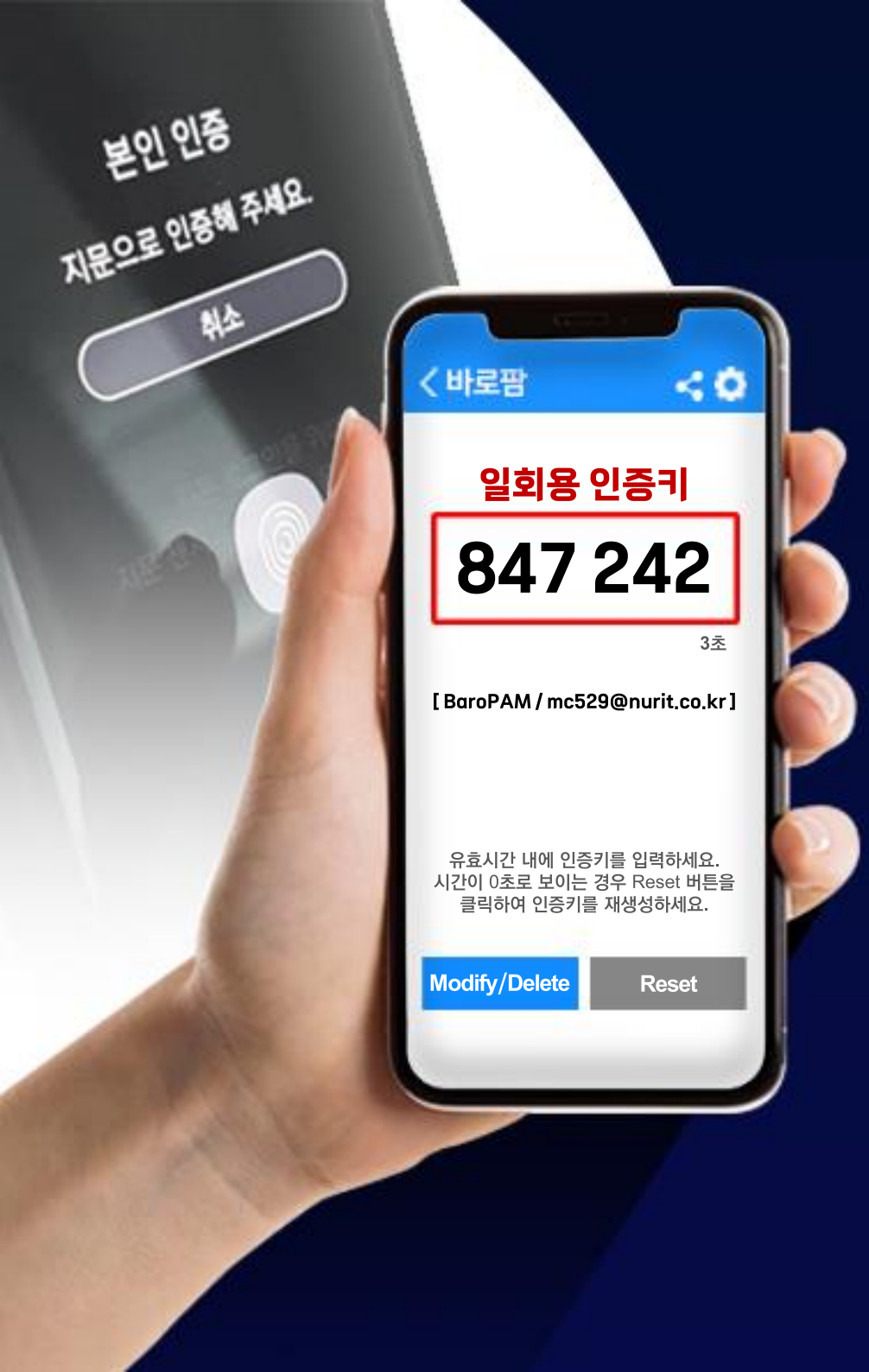
nurit

“ 정보자산의 보안강화를 위하여 다계층 인증을 위한 ”

BaroPAM 솔루션 소개서

2025.06

1등급 GOOD Software



Content

Ⅰ 배경 및 변화

Ⅱ BaroPAM

Ⅲ 기타

nurit

시작 전에

“ 기본 보안부터 ” 철저히 해야

현재의 보안체계로는
정보자산을 충분히 지킬 수 없다는 거,
보안 전문가라면 다 알고 있습니다.

주요 인프라 공격의 85%가 **패치, 2차 인증(추가 인증), 최소 권한 원칙** 등 기본적인 수준의 보안을 지키지 않아서 발생한 것으로 나타납니다.

랜섬웨어를 포함한 **침해 사고의 80~90%가 원격 접속과 관련된 문제**입니다.

보안 솔루션 중 도입해야 할 1순위가 **계정도용, 권한상승, 우회/원격접속을 차단할 수 있는 2차 인증 솔루션**입니다.

기본 보안 정책만 지켜도 대부분의 공격은 막을 수 있습니다.

또한, **망분리**는 새로울 것도, 특별할 것도 없는 보안 전략이자 개념입니다.

망분리 했다고 해커들의 침투를 100% 막을 수 없다는 걸 인정해야만 하는 때가 도래했습니다. 이 시대에는 피해를 줄이는 게 보안의 가장 큰 임무였습니다.

이게 어디까지 갔냐면, **“사이버 공격자들이 이미 네트워크에 들어와 있는 걸 상정하고 보안 전략을 마련해야 한다”**가 보안의 명제가 되었습니다.

외부의 해커 또는 내부 사용자가 불법적으로 정보자산에 접근하는 상황을 제한하고, 보안의 위험을 분산함으로써 피해를 최소화해야 합니다.

최근 들어, 중앙 집중식 관리 서버의 운영체제(OS) 및 관리자 계정이 해킹되어, 관리 서버를 장악하고 정보를 유출하여 도용 및 악용하거나, 악성코드 삽입, 정보를 삭제한 후 관리 서버를 무력화시켜 서비스를 불능 상태로 만드는 **“단일 지점 공격”**의 침해사고가 발생하여 기업에 많은 피해를 주고 있습니다.

Copyright © nurit Corp. All rights reserved.

I 배경 및 변화

1 보안 모델의 변화

AS-IS

경계보안 모델

내부 침투시 위협 내부 전파 가능

TO-BE

제로 트러스트 모델

내부 침투시에도 위협 내부 전파 불가능

- 강화된 인증
- 마이크로 세그멘테이션
- 소프트웨어 정의 경계

- 전통적인 네트워크 경계 기반 보안모델로 충분하지 않음
- 공격자가 경계를 침해한 후 내부에서 이동하는 것에 대한 한계성 내포

"절대 믿지 말고, 계속 검증하라(Never Trust, Always Verify)"

Copyright © nurit Corp. All rights reserved.

“보안 모델의 변화로 기존 보안 솔루션으로는 이젠 막을 수 없으며,”
보안 솔루션의 변화가 필요한 시점

경계보안에서
제로 트러스트 보안으로
보안모델의 변화

공격 표면으로
보안 취약점을
약용한 공격

보안 위험의
최소화하기 위한
위험 분산 필요

중앙집중식에서
벗어나
탈중앙화 필요

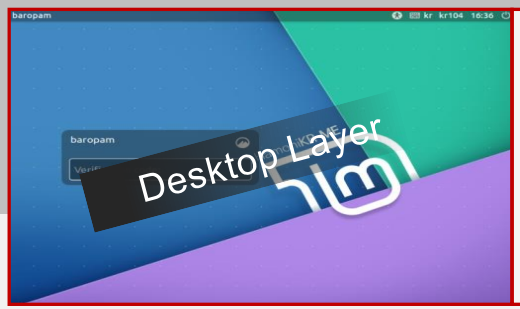
단일지점 공격으로
보안 솔루션의
무력화 차단 필요

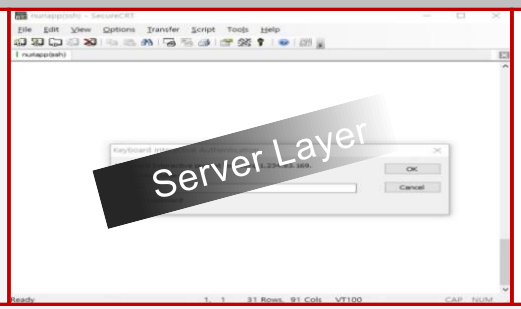
Copyright © nurit Corp. All rights reserved.

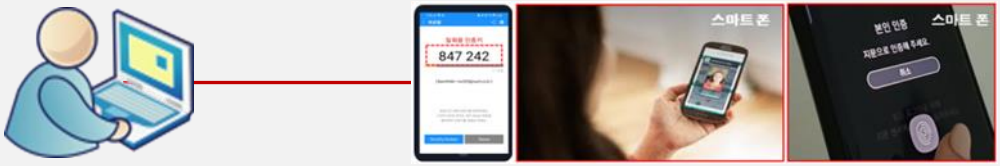
I 배경 및 변화 2 다계층 인증 체계(Multi-layer authentication system)

“ 다양한 사이버 공격에 대비하여 중앙 집중식에서 벗어나 탈중화로 각각의 컴포넌트 ”
하나하나(레이어별)를 ‘단일 지점 공격’에서 시스템을 보호하는 인증 체계
(다중 인증(MFA)은 다계층 인증 체계의 한 요소임)

Desktop/PC	Application	Server/Network 장비	Database/Storage
로그인-ID, 비밀번호 이외의 추가 인증(2차 인증) (일회용 인증키)	비밀번호 대체 또는 추가 인증(2차 인증) (일회용 인증키)	로그인-ID, 비밀번호 이외의 추가 인증(2차 인증) (일회용 인증키)	로그인-ID, 비밀번호 이외의 추가 인증(2차 인증) (일회용 인증키)







※ 다계층 인증 체계는 제로 트러스트 모델의 핵심 요소 중 하나이며, 각 레이어별로 인증을 강화하여 네트워크 보안을 혁신하는 안전한 해결책.

Copyright © nurit Corp. All rights reserved.

I 배경 및 변화 3 다계층 인증 체계의 필요성

"조직의 민감한 자산을 보호하고, 규제 준수를 보장하며," 궁극적으로 사용자에게 더욱 안전하고 신뢰할 수 있는 서비스를 제공하는 데 핵심적인 역할을 수행

보안 강화 및 무단 접근 방지	진화하는 사이버 위협에 대한 대응	규제 준수 및 신뢰도 향상	비즈니스 연속성 확보 및 비용 절감 효과
보안을 획기적으로 강화하여 해커나 무단 사용자의 접근을 차단. ▶단일 인증의 취약성 극복 ▶비밀번호 유출/도용 시 보호 ▶심층 방어(Defense in Depth) 전략	오늘날 사이버 공격은 점점 더 지능적이고 정교해지는 위협에 대한 필수적인 방어선 역할. ▶다양한 공격 방식 방어 ▶다양한 정보 자산 보호	단순히 보안 기술을 넘어 조직의 신뢰도를 높이고 법적, 규제적 요구사항을 충족. ▶법적 및 규제 요구사항 충족 ▶고객 및 사용자 신뢰도 향상	사고 발생 위험을 줄여 비즈니스 연속성을 확보하고 장기적인 비용 절감에 기여. ▶사고 대응 비용 절감 ▶운영 효율성 증대.

※ 다계층 인증 체계는 제로 트러스트 모델의 핵심 요소 중 하나이며, 각 레이어별로 인증을 강화하여 네트워크 보안을 혁신함.

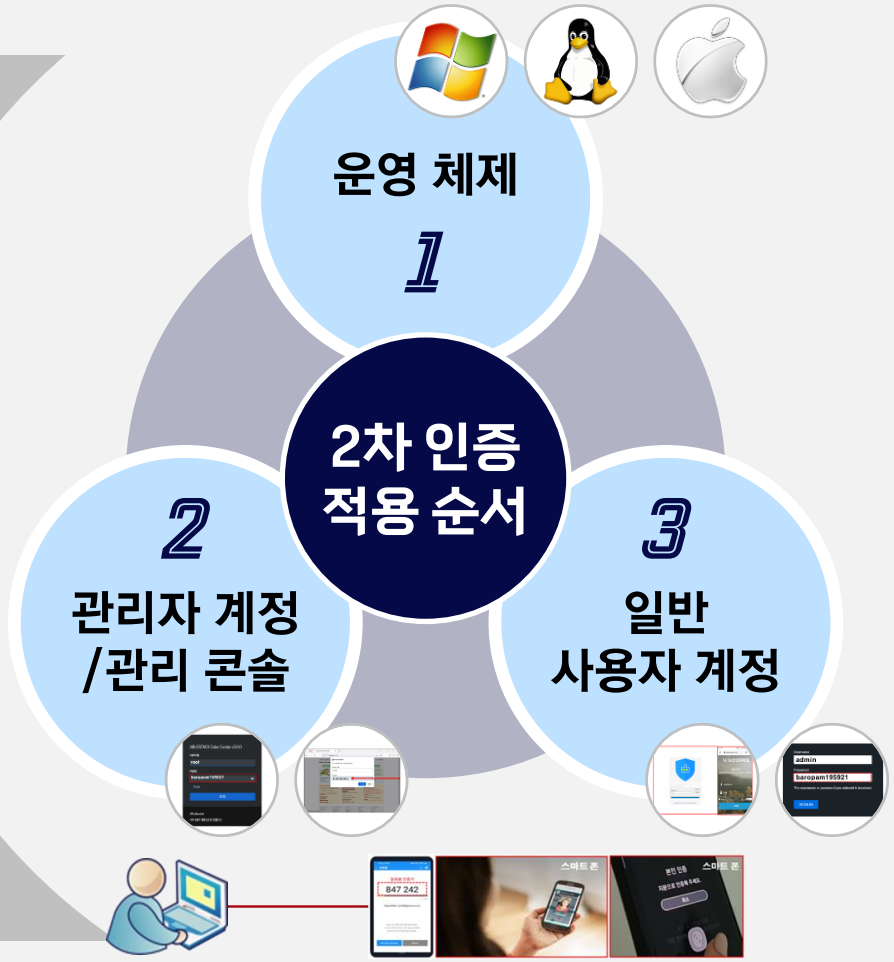
Copyright © nurit Corp. All rights reserved.

I 배경 및 변화

4 침해 사고가 발생한 기업의 특징

“ 주요 인프라 공격의 85%가 패치, 2차 인증(추가 인증), 최소 권한 원칙 등 ”
기본적인 수준의 보안을 지키지 않아서 발생.

1. 최신패치 및 업데이트 하지 않음
2. 2차 인증(추가 인증)을 사용하지 않음
3. 기본 포트를 그대로 사용함
   예) SSH/SFTP:22, VPN:4433, RDP:3389, SMB:139, 445 등
4. 불필요한 서비스를 비활성화 하지 않음
5. 정기적인 보안 감사를 하지 않음
6. 직원들의 보안에 대한 인식 결여(보안 교육 미비)



Copyright © nurit Corp. All rights reserved.

“ 모듈인증 방식으로 한번 사용된 인증키는 재사용할 수 없으며, ” 인증키 유추가 어려워 다양한 해킹 공격에도 강력한 보안성을 제공

전제조건

동일한 알고리즘

동일한 키

동일한 시간(UTC)

인증키 생성기

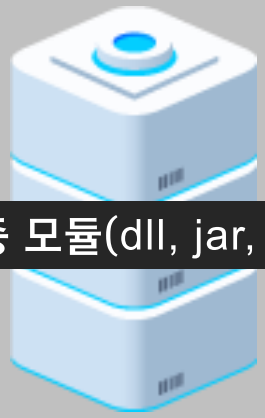
생성 모듈 (jar, so)

일회용 인증키

=

통신 안함

정보자산(OS/App)

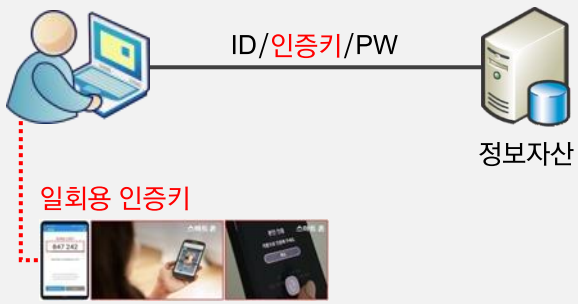


검증 모듈(dll, jar, so)

Copyright © nurit Corp. All rights reserved.

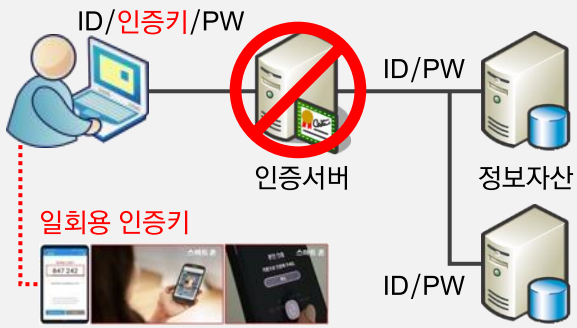
“ 다양한 운영체제와 애플리케이션에 플러그인 가능한 인증 모듈(PAM) 방식을 기반으로 하는 보안에 최적화된 다계층 인증 체계를 지원하는 솔루션 ”

정보자산 접근 보안강화



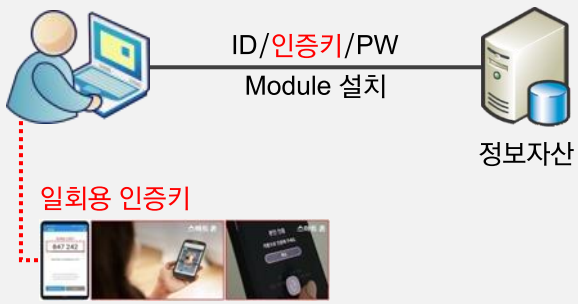
- 외부의 해커 또는 내부 사용자가 불법적으로 정보자산에 접근하는 상황을 제한하여 정보자산의 보안 강화
- 2-Factor 인증으로 기존의 "지식기반 인증"인 ID/PW 인증에 다른 요소인 소유기반/속성기반 인증요소를 추가한 인증기법

서비스의 용이성



- 2차 인증을 별도 인증키 토큰/카드 필요 없이 BaroPAM 앱을 이용하여 인증이 용이함
- 별도 인증서버나 Windows/서버 접근 제어를 관리하는 서버가 필요 없는 구조로 관리/운영비용 절감

손쉬운 적용



- 각 Windows 또는 서버에 모듈을 설치하는 구조로 간단히 적용 가능
- Windows 또는 서버를 재기동하지 않기 때문에 운영 중에도 적용 가능
- 기존 네트워크 장비의 설정변경 불필요

Copyright © nurit Corp. All rights reserved.

“ 보안성이 강하고, 단순하고, 관리도 필요 없고, 장애도 없고, 누구나 손쉽게 곧바로 ” 적용하여 사용할 수 있고, 솔루션을 도입할 때 별도의 서버나 DB 같은 추가 도입이 필요 없는 저비용 고효율의 솔루션

➢ 별도의 인증서버가 필요 없는 모듈인증 방식의 다계층 인증 체계 지원 ➢ 빠른 인증속도로 서비스 보장(평균 인증시간 0.01초 이내)	➢ BaroPAM 앱 소스 난독화 및 화면 캡쳐 방지 기능 제공 ➢ BaroPAM 앱 실행 시 생체인증(지문인식, 얼굴인식) 기능 제공
➢ 전세계적으로 인정된 512Bit 표준 Hash 함수 사용 (HMac-SHA512/인터넷 보안표준 IETF RFC 6238) ➢ 금감원에서 권장하는 Time-Sync, 동적 Secret key 방식 지원	➢ 환경 설정 정보를 파일 이외에 MariaDB와 연동 기능 제공 ➢ 인증의 제한 횟수 및 제한 시간(예:30초에 3회) 설정 기능 제공 ➢ 중간자(man-in-the-middle) 공격을 예방하는 기능 제공
➢ 빈번하게 발생하는 통신 장애 또는 보안 지역에서도 인증 가능 ➢ 매번 변하거나 한번 사용하고 버리는 일회성/휘발성 같은 동적인 보안 지원	➢ 인증절차 시 인증정보가 위변조 되더라도 우회인증 불가능 ➢ 인증 우회(우회기술, 피로공격 등) 불가능
➢ 간단(느슨)한 구성에서 시작해 더 복잡(견고)한 보안 시스템으로 진화 가능 ➢ iOS는 자체적으로 본인인증 할 수 있는 기능 제공	➢ 자동 로그인 기능을 악용한 계정 정보 탈취해도 로그인 불가능 ➢ 스마트 폰 이용 불가 시 응급 일회용 인증키 제공
➢ 다양한 정보자산 등 2차 인증이 필요한 모든 분야에서 적용가능 (정보자산의 RADIUS 인증 중 PAM/SQL/HTTP 인증도 지원) ➢ 2차 인증에서 허용/제외할 수 있는 계정에 대한 ACL 기능 제공	➢ 자유로운 Customizing 및 다양한 응용 프로그램과의 연동 개발 제공 (Java, C, C++ 등의 API 연동)

※ HMac(Hash-based Message Authentication Code) : 해쉬 기반 메시지 인증 코드

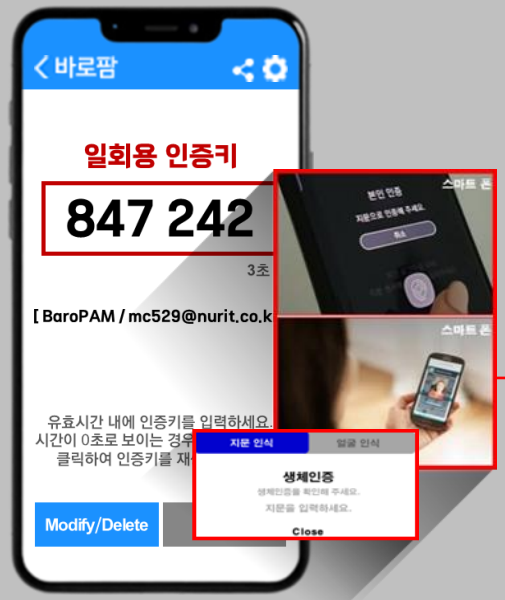
HMac는 Key를 조합하여 Hash 함수를 구하는 방식으로, 송신자와 수신자만이 공유하고 있는 Key와 메시지를 혼합하여 Hash값을 만드는 방식이다.
또한 채널을 통해 보낸 메시지가 훼손되었는지 여부를 확인하는데 사용할 수 있으며 Mac 특성상 역산이 불가능하므로 수신된 메시지와 Hash값을 다시 계산하여 계산된 HMac과 전송된 HMac이 일치하는지를 확인하는 방식이다.

Copyright © nurit Corp. All rights reserved.

BaroPAM 4 솔루션 구성

“ 사용자가 일회용 인증키를 생성하는 장치, 일회용 인증키를 적용하는 정보자산, ”
일회용 인증키를 검증하는 모듈, BaroPAM 앱과 데스크탑의
블루투스/애플리케이션간 통신하는 BaroBLE로 구성

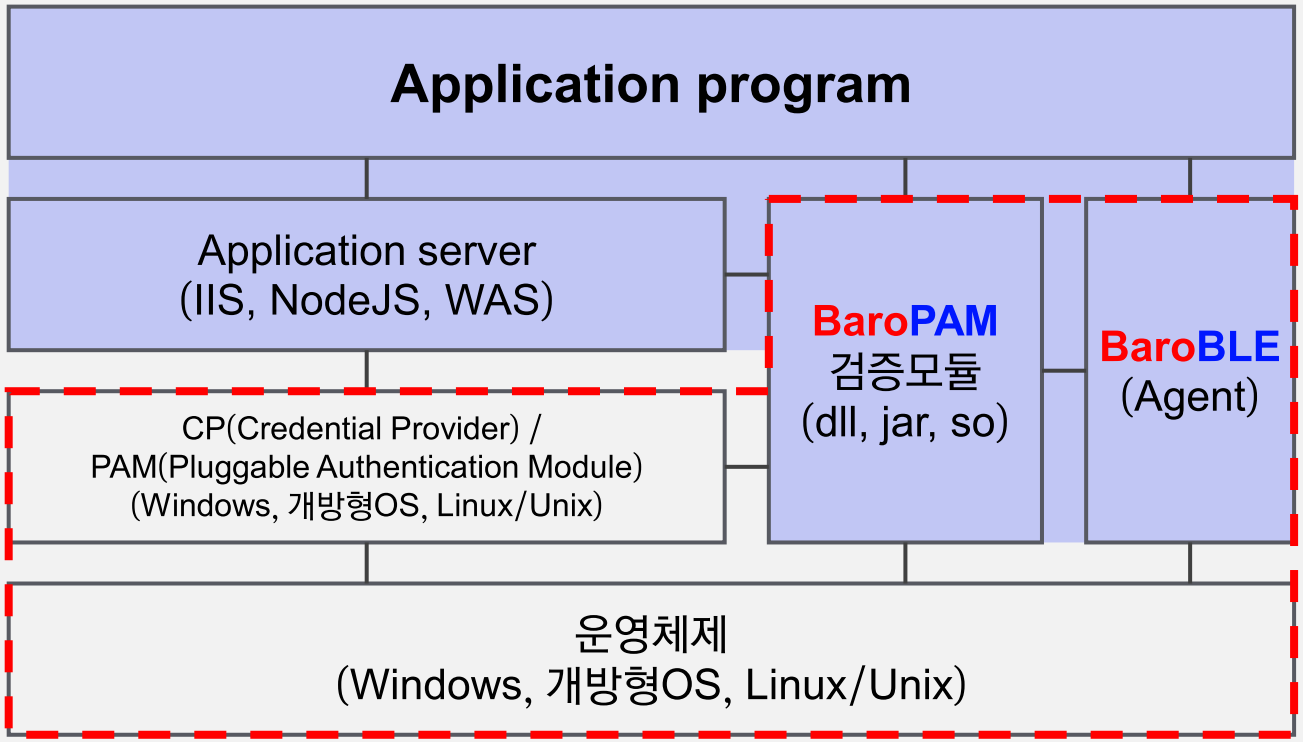
인증키 생성(사용자)



스마트폰

인증키

정보자산



Copyright © nurit Corp. All rights reserved.

“ 다양한 개발 및 운영환경을 지원 ”

No	구분		내용	비고
1	OS	Windows 계열	Windows 8.1 이상 Windows server 2012 R2 이상	
		Linux 계열	Radhat, CentOS, AlmaLinux, RockyLinux, NAVIX, Oracle linux, Debian, Fedora, Mint, Ubuntu, openSUSE, KaliLinux, 개방형 OS(하모니카OS, 구름OS) 등 Open Linux 지원	
		Unix 계열	AIX, HP-UX, Solaris, FreeBSD, MacOS 등	
2	Language		C, C++, C#, Java, ASP, PHP, PowerBuilder, Delphi 등	
3	Application	ARM system	Shard object 제공(인증, 암복호화)	
		IIS	dll 제공(인증, 암복호화)	
		NodeJS	jar 제공(인증)	
		WAS	jar 제공(인증, 암복호화)	
4	Database	암복호화	Oracle, Tibero, Cubrid, MySQL, MariaDB, PostgreSQL, SQL Server 등	
		인증	Oracle, MySQL, MariaDB, PostgreSQL 등 RADIUS 인증을 지원하는 데이터베이스	
5	Network 장비		Open Linux 및 RADIUS 인증을 지원하는 장비, OpenVPN은 PAM/RADIUS 인증 지원	
6	저장장치		상용OS를 지원하는 장치	

Copyright © nurit Corp. All rights reserved.

“ 동적 Secret 값을 사용하기 때문에 유출 및 유추가 어려워서 보안에 강함 ”

1. 동적 Secret 값을 사용
2. 중간자(man-in-the-middle) 공격을 예방하는 기능
3. iOS는 자체적으로 본인인증 할 수 있는 기능
4. 중앙 집중화 방식이 아닌 탈 중앙화 방식
5. 별도의 인증 서버 방식이 아닌 모듈인증 방식
6. 다계층 인증 체계를 지원
7. 다양한 운영체계와 애플리케이션을 지원
8. 일회성/휘발성 같은 동적인 보안 지원
9. 별도의 추가 장비 (서버, DB)가 필요 없음
10. 해외 어디서든 사용 및 적용에 문제 없음
11. 손쉬운 적용 및 장애가 없음

Copyright © nurit Corp. All rights reserved.

“새로운 적용 방안인 추가 인증, 비밀번호 대체, 새로운 비밀번호가 필요”

1안 추가 인증

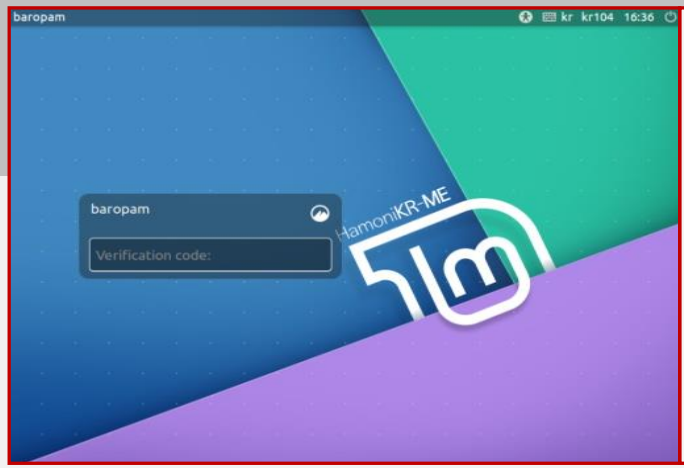
로그인-ID, 비밀번호
이외의 추가 인증(2차 인증)으로
일회용 인증키 적용
(ID/PW/OTA)

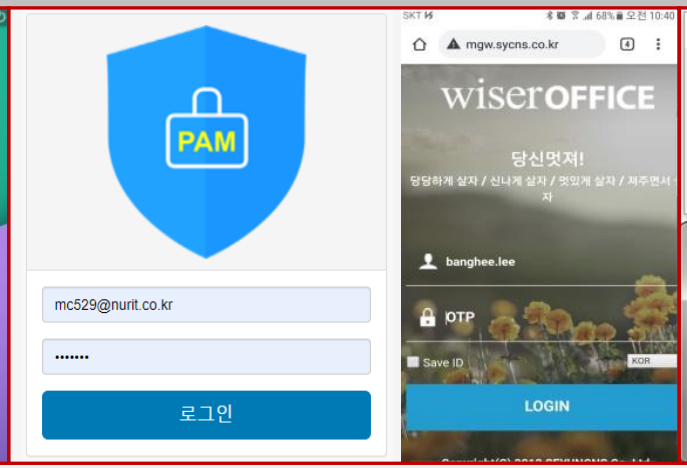
2안 비밀번호 대체

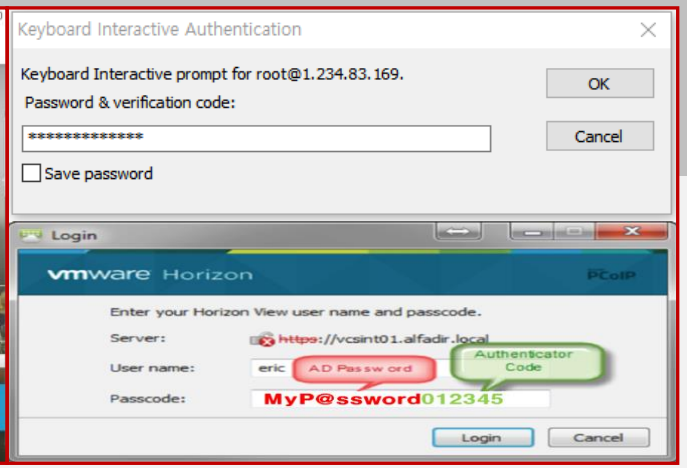
비밀번호를 제거하고
일회용 인증키로
대체
(ID/OTA)

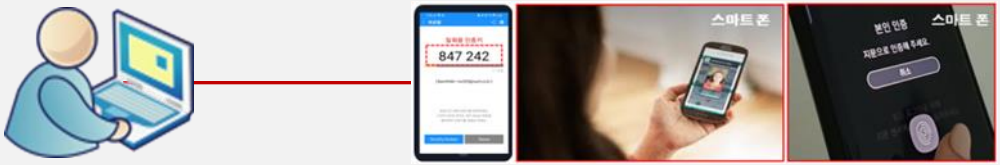
3안 새로운 비밀번호

비밀번호와 일회용 인증키 결합하여
비밀번호를 일회용 인증키 생성주기별로
새로운 일회용 비밀번호를 생성하여 적용
(ID/PW+OTA)









Copyright © nurit Corp. All rights reserved.

“ 백신 솔루션/서버접근통제 솔루션과 BaroPAM 솔루션이 결합하여 ”
정보자산의 보안을 강화하는 시너지 효과를 발생

정보자산 보안

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

=

악성코드 탐지/제거
(백신)

V3

“관리 서버 보안 취약”

서버접근통제솔루션

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

+

우회/원격 접속차단
(BaroPAM)

Desktop to Application
Desktop to Desktop
Desktop to Server
Desktop to Database
Server to Server

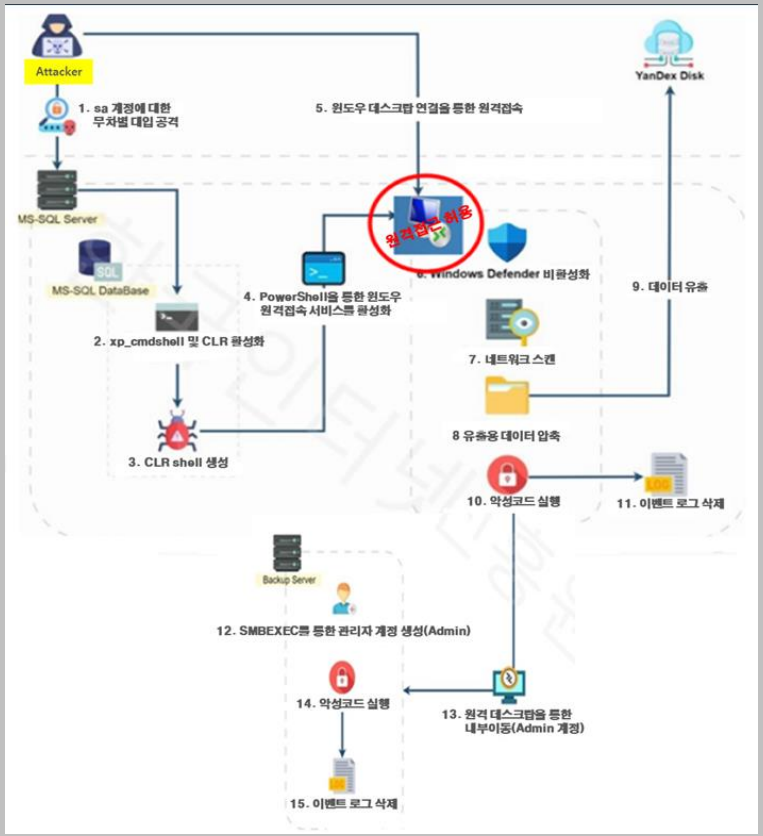
Copyright © nurit Corp. All rights reserved.

BaroPAM 9 해킹 차단 사례(Windows 환경)

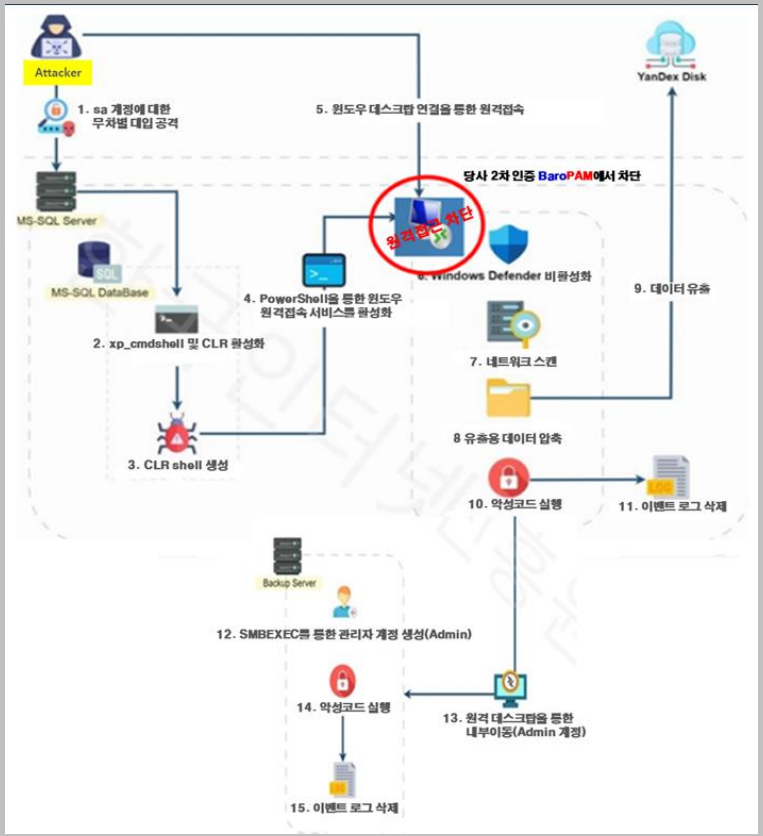
해커들이 계정에 대한 무차별 대입 공격 또는 네트워크, 서버 등 하드웨어 취약점을 스캔/악용하여

SQL Injection 공격으로 PowerShell를 통한 권한상승 및 원격접속 서비스를 활성화한 후 원격데스크탑(RDP) 연결로 원격 접속을 시도

침해사고 발생



침해사고 방어



Copyright © nurit Corp. All rights reserved.

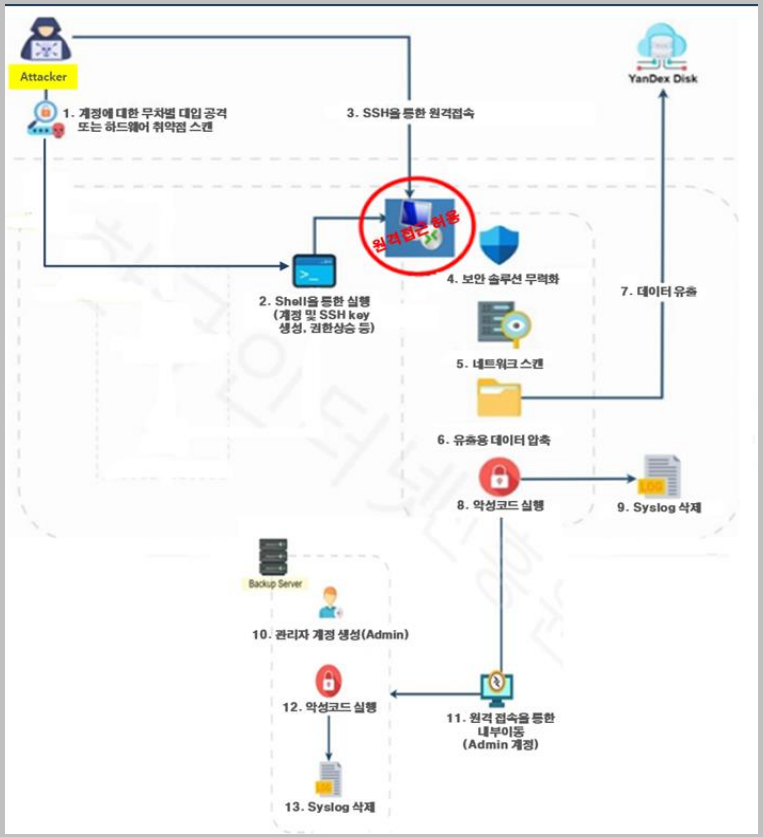
BaroPAM 9 해킹 차단 사례(Linux/Unix 환경)

해커들이 계정에 대한 무차별 대입 공격 또는 네트워크, 서버 등 하드웨어 취약점을 스캔/악용하여

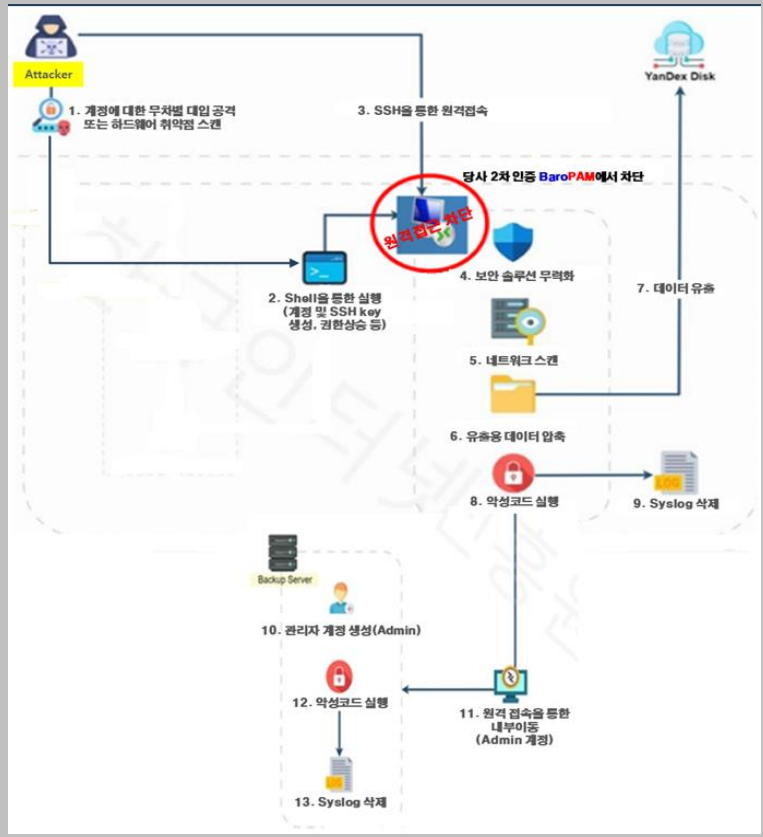
원격코드 실행(RCE)을 통한

계정 및 SSH key 생성, 권한 상승, 우회/원격 접속을 시도

침해사고 발생



침해사고 방어



Copyright © nurit Corp. All rights reserved.

“ 망분리했다고 해커들을 침투를 100% 막을 수 없다는 걸 인정하고, ” 해커들이 이미 망 내에 들어와 있는 걸 상정하고 보안 전략을 마련해야

아직도 보안에 취약한 이런 방식이 사용되고 있다는 현실

- 2차 인증 중 해커들의 가장 좋아하는 적용 방식 : Gateway(+Proxy) 방식
- 2차 인증 중 가장 취약한 인증 방식 : SMS, 이메일 등 문자기반의 인증
- 2차 인증 중 해커들이 가장 애용하는 우회 기술과 피로공격에 취약한 인증 방식 : 2채널 인증
- 피싱 공격에 잘 속는 링크 방식 : QR코드 방식

정보자산의 보안 강화를 위해서는 가장 중요한 기본 사항

- 보안 관점에서 위험을 얼마나 분산 시킬 것인지?
- 인증 절차 시 데이터 위변조를 어떻게 방어할 것인지?
- 계정 정보 도용 및 악용은 어떻게 차단할 것인지?
- 권한상승은 어떻게 차단할 것인지?
- 브라우저 자동 로그인은 어떻게 방어할 것인지?
- 단일 지점 공격을 어떻게 방어할 것인지?
- 우회/원격접속을 어떻게 차단할 것인지?
- 중간자 공격을 어떻게 방어할 것인지?
- 다중 인증(MFA)의 우회기술/피로공격을 어떻게 방어할 것인지?

Copyright © nurit Corp. All rights reserved.

Ⅲ 기타 1 회사 소개

일반현황

상호	주식회사 누리아이티
설립일	2018년 1월 19일
주사업분야	정보자산의 보안강화를 위한 다계층 인증 S/W
사업장	서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)
주요 품목	BaroPAM, BaroCRYPT, BaroCollector, BaroFDS, BaroIDS
자문 교수	문영상 숭실대학교정보과학대학원 소프트웨어공학과 겸임교수

「BaroPAM 솔루션의 전략은 정보자산에 대한 보안을 강화하기 위하여 탈중앙화 방식의 다계층 인증 체계를 지원하는 방향으로!」

연혁

2025.02 Linux용 BaroPAM에 환경설정 정보를 MariaDB와 연동하는 모듈 출시
2025.02 도어락용 BaroPAM 출시

2024.09 파트너 체제에서 총판 체제로 전환
2024.06 Cloudera Data Platform과 Hi-ware 접근제어 솔루션에 BaroPAM 연동
2024.05 피앤피 시큐리티 서버접근제어 솔루션에 BaroPAM 연동
2024.04 오픈소스 협업 툴인 Mattermost 에 BaroPAM 연동

2023.08 Cisco VPN, Foti-gate VPN, OpenVPN OpenVPN에 BaroPAM 연동
2023.04 BaroPAM 앱에 생체인식(지문, 얼굴인식) 기능 추가

2022.12 Palo Alto Networks Firewall(비전테크 공급)에 BaroPAM 연동
2022.11 KOICA 클라우드 컴퓨팅 기반환경 구축 및 무선 네 트워크 고도화 용역 사업에 2차 인증으로 BaroPAM 선정
2022.11 시큐어레터의 Anyclick AUS에 Wifi 접속 시 2차 인증으로 BaroPAM 적용
2022.08 Beyondtrust Password safe(아이리스인포테크 공급)에 2차 인증으로 BaroPAM 연동
2022.06 2022년 정보보호 선도기술 개발 지원사업에 BaroCARD(지문인식OTP카드) 참여
2022.05 TTA에서 하모니카 OS와 BaroPAM 제품의 SW상호운영성 시험진행

2021.10 FreeRADIUS에 BaroPAM 연동
2021.08 Windows용 BaroPAM에 화면 보호기의 잠금 방지 및 해제 기능 추가
2021.07 BaroPAM v1.0 조달 등록
2021.07 2021 보안솔루션(SECaaS)공급 Pool 등록 솔루션에 BaroPAM 선정
2021.04 세윤씨엔에스에서 Microsoft365, Power Apps, ERP 등 Microsoft 제품과 BaroPAM 연동
2021.04 TS Solution의 NVR 솔루션에 BaroPAM 임베디드 공급

2021.03 Sophos SSLVPN(엘리시스 공급)에 BaroPAM 연동
2020.09 중소기업벤처기업부 'K-비대면 바우처 플랫폼', 네트워크, 보안 솔루션 분야에 BaroPAM 참여
2020.09 2020년 엘지유플러스 정부업무망 모바일화 레퍼런스 실증 사업에 2차 인증 SW(BaroPAM) 납품
2019.10 "범정부 데이터 플랫폼 2단계 구축" 사업(309개 공공기관)에 BaroPAM 공급
2019.05 개방형OS인 하모니카OS, 구름OS용 BaroPAM 출시
2019.04 유도전류를 이용한 무충전 방식의 지문인식 출입카드 출시
2019.04 BaroPAM GS인증 누리아이티→주식회사 누리아이티로 양도양수
2019.03 BaroPAM 저작권 등록

2018.12 웹용 일회용 인증키 생성기 오픈(www.baropam.com)
2018.07 BaroPAM 인증카드 및 지문인식 인증카드 출시
2018.06 Windows용 BaroPAM 출시
2018.04 금융결제용 OTP토큰/카드 Firmware 개발
2018.01 주식회사 누리아이티 설립(마곡나루)

2017.09 BaroPAM 어플 서비스 개시
2017.07 BaroIDS(이상접속 탐지 및 차단) 제품 출시
2017.07 바로팜 V1.0(BaroPAM V1.0) GS인증 1등급 인증
2017.05 BaroCRYPT(암복호화) 제품 출시
2016.11 Linux/Unix용 BaroPAM(정보자산 2차 인증) 제품 출시
2016.05 BaroKEY(일회용 인증키) 제품 출시
2016.01 BaroFDS(이상금융거래 탐지시스템) 제품 출시
2015.10 BaroCollector(실시간 로그 수집기) 제품 출시
2014.04 특허출원(OTP카드를 이용한 본인인증 결제시스템 및 그 방법)
2009.11 누리아이티로 상호 변경
2006.03 케이피엘 인포텍 설립(대방동 경원빌딩)

Copyright © nurit Corp. All rights reserved.

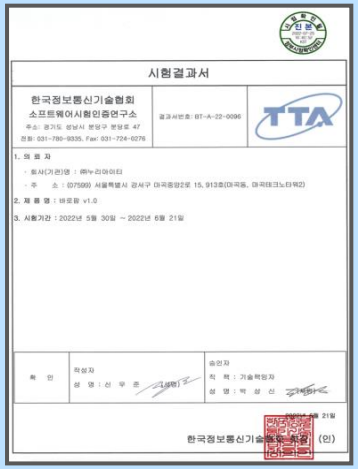
III 기타 2 소프트웨어 품질인증(GS 인증서 / 시험성적서 / 특허증 / 저작권 등록증)

2017년 7월
GS인증 1등급

2014년 6월
특허번호
제 10-1413971호

2019년 3월
저작권 등록증

2017년 7월
TTA 시험성적서



2022년 6월
SW상호운용성시험

Copyright © nurit Corp. All rights reserved.

3 BaroSolution Download

BaroSolution 소개서 Download (https://mc529.tistory.com/1401)

BaroSolution 가이드 Download (https://mc529.tistory.com/1406)

BaroSolution Software Download (https://mc529.tistory.com/1407)

Copyright © nurit Corp. All rights reserved.

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