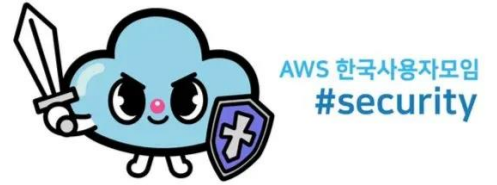



최소 비용으로 “Zero Trust” 엔드포인트 아키텍처 구성하기

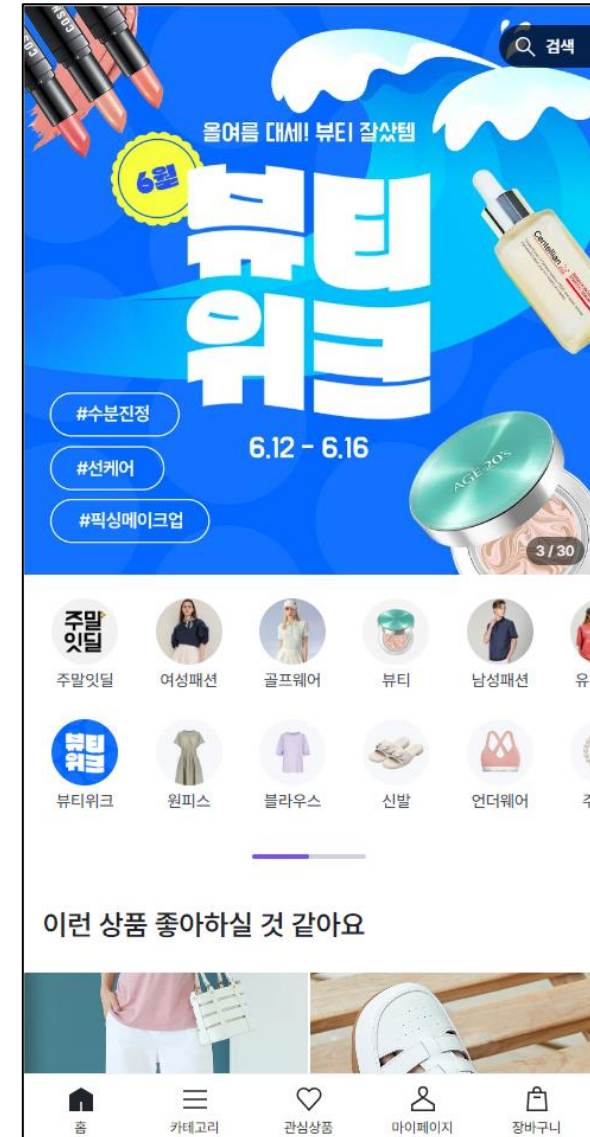
공지훈(zero)

24.6.27.

발표자 소개



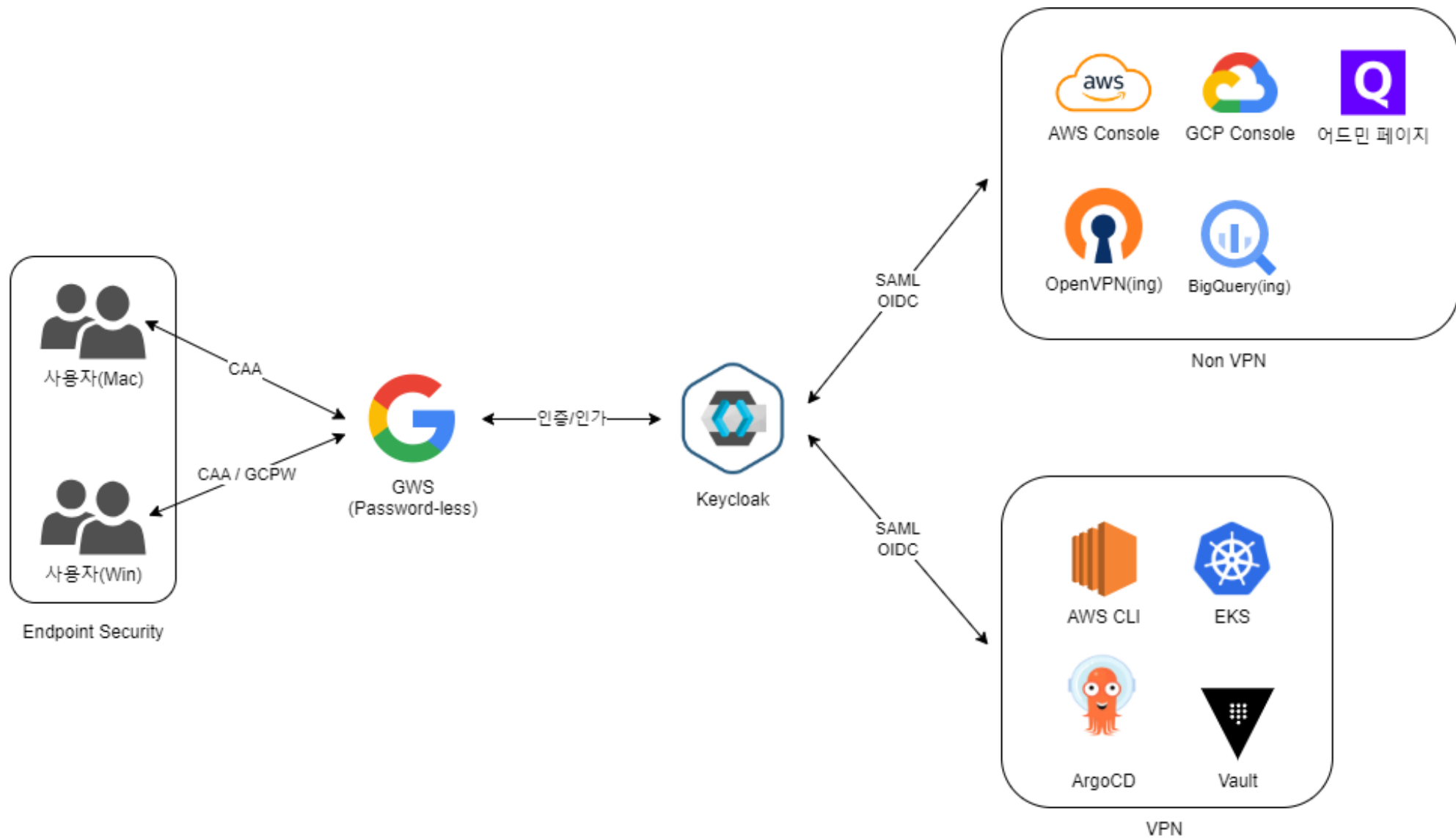
- 공지훈 
- 라포랩스(퀸잇) Security Manager
- KISA, 금융보안원, 카카오뱅크, 스타트업 ing



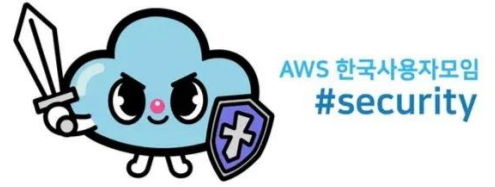
아키텍처



AWS 한국사용자모임
#security



목차



1. Zero Trust...?
2. 구성 전략
3. 아키텍처 소개

1. Zero Trust...?

보안뉴스

[이슈인터뷰] 코제타 배한국 2대 의장, “제로트러스트 보안, 이미 우리 안에 배어 있는 신기술”

한국제로트러스트위원회, 디플정위에서 언급한 '제로트러스트 보안' 다루는 공적 협의체 제로트러스트 보안 모델, 국제표준 준수해야.

5일 전



Da 디지털데일리

[NSIS 2024⑥] 한국형 제로트러스트 모델, 어디까지 왔나?

디지털데일리>가 주최하는 차세대 보안 혁신 서밋 [NSIS 2024]가 오는 5월28일 서울 소공동 롯데호텔 사파이어볼룸에서 열립니다.

4주 전



A 아이티데일리

[시장동향] 국내 보안 기업들, 제로 트러스트 확산 위해 '합종연횡'

[아이티데일리] 전 세계 사이버 보안 업계의 큰 흐름인 '제로 트러스트(Zero Trust)'. 국내 보안 업계 역시 제로 트러스트를 본격적으로 확산시키고자...

2주 전



Chosunbiz

정부가 지원 나선 '제로트러스트' 보안... 기업들도 합종연횡 - 조선비즈

정부가 지원 나선 제로트러스트 보안 기업들도 합종연횡 美·日·英, 정부가 앞장서 제로트러스트 강조 IT 시스템 각각 영역 분리·보호 KOZETA 회원사...

1개월 전



not 정보통신신문

KISIA, 한국제로트러스트위원회 1차 회의 개최

[정보통신신문=박남수기자] 한국정보보호산업협회(KISIA)는 과기정통부의 제로트러스트 아키텍처 구현 전략에 부합하는 실증사업 안내,...

1개월 전



뉴스투데이

한국제로트러스트보안협회, 국회에서 '제로트러스트보안' 세미나 개최

[뉴스투데이=김한경 기자] 한국제로트러스트보안협회가 국회ICT융합포럼(공동대표 변재일 의원, 조명희 의원) 및 공공부문발주자협의회·한국IT서비스...

2023. 10. 7.



사용자모임
curity

D 디지털투데이

KOZETA 1차 회의 개최...제로 트러스트 보안모델 도입 활성화 논의

[디지털투데이 황치규 기자]한국정보보호산업협회(KISIA)는 과학기술정보통신부 제로트러스트 아키텍처 구현 전략에 부합하는 실증사업 안내,...

1개월 전



보안뉴스

방위산업학회·국방혁신기술보안협회·제로트러스트보안협회, K-방산 보안 위해 '맞손'

한국방위산업학회(회장 채우석), 한국국방혁신기술보안협회(회장 김승주), 한국제로트러스트보안협회(회장 이무성)는 AI와 디지털 국방기술에 기반한...

2023. 12. 27.



보안뉴스

K-방산의 사이버보안 역량 강화 위한 '미래 국방보안 강화 컨퍼런스' 개최

한국방위산업학회(회장 채우석), 국방혁신기술보안협회(회장 김승주), 한국제로트러스트보안협회(회장 이무성)는 AI와 디지털 국방기술에 기반한 K-...

2024. 3. 26.



보안뉴스

제로트러스트 가이드라인 2.0 내년 상반기 발표... 산학연관 뭉쳤다

제로트러스트 활성화를 위한 전문가들의 의견 개진 및 실제 사례를 전파하는 시간이 마련됐다. 한국정보보호산업협회(회장 이동범, 이하 KISIA)와...



1. Zero Trust...?



AWS 한국사용자모임
#security

제로트러스트 기본철학

- ① 모든 종류의 접근에 대해 신뢰하지 않을 것(명시적인 신뢰 확인 후 리소스 접근 허용)
- ② 일관되고 중앙집중적인 정책 관리 및 접근제어 결정·실행 필요
- ③ 사용자, 기기에 대한 관리 및 강력한 인증
- ④ 자원 분류 및 관리를 통한 세밀한 접근제어(최소 권한 부여)
- ⑤ 논리 경계 생성 및 세션 단위 접근 허용, 통신 보호 기술 적용
- ⑥ 모든 상태에 대한 모니터링, 로그 기록 등을 통한 신뢰성 지속 검증·제어

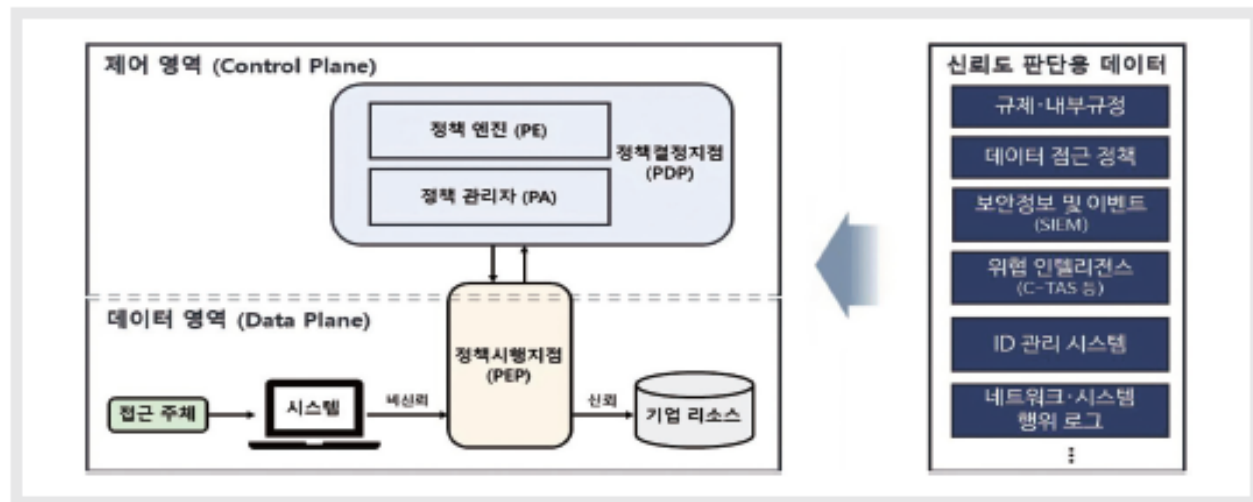
- (핵심원칙) 제로트러스트 아키텍처를 구현하기 위한 접근방법으로 네트워크 환경에 따라 일부 상이할 수 있으나, 완전한 제로트러스트 솔루션은 3가지 핵심원칙을 모두 포함

* 기존 경계 기반 보안과 달리 내부자조차도 더 이상 신뢰하지 않으므로, 강력한 관리, 인증, 접근제어 및 상태 감시를 통한 통제 필요

제로트러스트 구현 핵심원칙

핵심 원칙	세부 내용
인증 체계 강화 (기본철학 중 ①②③⑥)	<p>▲ 각종 리소스 접근 주체에 대한 신뢰도(사용하는 단말, 자산 상태, 환경 요소, 접근 위치 등을 판단)를 핵심요소로 설정하여 인증 정책 수립</p> <p>※ 기업내 사용자에게 여러 아이디를 허용하여 일관된 정책을 적용하지 않거나, 신뢰도 판단없이 단일 인증 방식만으로 접속을 허용할 경우 크래덴셜 스테핑에 취약</p>
마이크로 세그멘테이션 (기본철학 중 ②④⑤)	<p>▲ 보안 게이트웨이를 통해 보호되는 단독 네트워크 구역(segment)에 개별 자원(자원그룹)을 배치하고, 각종 접근 요청에 대한 지속적인 신뢰 검증 수행</p> <p>※ 개별 자원별 구역 설정이 없으면, 기업망 내부에 침투한 공격자가 중요 리소스로 이동하기 쉬워 공격이동 공격 성공 가능성이 높아짐</p>
소프트웨어 정의 경계 (기본철학 중 ①②⑤)	<p>▲ 소프트웨어 정의 경계 기법을 활용하여 정책 엔진 결정에 따르는 네트워크 동적 구성, 사용자 단말 신뢰 확보 후 자원 접근을 위한 데이터 채널 형성</p> <p>※ 클라우드 온프레미스로 구성된 기업 네트워크 내부에서 단말이 임의 데이터를 전송할 수 있다면, 네트워크 및 호스트 취약성에 따르는 피해 가능성이 커짐</p>

제로트러스트 접근제어 논리 컴포넌트 구성도



[참조 : NIST SP 800-207, 제로트러스트 아키텍처 논리 컴포넌트 재구성]

제로트러스트 접근제어를 위한 주요 컴포넌트

구분	주요기능
정책 결정지점 (Policy Decision Point)	<p>정책 엔진 (Policy Engine)</p> <p>▲ '신뢰도 평가 알고리즘' 기반으로 접근 주체가 리소스에 접근할 수 있을지를 최종적으로 결정</p> <p>* ① 접근정보(OS 이름·버전, 사용중 소프트웨어, 권한 등) → ② 특징기준, 점수, 가중치, 머신러닝 등 다양한 방식으로 신뢰도를 평가하는 알고리즘</p>
	<p>정책 관리자 (Policy Administrator)</p> <p>▲ 정책엔진의 결정을 정책시행지점에 알려주어 접근 주체와 리소스 사이의 통신 경로를 생성 또는 폐쇄</p>
정책시행지점 (Policy Enforcement Point)	<p>▲ 데이터 영역에서 접근 주체가 기업 리소스 접근 시 결정된 정책에 따라 최종적으로 연결·종료 역할 담당</p> <p>※ 방화벽, 네트워크 접근통제 등 단순 일부 제품 도입을 통해 높은 성숙도의 제로트러스트 보안모델 구현은 어려우며, 다양한 정책·제품이 조화를 이루어야 함</p>

자
가
공

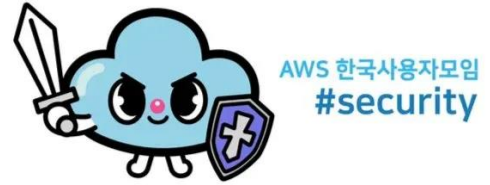


AWS 한국사용자모임
#security

의
응
?

MBC 2011 프로야구 플레이

1. Zero Trust...?



- **철학**

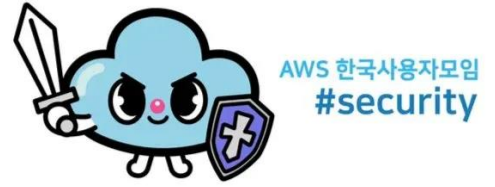
- 경계 보안 모델을 탈피하여 네트워크 내·외부를 구분하지 않고 모든 접근을 잠재적인 위협으로 간주

- **목표**

- 사용자와 디바이스를 지속적으로 인증(사용자의 신원과 디바이스 상태를 기반으로 접근 권한 부여)
- 애플리케이션에 대한 접근권한 세분화 및 최소권한 부여
- 모든 활동을 지속적으로 모니터링하고 이상행동 탐지 및 대응

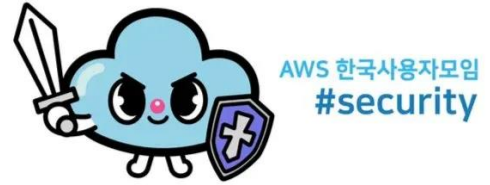
2. 구성 전략

2. 구성 전략



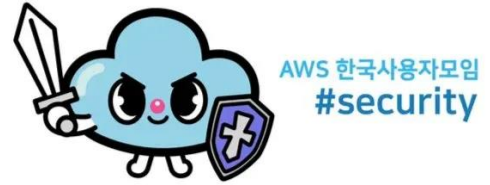
- 구현 범위
- 조직 규모
- 가용 예산

2. 구성 전략



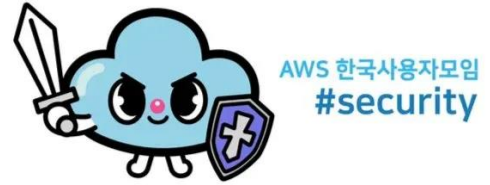
- 구현 범위(엔드포인트 접근 VS 인증/인가 VS 모니터링)
 - 조직의 보안 성숙도
 - 우선순위가 높은 것
 - 상대적으로 구현(운영)이 수월한 것

2. 구성 전략



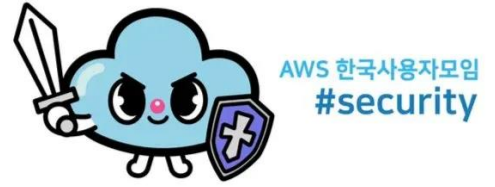
- 조직 규모(엔지니어링 조직 & 보안팀 규모 Large / Medium / Small)
 - 아키텍처를 구성 및 운영할 보안팀 규모(1인 담당자)
 - 엔지니어링 조직(60명 이하) / 전사 조직(약 150명)
 - 복잡도 ↑ == 리소스 ↑ == 야근 ↑

2. 구성 전략



- 가용 예산(상용 솔루션 VS 오픈소스+기존 솔루션)
 - Winter is coming
 - 상용 솔루션 연간 비용이...
 - 기존에 사용중인 오픈소스와 솔루션 활용
 - 마른 오징어도 비틀면 (아마도)물이 나온다

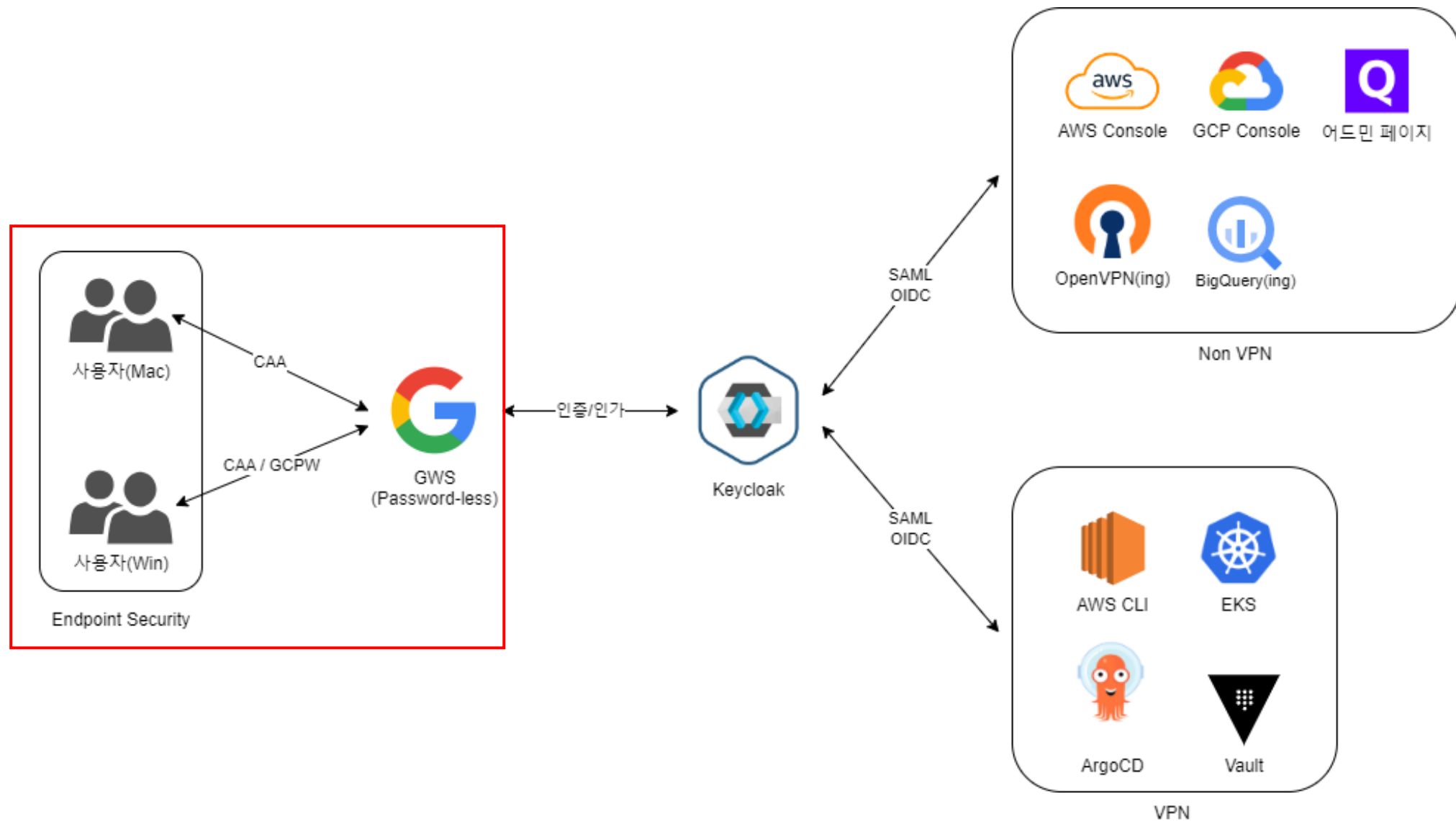
2. 구성 전략



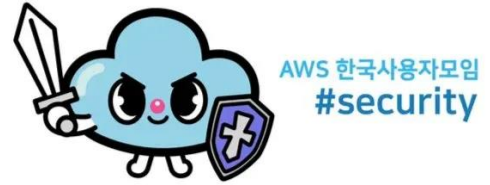
현재 우리 조직에 가장 적합한 엔드포인트 아키텍처는 무엇일까?

3. 아키텍처 소개

3. 아키텍처 소개



3. 아키텍처 소개



- **CAA(Context-Aware Access)**
 - IP, Geo Location, 기기, OS에 따른 GWS APP 접근통제
 - 업무용 PC의 SN 등록
 - GCP의 VPC Service Controls와 연계 가능
- **GCPW(Google Credential Provider for Windows)**
 - GWS 계정을 Windows OS 로그인 정보로 사용
 - 일부 MDM 기능도 수행
 - 전사 적용 전 PoC 필수

3. 아키텍처 소개



AWS 한국사용자모임
#security

조건 4

사용자가 다음과 같은 경우 앱 액세스를 허용하거나 규칙을 적용

☒ 모든 속성 충족(AND) ☐ 1개 이상의 속성을 충족하지 않음(OR)

⚠ 데스크톱 기기 정책을 시행하는 경우 사용자는 Chrome 브라우저를 사용하고 엔드포인트 확인 Chrome 확장 프로그램을 설치해야 합니다. [자세히 알아보기](#)

⚠ 회사 소유 기기에서 MDM Basic을 사용하는 경우 Google Workspace에 액세스할 수 없습니다.

⚠ 기기 OS를 선택하는 경우 사용자는 선택한 운영체제에서만 Google Workspace에 액세스할 수 있습니다. [자세히 알아보기](#)

기기

같음

회사 소유



기기 OS

Windows

같음

최소 버전
버전 무관



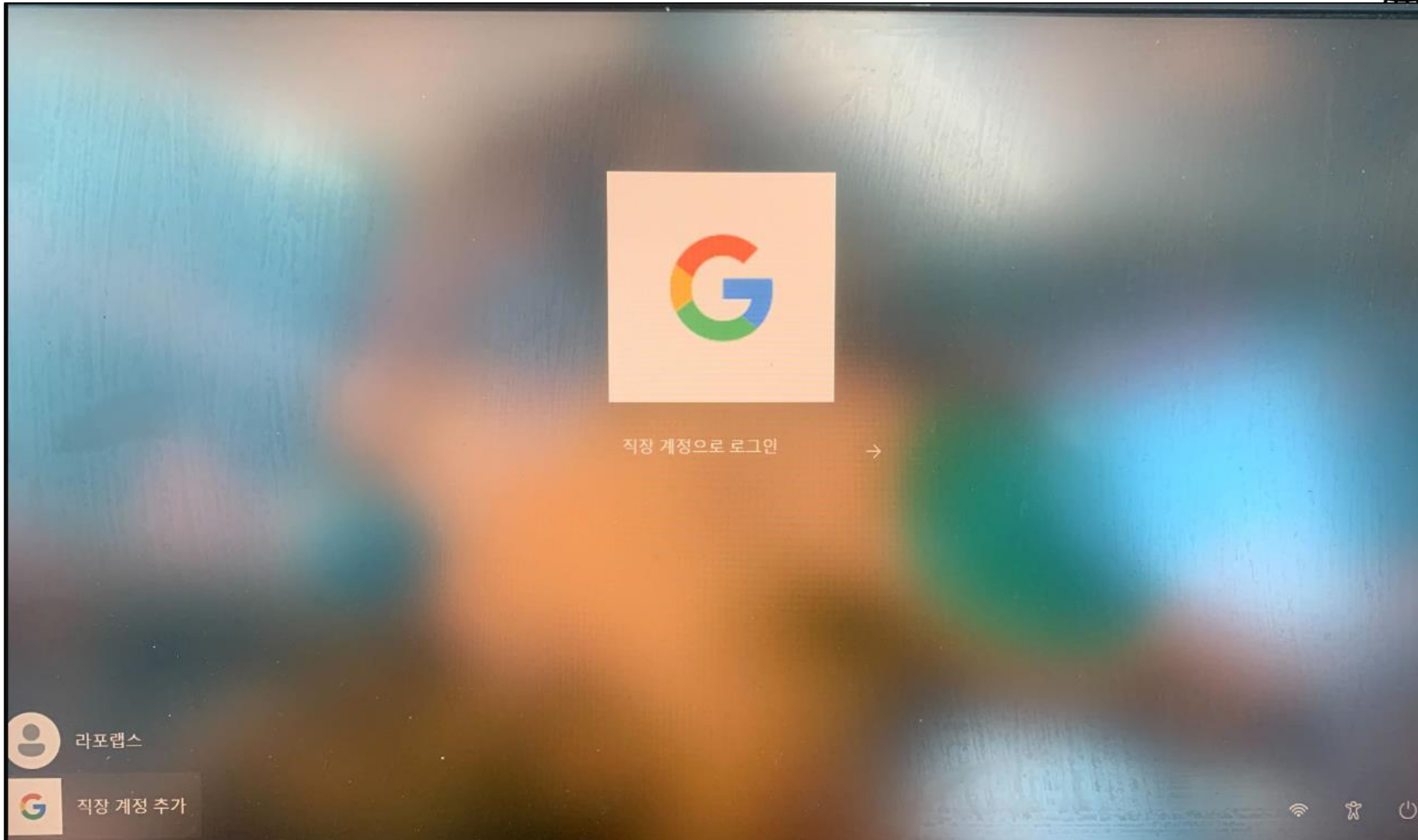
최소 버전 표시는 MAJOR.MINOR.PATCH 형식
이어야 합니다.

[속성 추가](#)

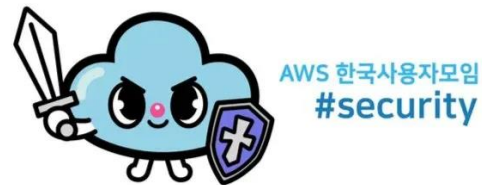
3. 아키텍처 소개



AWS 한국사용자모임
#security



3. 아키텍처 소개



- **GWS Password-less**
 - Mac 사용자에게 효과 ↑
 - Windows는 So So

패스워드리스{베타}

비밀번호 건너뛰기
재정의

패스키만으로 안전하게 인증할 수 있는 경우 사용자가 로그인 시 비밀번호를 건너뛸 수 있도록 하려면 선택합니다. [비밀번호 건너뛰기에 대해 알아보기](#)

!

서드 파티 ID 공급업체에서 사용자를 인증한 경우에는 이 설정이 적용되지 않습니다.

☒ 사용자가 패스키를 사용하여 로그인 시 비밀번호를 건너뛰도록 허용

i

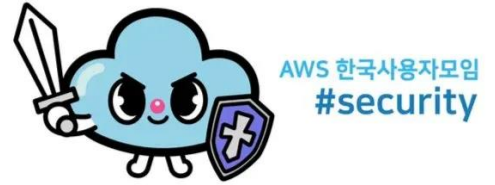
대부분의 변경사항은 몇 분 안에 적용됩니다. [자세히 알아보기](#)
감사 로그에서 이전 변경사항을 볼 수 있습니다.

상속

취소

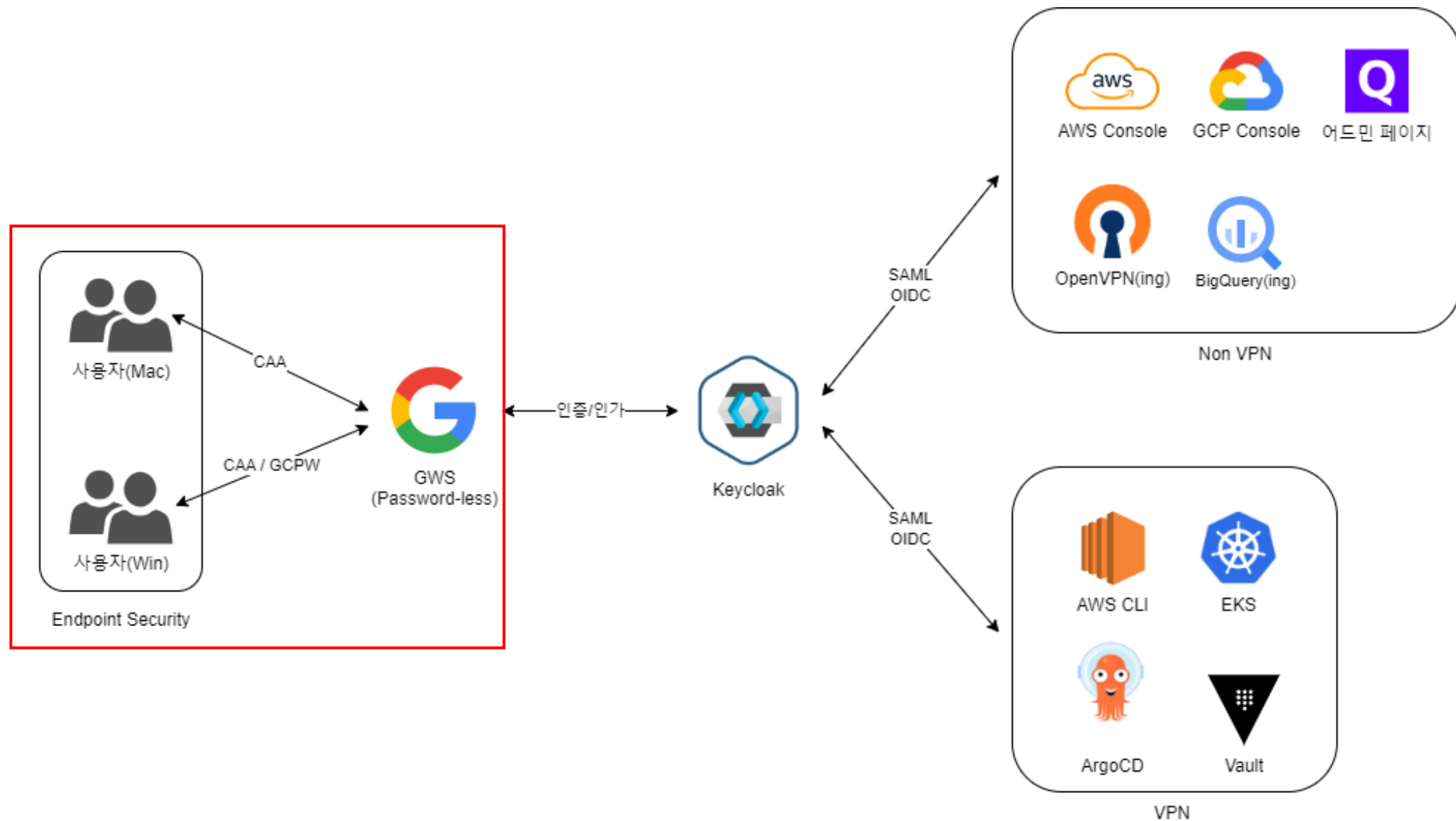
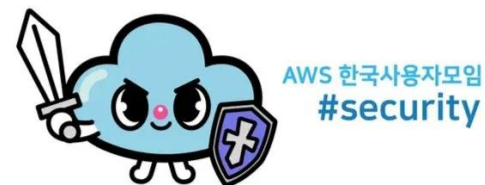
저장

3. 아키텍처 소개



- **Endpoint Security(SaaS)**
 - 백신
 - DLP
 - 웹 접속 제어
 - 애플리케이션 제어(사용 / 파일 업로드 통제)
 - 기타(출력물 통제, PC보안점검, (기본적인)패치관리, 개인정보 저장 관리)

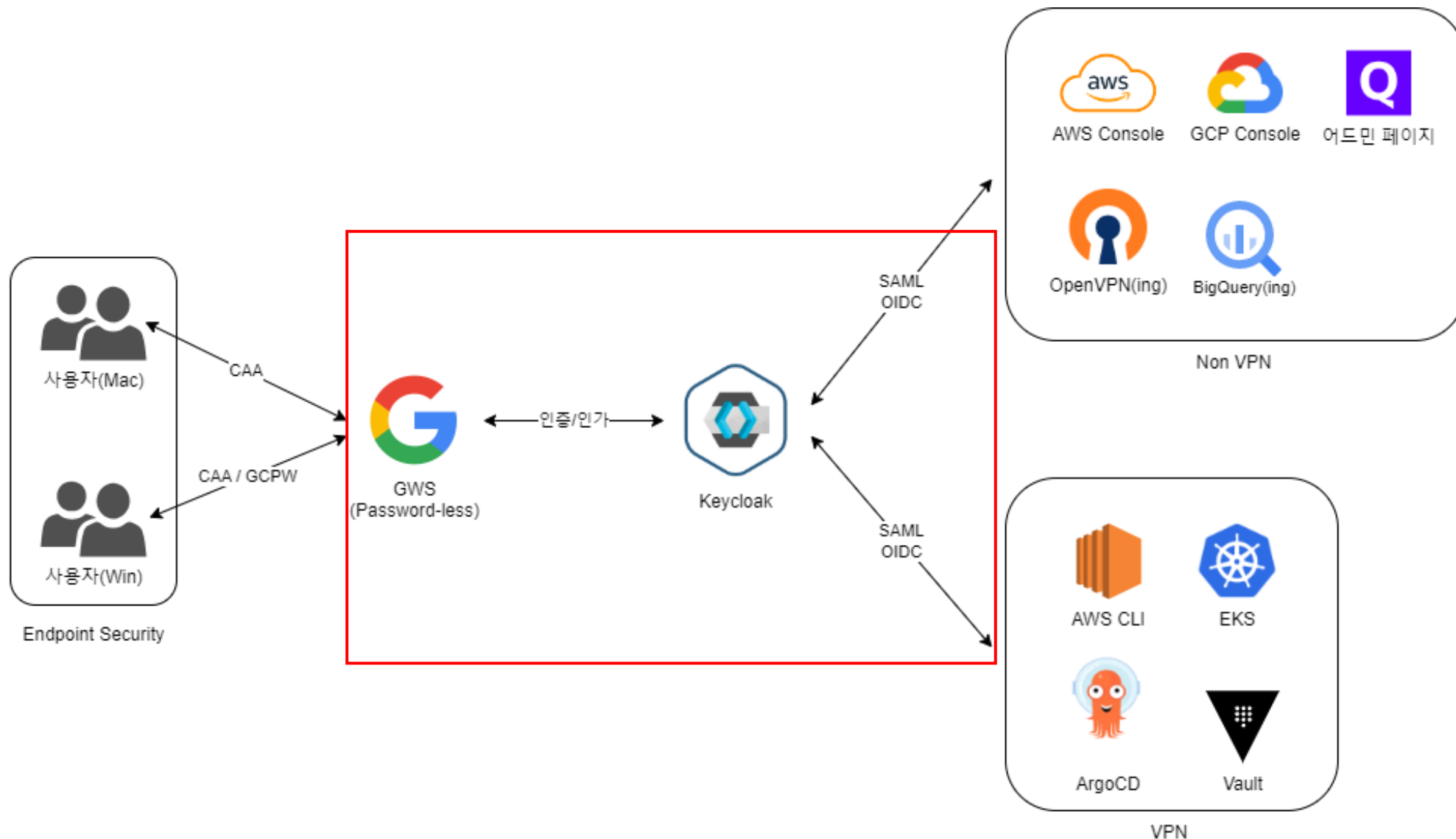
3. 아키텍처 소개



3. 아키텍처 소개



AWS 한국사용자모임
#security



3. 아키텍처 소개



- GWS SAML 설정

앱(4) 앱 추가 설정

이름: "rpls" 필터 지우기

<input type="checkbox"/>	이름 ↑	플랫폼	인증	사용자 액세스	세부정보
<input type="checkbox"/>	RP RPLS Apps	웹	SAML	조직 단위 1개에 대해 사용 설정	
<input type="checkbox"/>	RP RPLS Apps DEV	웹	SAML	조직 단위 1개에 대해 사용 설정	
<input type="checkbox"/>	RP RPLS Apps STG	웹	SAML	조직 단위 1개에 대해 사용 설정	
<input type="checkbox"/>	RP RPLS Dev Util	웹	SAML	조직 단위 1개에 대해 사용 설정	

3. 아키텍처 소개



- Keycloak IdP 및 Mapper 설정

Identity providers > Provider details

Rapportlabs.kr 로그인

Settings Mappers

General settings

Redirect URI ?	<input type="text" value="https://keycloak"/>	
Alias * ?	<input type="text" value="rapportlabs-google-workspace"/>	
Display name ?	<input type="text" value="rapportlabs.kr 로그인"/>	
Display order ?	<input type="text" value="0"/>	
Endpoints ?	SAML 2.0 Service Provider Metadata	

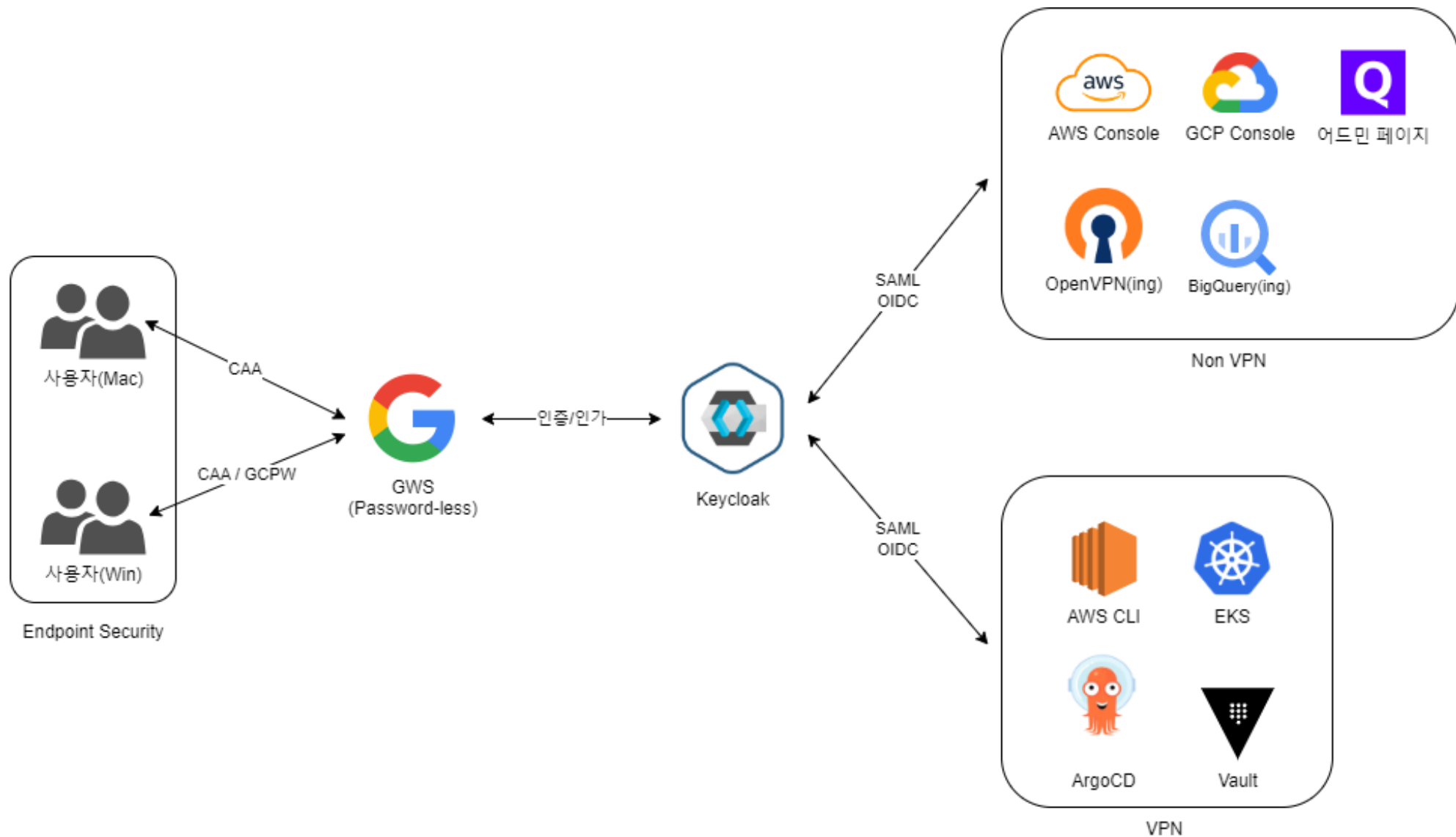
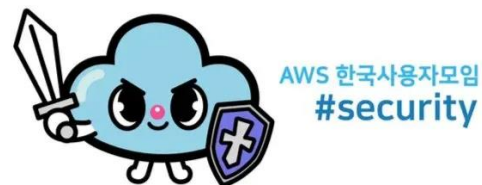
3. 아키텍처 소개



- Keycloak Clients 설정

Clients					
Clients are applications and services that can request authentication of a user. Learn more					
<div>Clients listInitial access tokenClient registration</div>					
<div><input type="text" value="Search for client"/> → Create client Import client 1 - 15</div>					
Client ID	Name	Type	Description	Home URL	
ac	\$f	OpenID Connect	—	https	⋮
ac	\$f	OpenID Connect	—	https	⋮
ad	\$f	OpenID Connect	—	—	⋮
br	\$f	OpenID Connect	—	—	⋮
gc	gc	OpenID Connect	—	https	⋮
gc	gc	OpenID Connect	—	https	⋮
gc	gc	OpenID Connect	—	https	⋮
ml	ml	OpenID Connect	—	—	⋮
ml	ml	OpenID Connect	—	/appl	⋮
ml	ml	OpenID Connect	—	https	⋮
re	\$f	OpenID Connect	—	—	⋮
sa	sa	OpenID Connect	—	https	⋮
se	\$f	OpenID Connect	—	https	⋮
urn:amazon:webservices	aws	SAML	—	/reali	⋮
vault-eks	vault-eks	OpenID Connect	—	https	⋮

3. 아키텍처 소개





QnA