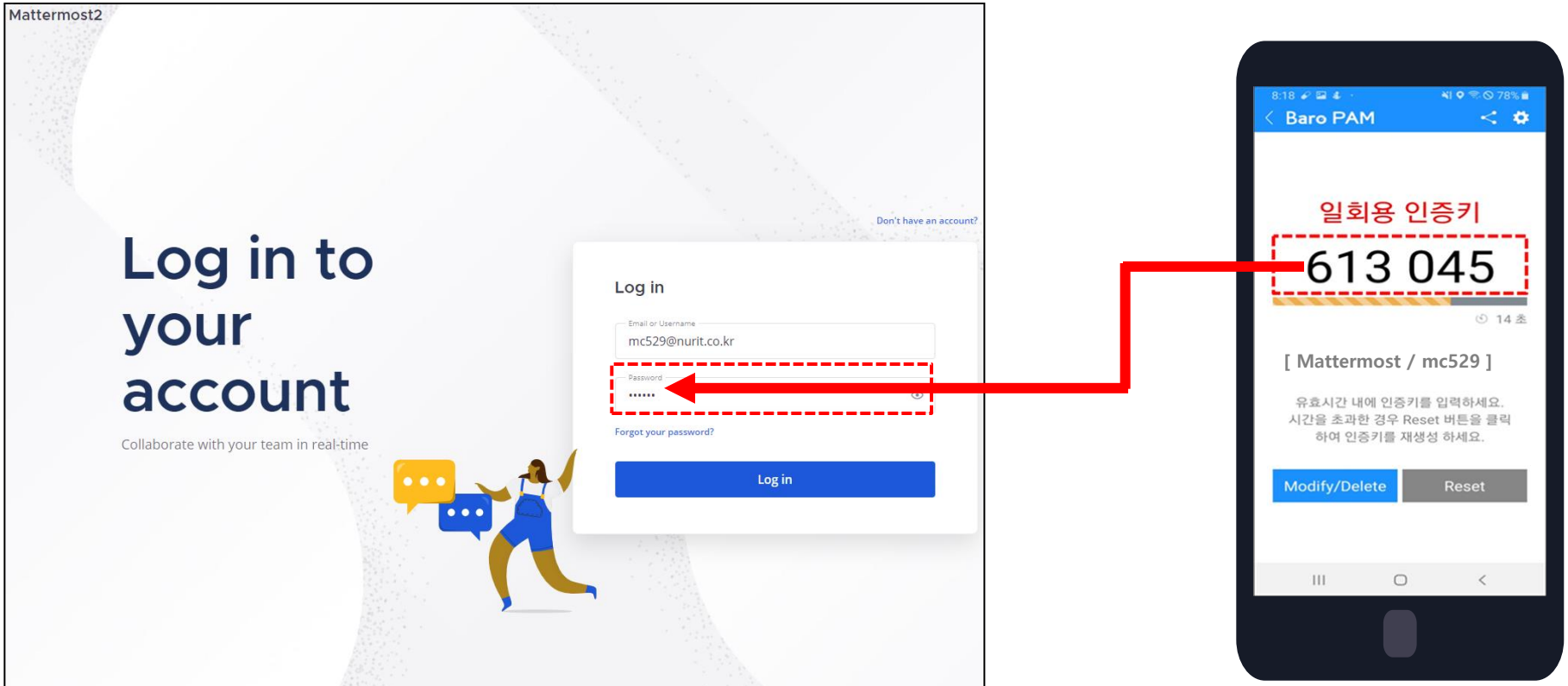


nurit

별첨. 적용 모습

15. Mattermost 솔루션과 융합

Mattermost는 파일 공유, 검색, 통합 기능을 제공하는 오픈 소스로 셀프 호스팅이 가능한 온라인 채팅 서비스로 단체와 기업을 위한 내부 채팅으로 설계되어 있으며, 대부분 그 자체를 슬랙과 마이크로소프트 팀즈의 오픈 소스 대안으로 보안 강화를 위한 사용자 식별 · 인증을 위하여 BaroPAM을 적용하여 보안을 강화 합니다.

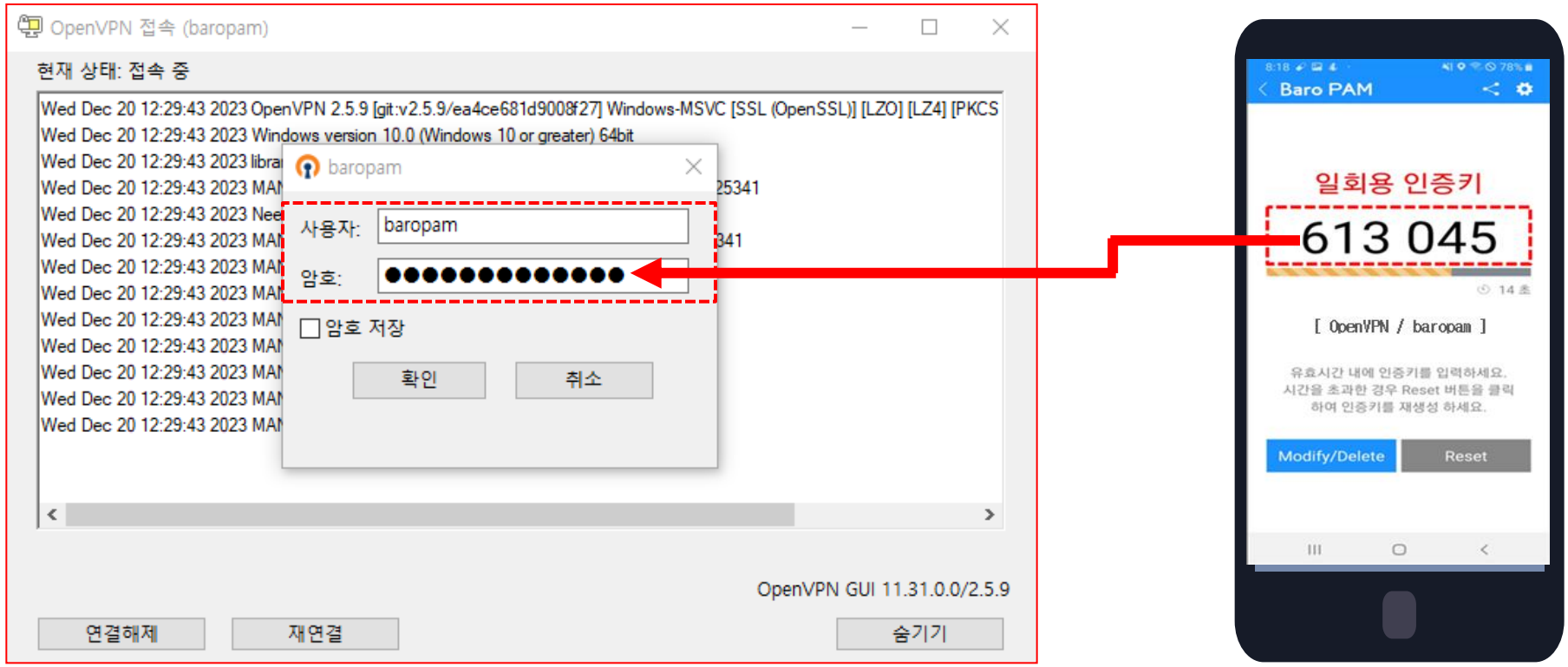


nurit

별첨. 적용 모습

16. OpenVPN 솔루션과 융합

가상 사설망(VPN, Virtual Private Network)는 별도의 사설 전용망 없이도 암호 기술에 기반한 터널링(tunneling) 프로토콜(통신규약)을 이용해 지점간을 연결함으로써, 저렴한 비용으로 원거리 통신망(WAN)을 구축할 수 있는 네트워크 솔루션으로 보안 강화를 위한 **사용자 식별 · 인증**을 위하여 **BaroPAM**을 적용하여 보안을 강화 합니다.



VPN 로그인 화면에서 암호를 먼저 입력하고 공백 없이 이어서 **일회용 인증키**를 입력하면 됩니다. 예를 들어, 암호가 "**nurit**" 이고, **일회용 인증키**가 "**613045**" 이라면 "**nurit613045**"으로 입력하면 됩니다.

별첨. 적용 모습

17. RADIUS 솔루션과 융합

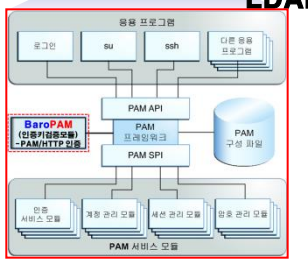
RADIUS(Remote Authentication Dial In User Service)는 네트워킹 프로토콜로 사용자가 네트워크에 연결하고 네트워크 서비스를 받기 위한 중앙 집중화된 인증으로 보안 강화를 위한 사용자 식별 · 인증을 위하여 BaroPAM을 적용하여 보안을 강화 합니다.

SOPHOS
NGF XG 방화벽

Radius:UDP 1812

Sophos SSLVPN Client

RADIUS인증
-PAM인증
-SQL인증
-HTTP인증
-AD인증
-LDAP인증



FreeRADIUS

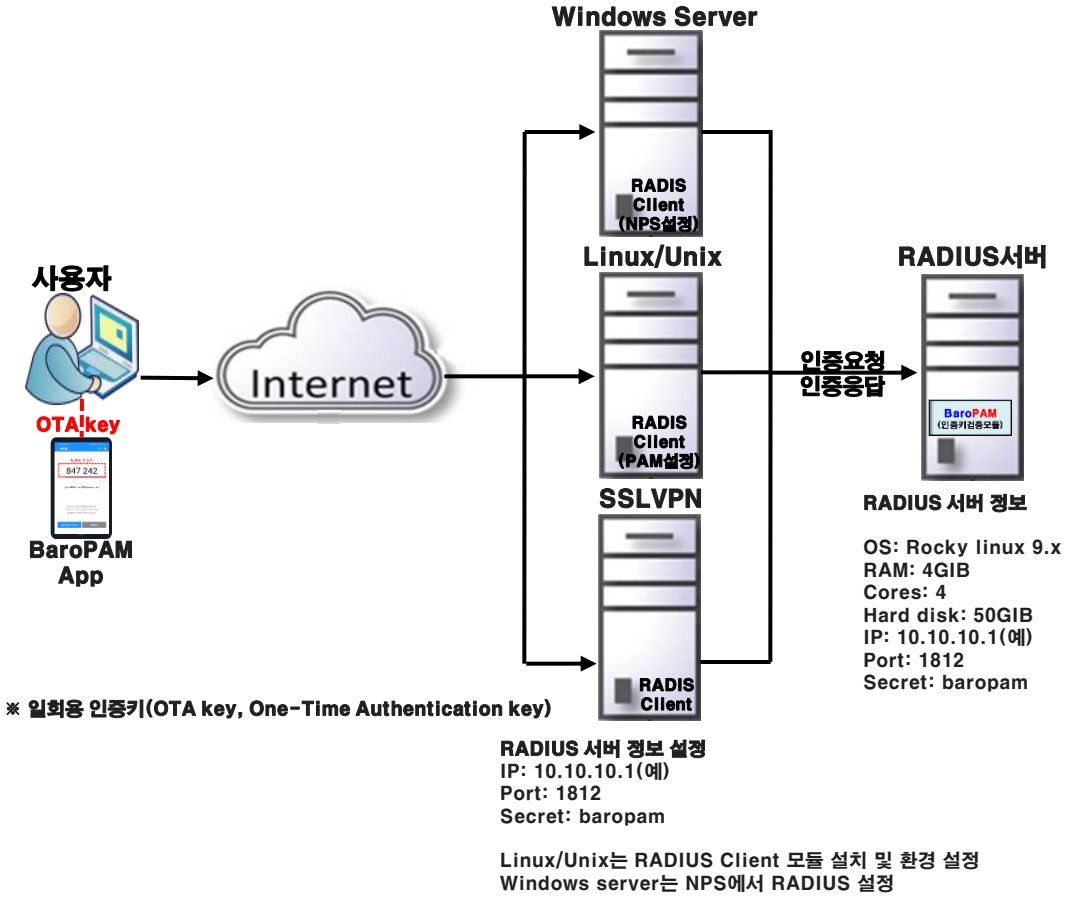
※ RADIUS는 무선AP, VPN 등의 네트워크 장비, Database, VMWare 등의 인증을 지원.

nurit

별첨. 적용 모습

18. RADIUS 연동한 통합계정/인증관리

RADIUS(Remote Authentication Dial In User Service)는 네트워킹 프로토콜로 사용자가 네트워크에 연결하고 네트워크 서비스를 받기 위한 중앙 집중화된 인증으로 보안 강화를 위한 통합 계정관리 및 통합인증을 위하여 BaroPAM을 적용하여 보안을 강화 합니다.



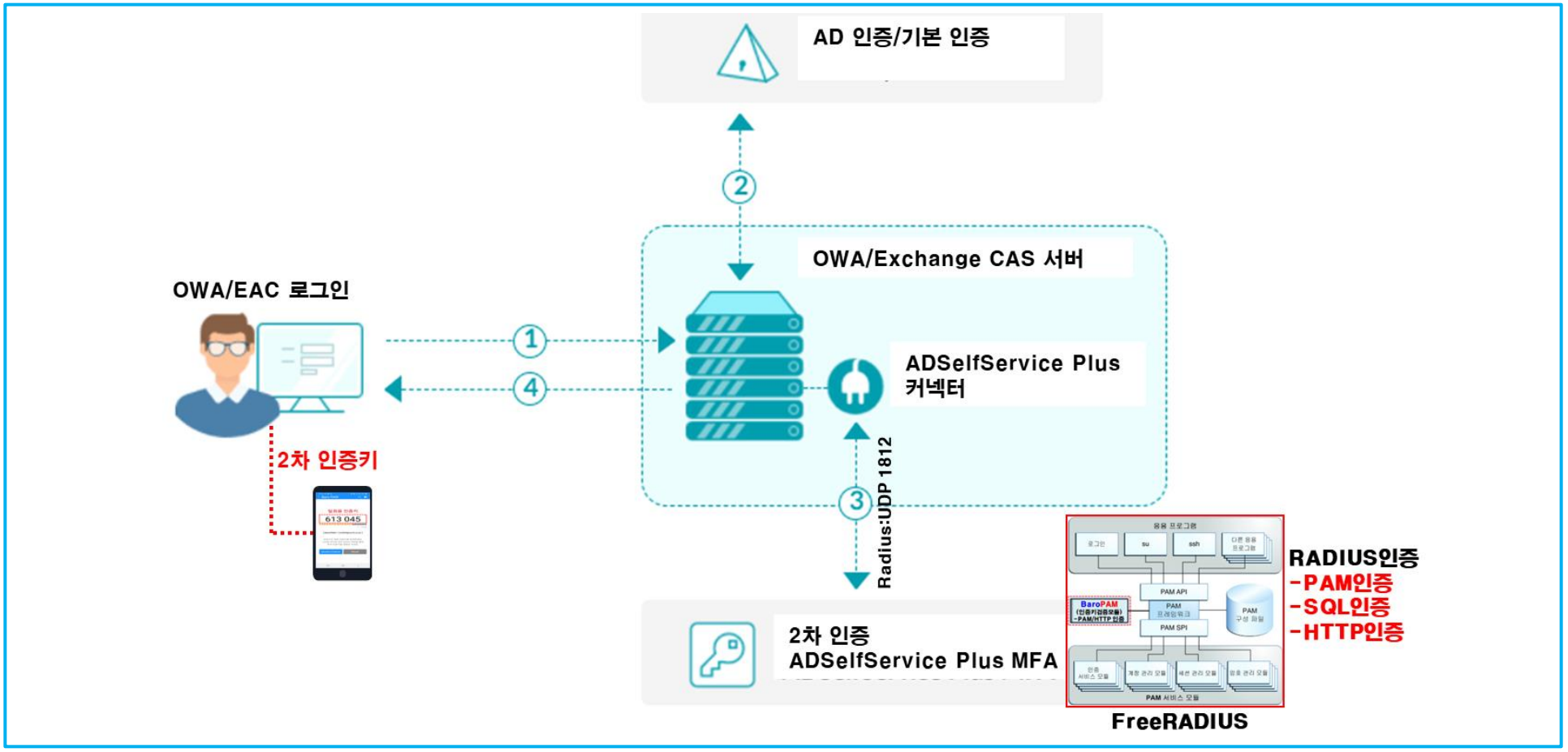
특장점

- ▶정보자산의 계정(아이디/비밀번호) 통합 관리 및 통합 인증
- ▶정보자산의 계정(아이디/비밀번호)는 OS 계정 사용
- ▶전세계적으로 인정된 512Bit 표준 Hash 함수 사용 (HMac-SHA512 / 인터넷 보안표준 IETF RFC 6238)
- ▶금융감독원에서 권장하는 시간 동기화(Time-Sync), 동적 HMac Key 방식
- ▶매번 변하거나 한번 사용하고 버리는 일회성/휘발성 같은 동적인 보안
- ▶빠른 인증속도로 서비스 보장 (평균 인증시간 0.01초 이내)
- ▶인증절차 시 인증정보가 위변조 되더라도 우회인증 불가능
- ▶정보자산별 / 계정별 일회용 인증키 및 생성주기 개별부여
- ▶인증 우회(우회기술, 피로공격 등) 및 MFA 피로 공격 (fatigue attacks) 불가능
- ▶자동 로그인 기능을 악용한 계정 정보 탈취해도 로그인 불가능
- ▶인증의 제한 횟수 및 제한 시간(예: 30초에 3회) 설정 기능 제공
- ▶중간자(man-in-the-middle) 공격을 예방하는 기능 제공
- ▶2차 인증에서 허용 / 제외할 수 있는 계정에 대한 ACL 기능 제공

별첨. 적용 모습

19. OWA(Outlook Web Access) 솔루션과 융합

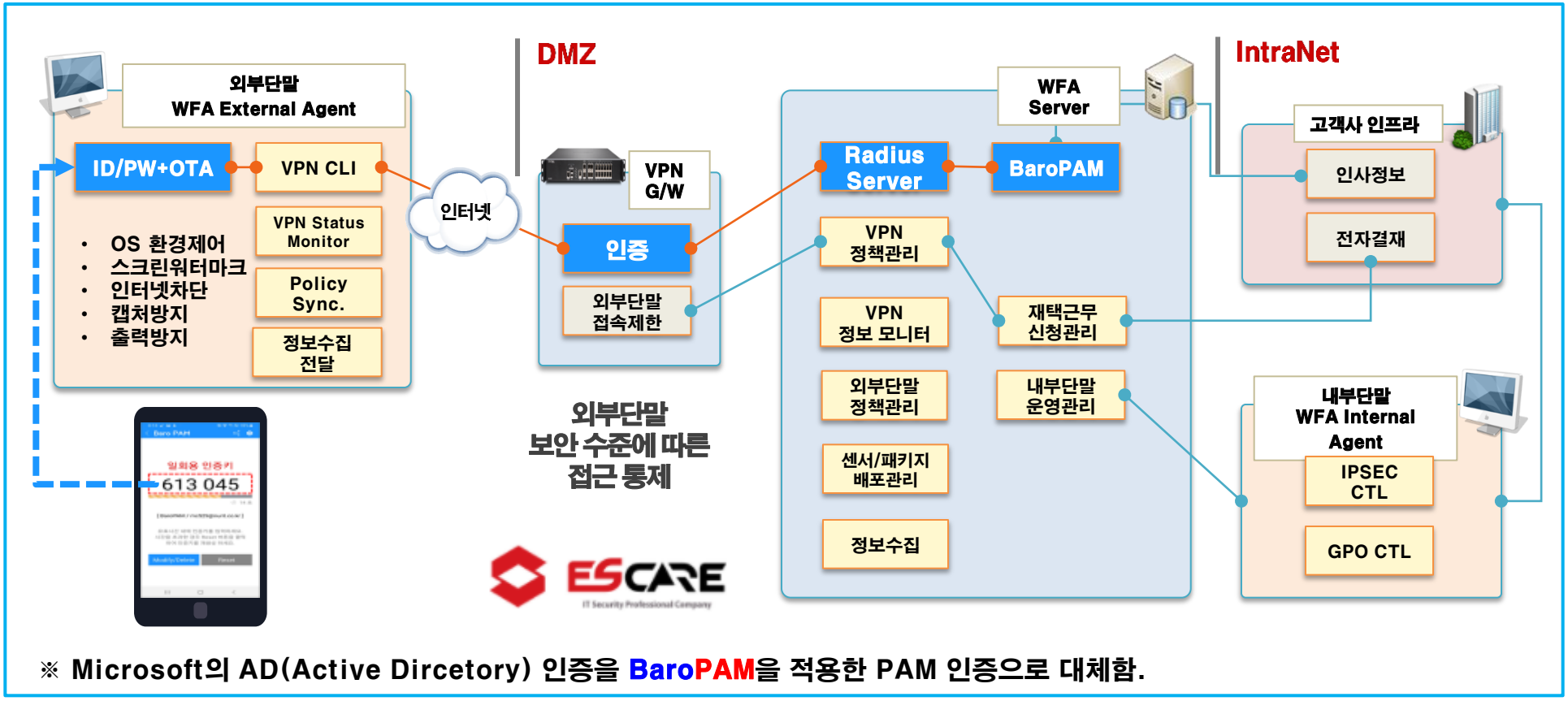
웹용 Outlook 또는 OWA(Outlook Web Access)는 온-프레미스 전자 메일 및 작업 관리 응용 프로그램인 Microsoft Outlook에 대응하는 브라우저 기반으로 민감한 비즈니스 정보와 사용자 간의 기밀 이메일 서신이 노출 될 위험의 보안 강화를 위한 사용자 식별 · 인증을 위하여 BaroPAM을 적용하여 보안을 강화 합니다.



별첨. 적용 모습

20. WFA(Work From Anywhere : 재택근무) 솔루션과 융합

재택근무솔루션(WFA)은 외부사용자 단말이 내부로 접속하여 업무를 해야 하는 환경에 대한 단말 무결성 검증 및 단말 상태에 따른 내부 접속 권한 보안체계를 적용하여 내부 접속의 보안 리스크 해소 및 단말 상태에 따른 차별화된 네트워크 접근 통제 환경을 제공하는 솔루션으로 보안 강화를 위한 내부 접근자 식별 · 인증을 위하여 BaroPAM을 적용하여 보안을 강화 합니다.



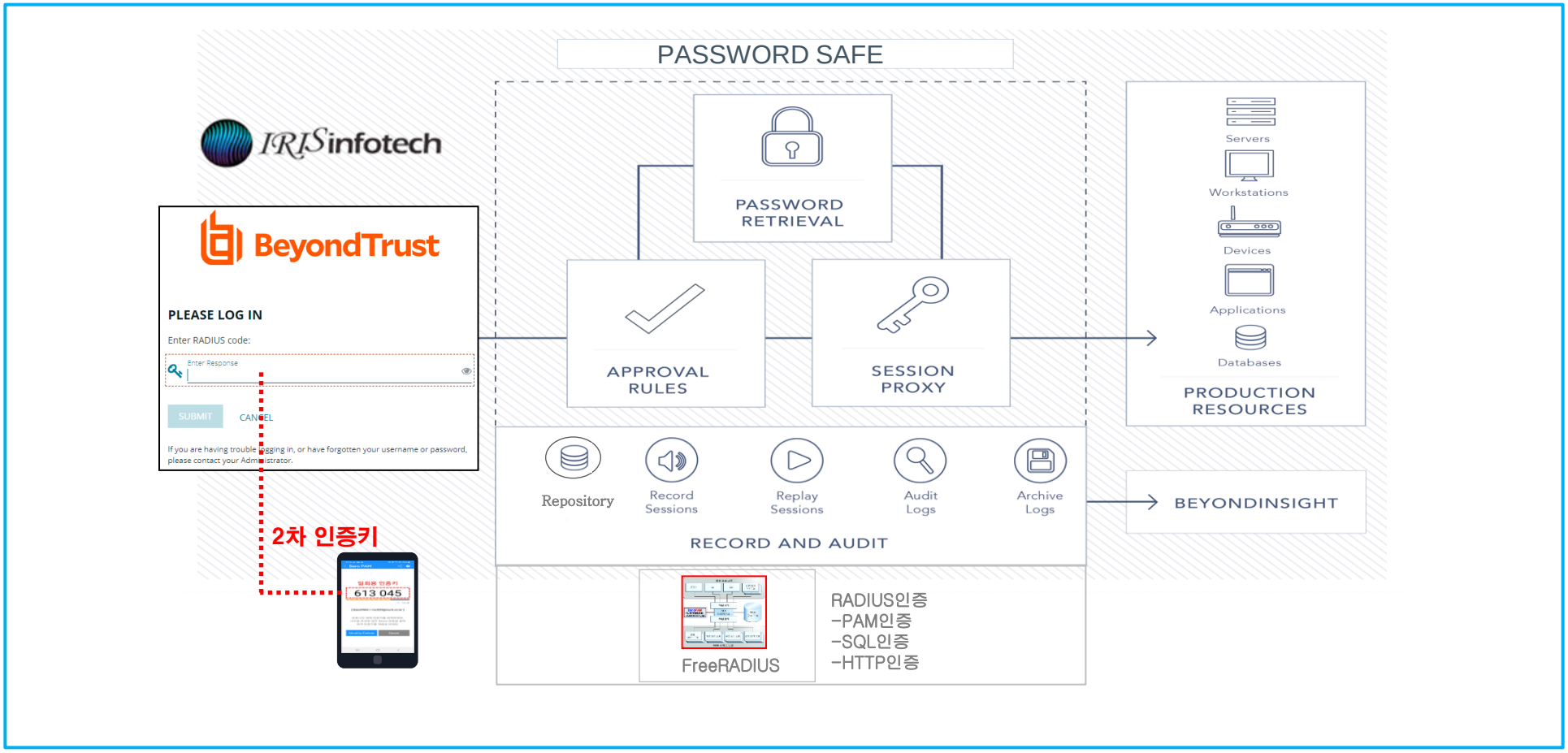
※ Microsoft의 AD(Active Dircetory) 인증을 BaroPAM을 적용한 PAM 인증으로 대체함.

nurit

별첨. 적용 모습

21. 접근제어/패스워드 관리/세션관리 솔루션과 융합

애플리케이션, 사용자 및 정보자산에 "최소 권한"만 부여하여 이를 통해 허가 받지 않은 접근을 제한하고, 접근 시도를 모니터링 분석하여 보안 침해 형태 및 유형을 감사할 수 있는 종합적인 접근제어 솔루션으로 보안 강화를 위한 사용자 식별 · 인증을 위하여 BaroPAM을 적용하여 보안을 강화 합니다.

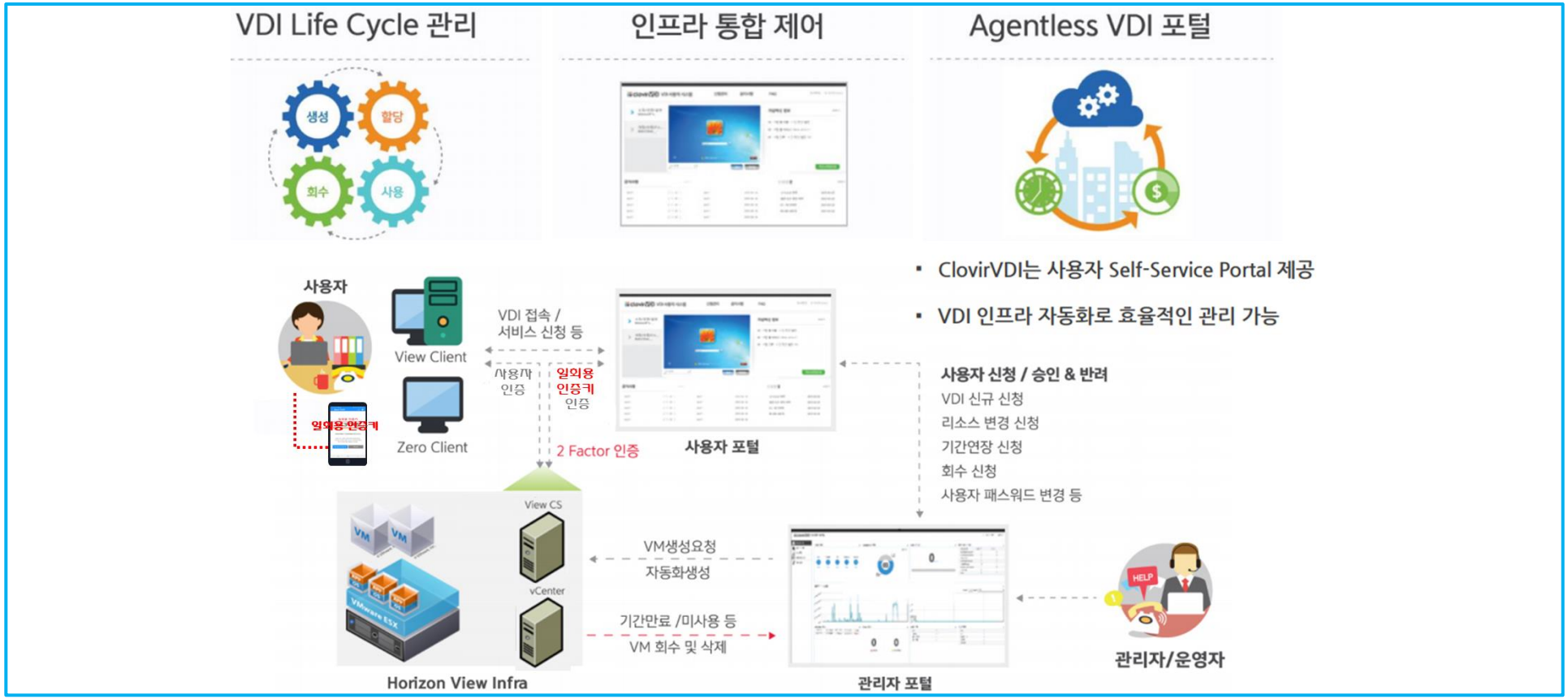


nurit

별첨. 적용 모습

22. Smart work 솔루션과 융합

Smart work은 IT를 이용해 시간과 장소에 제한 없이 업무를 볼 수 있는 유연한 근무환경으로 정보보안을 위하여 화면차단 5분, 화면보호기 10분, 강제 종료 4시간으로 설정하는 등 단말기 보안과 절전 기능을 설정하는데, 정보보안은 강화하고 사용자의 불편함을 최소화 및 사용자 식별 · 인증을 위하여 BaroPAM을 적용하여 보안을 강화 합니다.



nurit

별첨. 적용 모습

23. 서버 접근제어 솔루션과 융합

네트워크, 서버 IT 인프라 운영 시스템으로의 모든 접속과 작업을 통제 · 관리하고, 작업 내역에 대한 실시간 모니터링과 로그 기록 저장으로 **사용자에 대한 철저한 통제와 감독하는 서버접근통제 솔루션**과 정보자산의 **다계층 인증**을 통한 **계정도용, 권한상승, 불법적인 우회/원격 접속, 중간자 공격 등을 차단하는 BaroPAM 솔루션이 결합**하여 **정보자산의 보안을 강화**하는 시너지 효과를 낼 수 있습니다.

정보자산 보안 = **서버접근통제솔루션** + **다계층 인증 솔루션 (BaroPAM)**

- Windows NT Server
- Mac OS
- Linux / Unix Server
- Application
- Database
- Network, IoT Device
- 저장장치

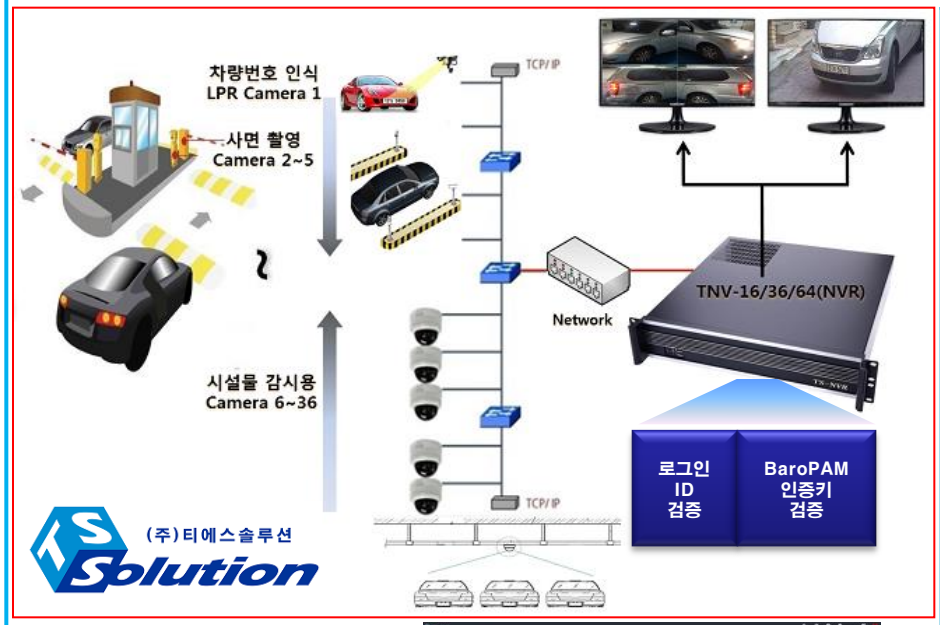
- ▶접근 권한 통제
- ▶시스템 명령어 통제
- ▶실시간 세션 통제
- ▶작업 로그 기록/ 감사

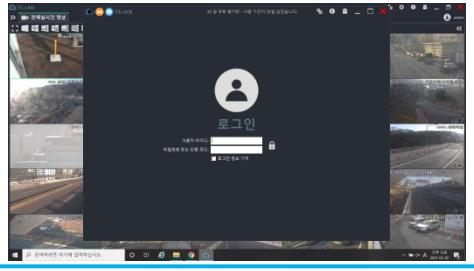
nurit

별첨. 적용 모습

24. CCTV 솔루션과 융합

지능형 CCTV란 일반 CCTV가 단순히 장면을 녹화해 보여주는 것과 다르게 장면을 녹화하면서 그 영상을 분석하는 여러 기능을 탑재한 CCTV 솔루션에 **사용자 식별 · 인증**을 위한 **BaroPAM**을 적용하여 보안을 강화 합니다.





문제점 /개선점

- 공공기관 CCTV 관리기관 대상으로 비밀번호 변경지시
  - CCTV 제품의 경우 기본 비밀번호를 그대로 사용
  - 인터넷을 통해 CCTV에 쉽게 접근하여 내부망 접근가능
- CCTV 관제 센타의 경우 수백, 수천 개의 CCTV 보유 중
  - 저장된 CCTV 영상을 민간업체에 위탁
  - 수동으로 수많은 CCTV의 관리 불가능 (일회용 인증)
- 개인영상정보보호법 준수 및 감사대응의 필요성

- 2차 인증(추가 인증)으로 CCTV의 정보자산을 보호
- 비밀번호를 일회용 인증키로 대체하여 불법사용 방지
- 영상정보 보호대책을 수립, 운영
- 영상정보 백업 시 암복호화 적용
- IP 카메라에 2차 인증(추가 인증)을 적용하여 보안 강화

nurit

별첨. 적용 모습

24. VDI/SSO/모바일 가상화 플랫폼/무선AP/VPN/SAC/CCTV 등의 인증

VDI/SSO/모바일 가상화 플랫폼/무선AP/VPN/SAC/CCTV 등의 로그인 시 로그인-ID를 입력한 후 BaroPAM 앱에서 일회용 인증키를 생성합니다. 생성한 일회용 인증키 입력하여 사용자 식별 · 인증을 위하여 BaroPAM을 적용하여 보안을 강화 합니다.

일회용 인증키 적용 전	일회용 인증키 적용 후
❖ 정보자산별 / 계정별 고정된 비밀번호 사용	❖ 정보자산별 / 계정별 일회용 인증키 사용
❖ 비밀번호 생성 규칙 적용	❖ 해시 알고리즘(SHA512)에서 발생한 값 적용
❖ 비밀번호 정보 DB에 보관	❖ 필요시 BaroPAM 앱에서 직접 생성
❖ 암호화 기술 등을 이용한 보안 조치(단방향 암호화) 필요	❖ 암호화 기술 등을 이용한 보안 조치 불필요
❖ 유출 위험 및 피해 발생	❖ 유출 위험 및 피해 발생하지 않음
❖ 의무적으로 비밀번호 변경주기 적용	❖ 개별 인증키 생성주기(3~60초) 적용
❖ 비밀번호 증후군 / 비밀번호 리셋 증후군 호소	❖ 비밀번호 증후군 / 비밀번호 리셋 증후군 발생하지 않음

nurit

기억할 필요가 없는 비밀번호!
BaroPAM이 함께 합니다.

감사합니다!

www.nurit.co.kr

서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)
주식회사 누리아이티 대표전화 : 02-2665-0119