전자신문

CIO Summit 2025

CIO SUMMIT 2025

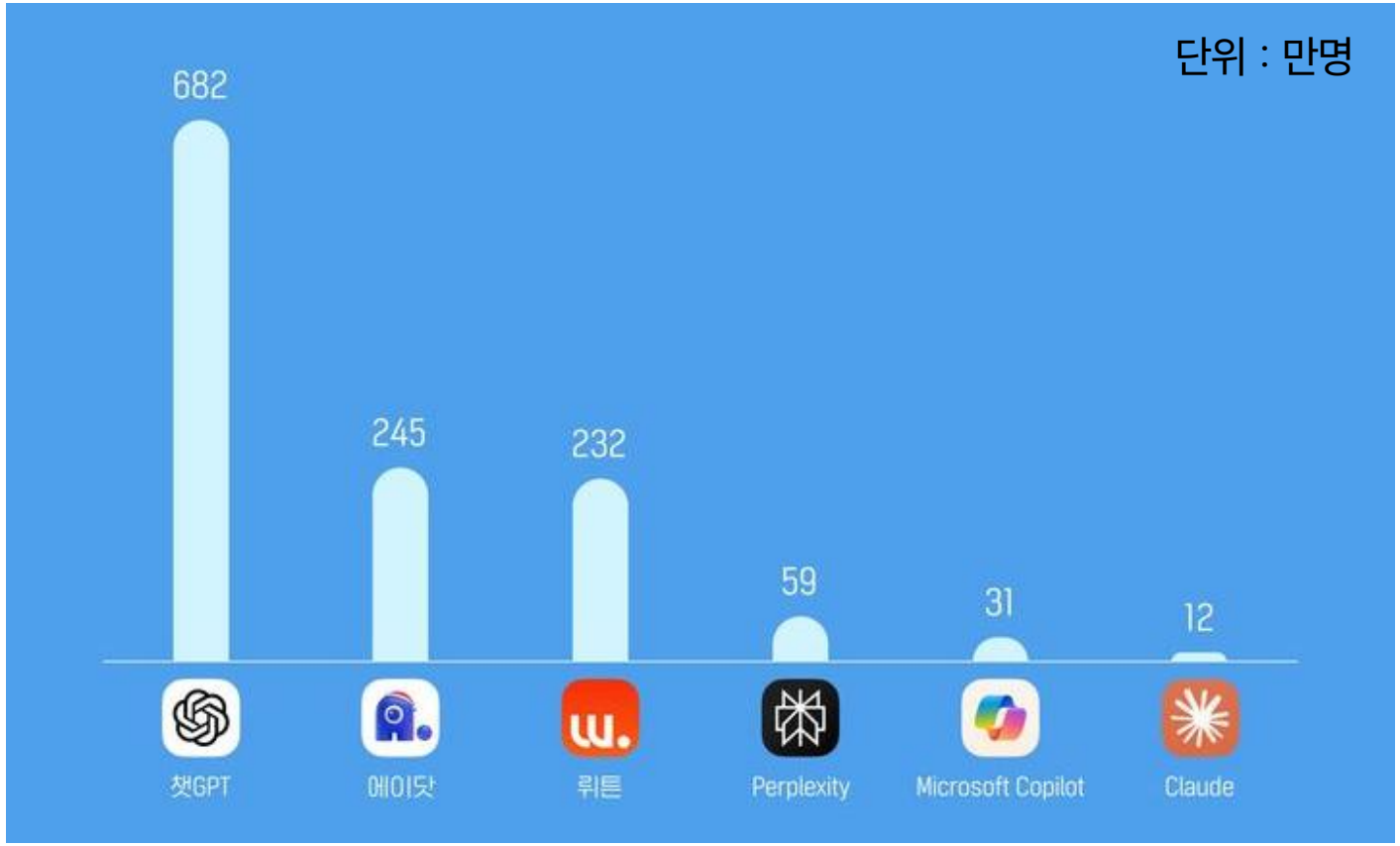
2025. 2. 27.(목) | 그랜드 인터컨티넨탈 서울 파르나스

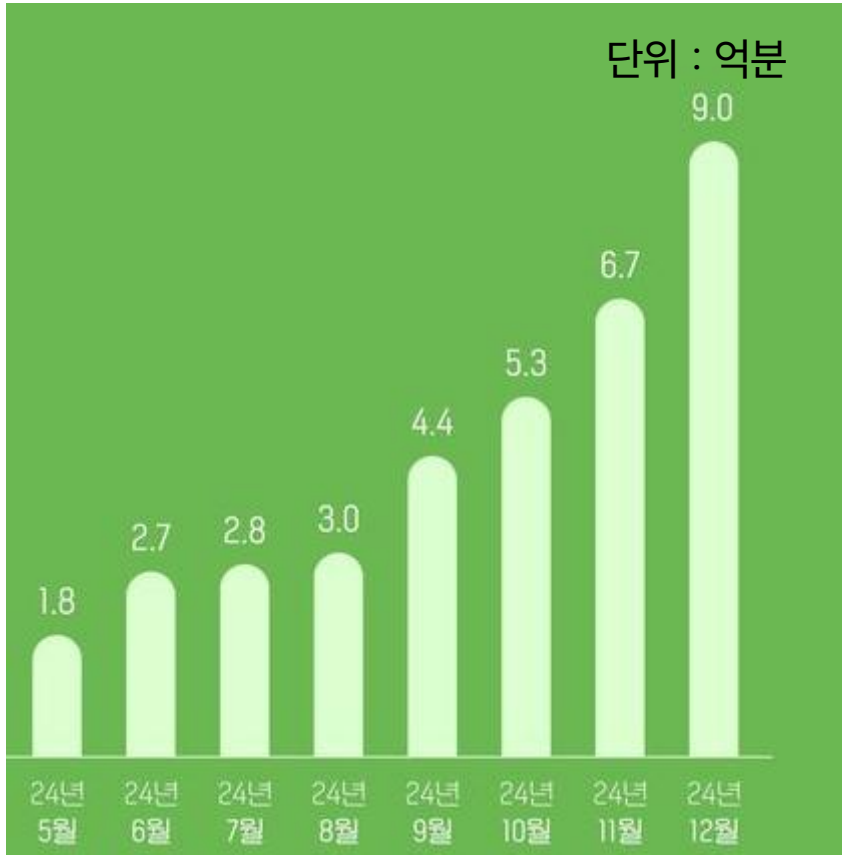




생성형 AI를 사용하는 개발자를 위한 VDI 플랫폼

- 일상생활 속 Gen AI





출처 : 와이즈앱·리테일

Gen AI를 통한 개발자 환경 변화

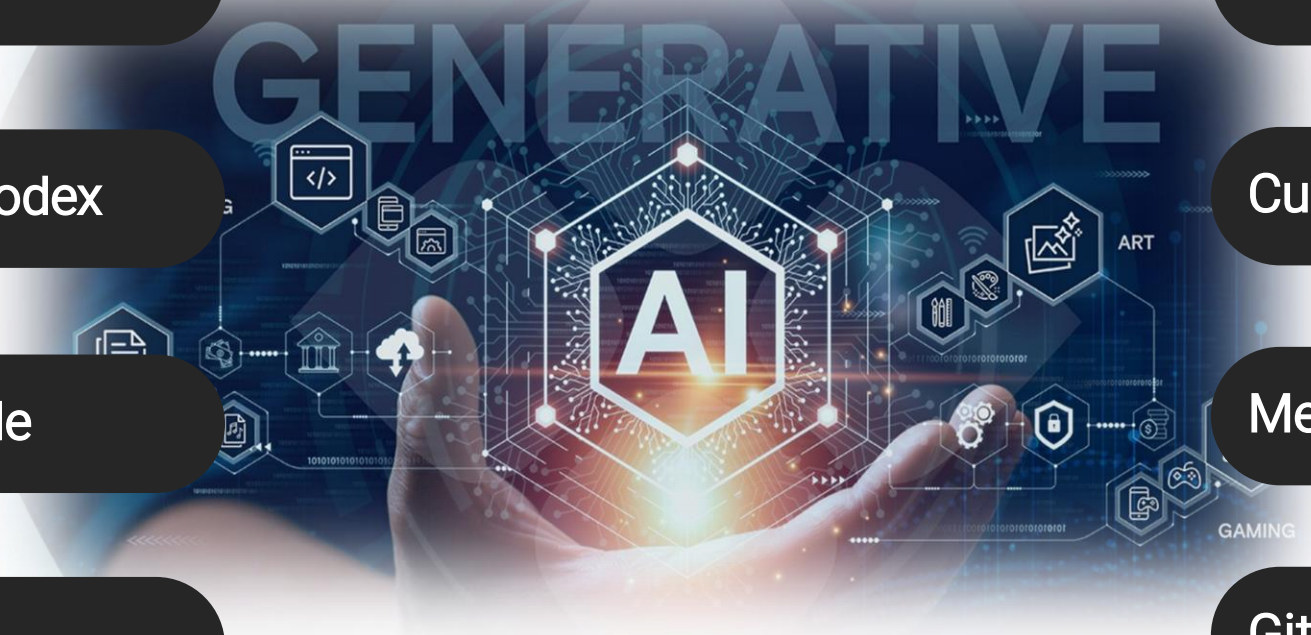
- 개발자를 위한 Gen AI Tools
  - 약 70% 이상의 개발자가 Gen AI를 활용

ChatGPT

OpenAI Codex

AlphaCode

Snyk



Google Gemini

Cursor AI

MetaGPT

GitHub Copilot

Gen AI를 통한 개발자 환경 변화

CIO Summit 2025

- 개발 방식의 변화
  - Gen AI는 소프트웨어 개발환경을 근본적으로 바꾸고 있습니다.

<생성형 AI로 인한 소프트웨어 개발의 변화 예측>

- 자연어 프롬프트에서 코드를 생성하는 것이 표준화된다
- 코드 검증은 개발자의 주요 책임이다
- '조립'이 새로운 개발 패러다임
- 코딩 작업은 줄어드는 반면 코드 공급망 위험은 커진다
- 통합을 가속화하는 새 패러다임이 등장한다
- 개발자가 AI 에이전트의 관리자 노릇을 한다
- AI가 SDLC의 여러 단계에 관여한다
- 생성형AI 및 인간 개발 페르소나가 등장한다
- AI가 개발 과정 중에 운영 능력을 향상시킨다
- 조직은 AI 위험으로부터 스스로를 보호해야 한다

Gen AI를 통한 개발자 환경 변화

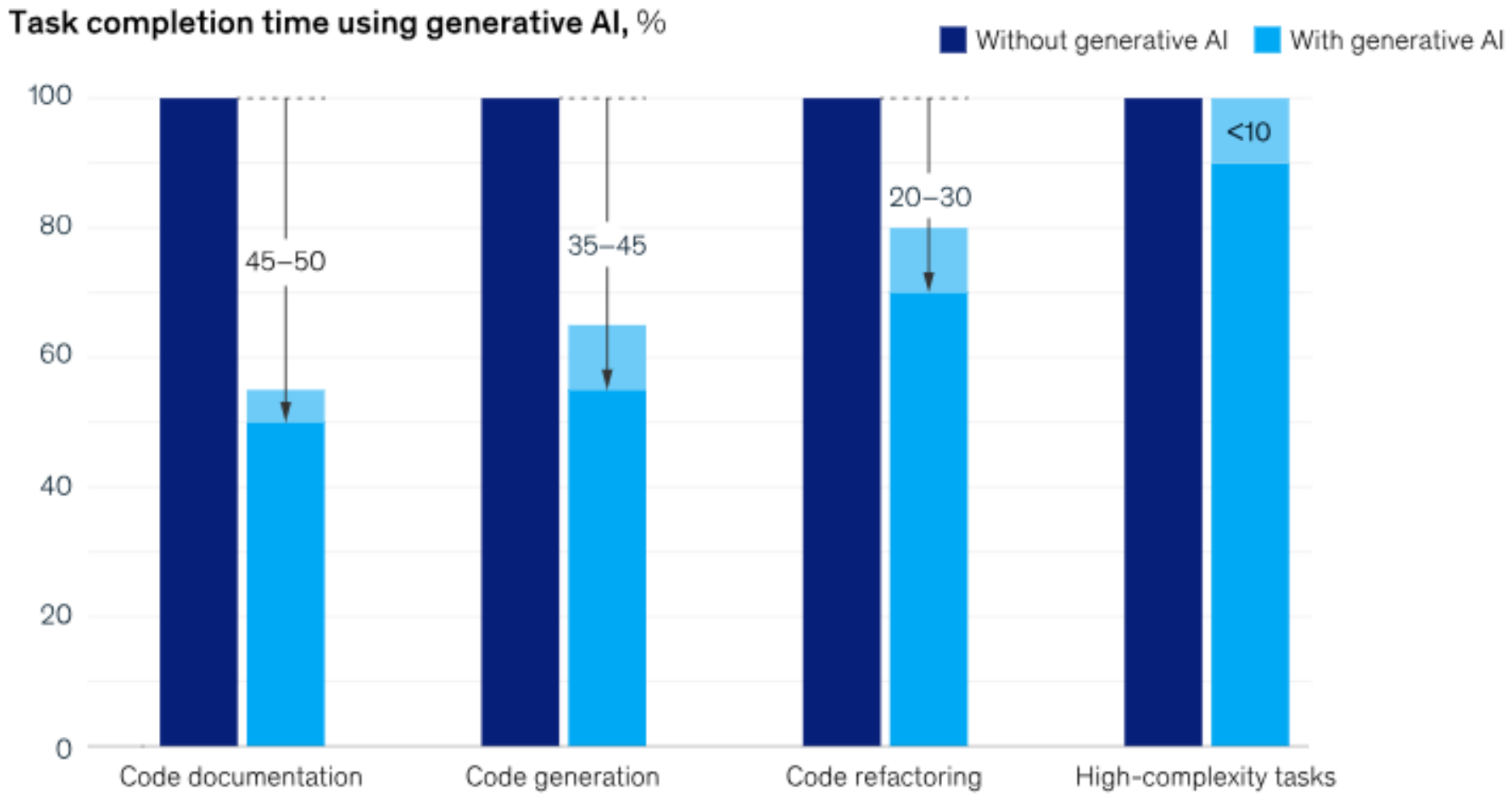
- 개발 방식의 변화
  - Gen AI는 소프트웨어 개발환경을 근본적으로 바꾸고 있습니다.

개발환경에서의 GenAI 활용

- AI-Backed Code Review
- Automated Code Generation
- Automation Testing and QA
- Smarter Debugging
- Automated Documentation Generation
- Deployments
- Conversational Coding Interfaces
- Code Refactoring
- Security, Compliance, and Threat Detection
- Code Translation and Porting
- AI-Assisted Design Workflows

Gen AI를 통한 개발자 환경 변화

- Gen AI 활용을 통한 생산성 향상

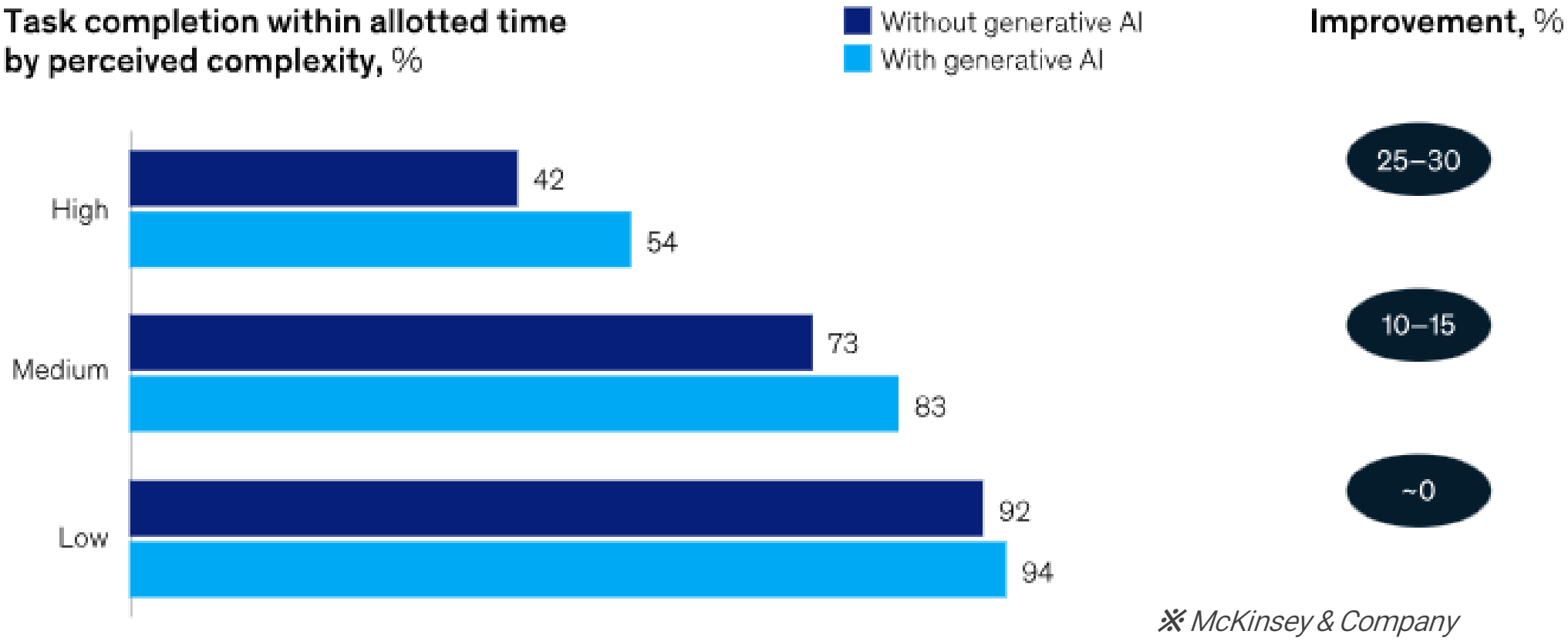


※ *McKinsey & Company*

Gen AI를 통한 개발자 환경 변화

- Gen AI 활용을 통한 생산성 향상

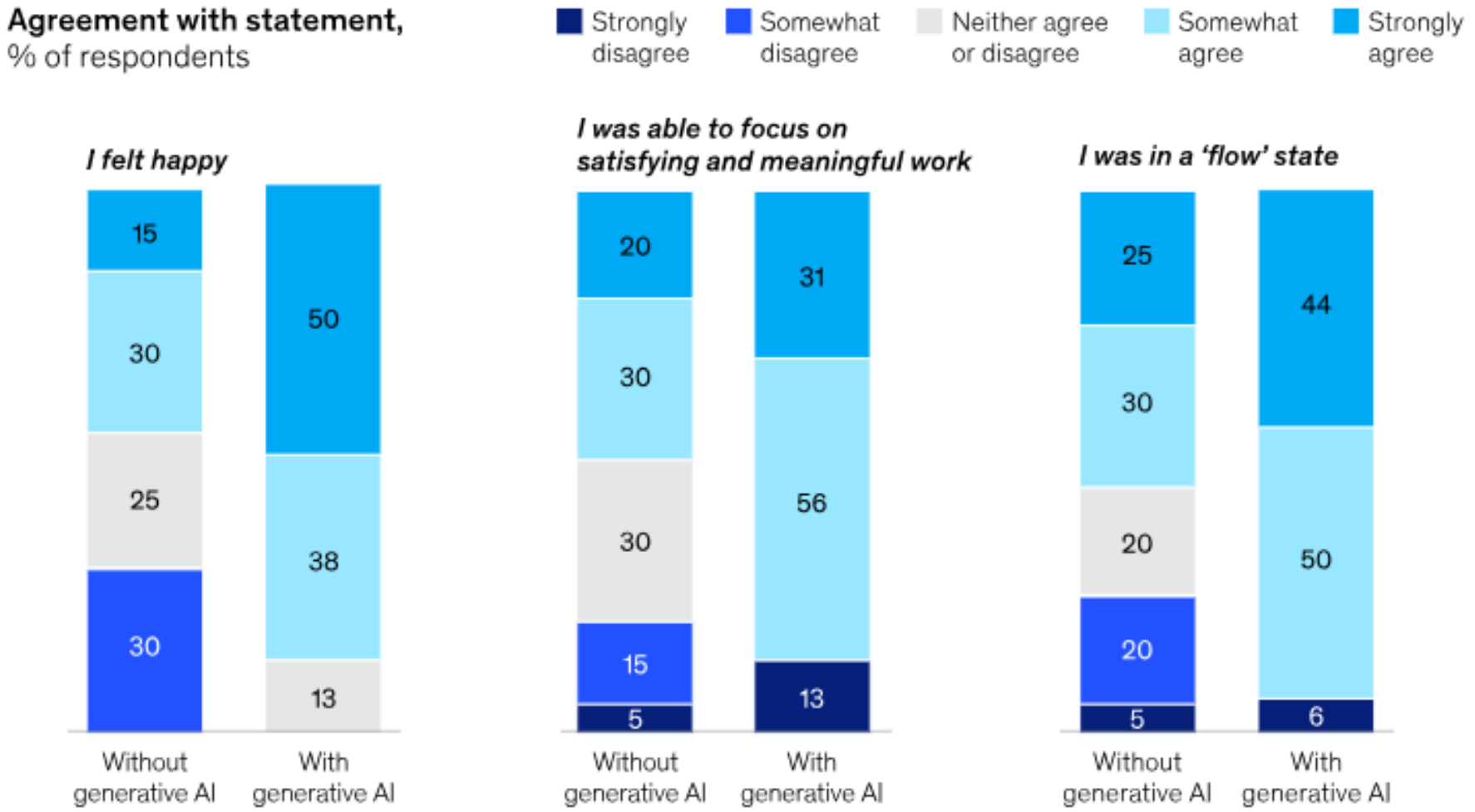
Developers using generative AI to assist with complex tasks were more likely to complete those tasks within a given time frame.



※ *McKinsey & Company*

Gen AI를 통한 개발자 환경 변화

- Gen AI 활용을 통한 생산성 향상



※ McKinsey & Company

개발 환경 보안에 대한 중요도 증가

- 다양한 방식의 소스코드 유출

게임 '리그 오브 레전드' 소스코드 유출…"해커의 돈 요구 거절"

'리그 오브 레전드' 등 인기 게임 해킹
"돈 요구 거절하고 조사 나서겠다" 밝혀

임지선 기자

수정 2023-01-25 17:02 등록 2023-01-25 17:02

Riot Games
@riotgames

Today, we received a ransom email. Needless to say, we won't pay.

While this attack disrupted our build environment and could cause issues in the future, most importantly we remain confident that no player data or player personal information was compromised.

출처 : https://www.hani.co.kr/arti/economy/economy_general/1076929.html

- 해외 외주 개발사

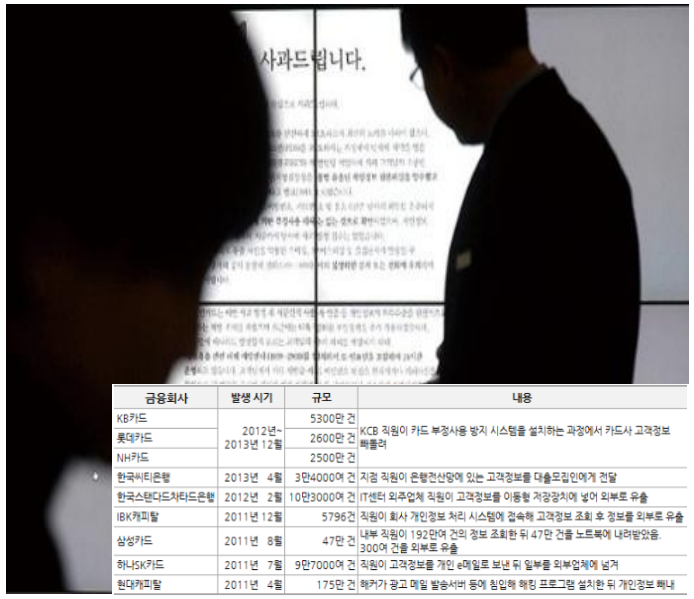


Zero Trust VDI

VDI 도입에 대한 시각 변화

- 망분리 또는 노후 PC 교체를 위한 VDI 도입에서 스마트 업무 환경 시대로 변화
- 코로나 19로 IT 변화 트랜드 가속화

시대의 흐름에 따른 변화

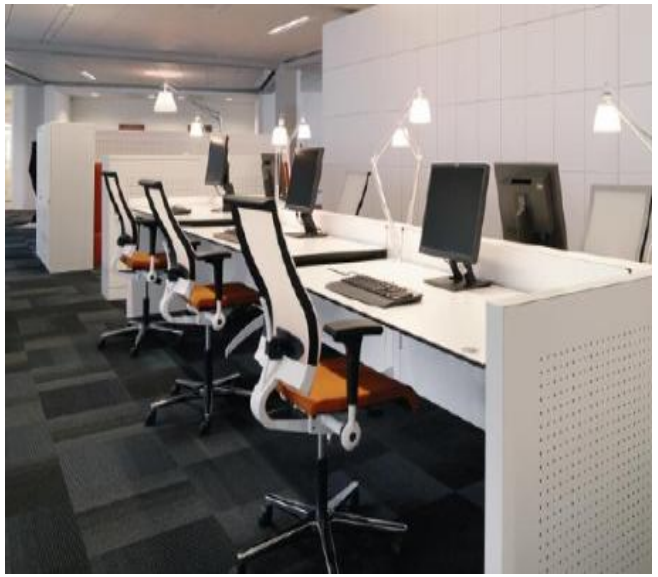


금융회사	발생 시기	규모	내용
KB카드	2012년~2013년 12월	5300만 건	KCB 직원이 카드 부정사용 방지 시스템을 설치하는 과정에서 카드사 고객정보 빼돌려
롯데카드		2600만 건	
NH카드		2500만 건	
한국씨티은행	2013년 4월	3만4000여 건	지점 직원이 은행전산망에 있는 고객정보를 대출모집인에게 전달
한국스탠다드차타드은행	2012년 2월	10만3000여 건	IT센터 외주업체 직원이 고객정보를 이동형 저장장치에 넣어 외부로 유출
IBK캐피탈	2011년 12월	5796건	직원이 회사 개인정보 처리 시스템에 접속해 고객정보 조회 후 정보를 외부로 유출
삼성카드	2011년 8월	47만 건	내부 직원이 192만여 건의 정보 조회한 뒤 47만 건을 노트북에 내려받았음. 300여 건을 외부로 유출
하나SK카드	2011년 7월	9만7000여 건	직원이 고객정보를 개인 e메일로 보낸 뒤 일부를 외부업체에 넘겨
현대캐피탈	2011년 4월	175만 건	해커가 광고 메일 발송서버 등에 침입해 해킹 프로그램 설치한 뒤 개인정보 빼내

- 개인정보 유출, 자료 유출 등 각종 보안 사고 발생
- 가이드라인에 따른 망분리를 위한 VDI 도입
- 노후 PC 교체





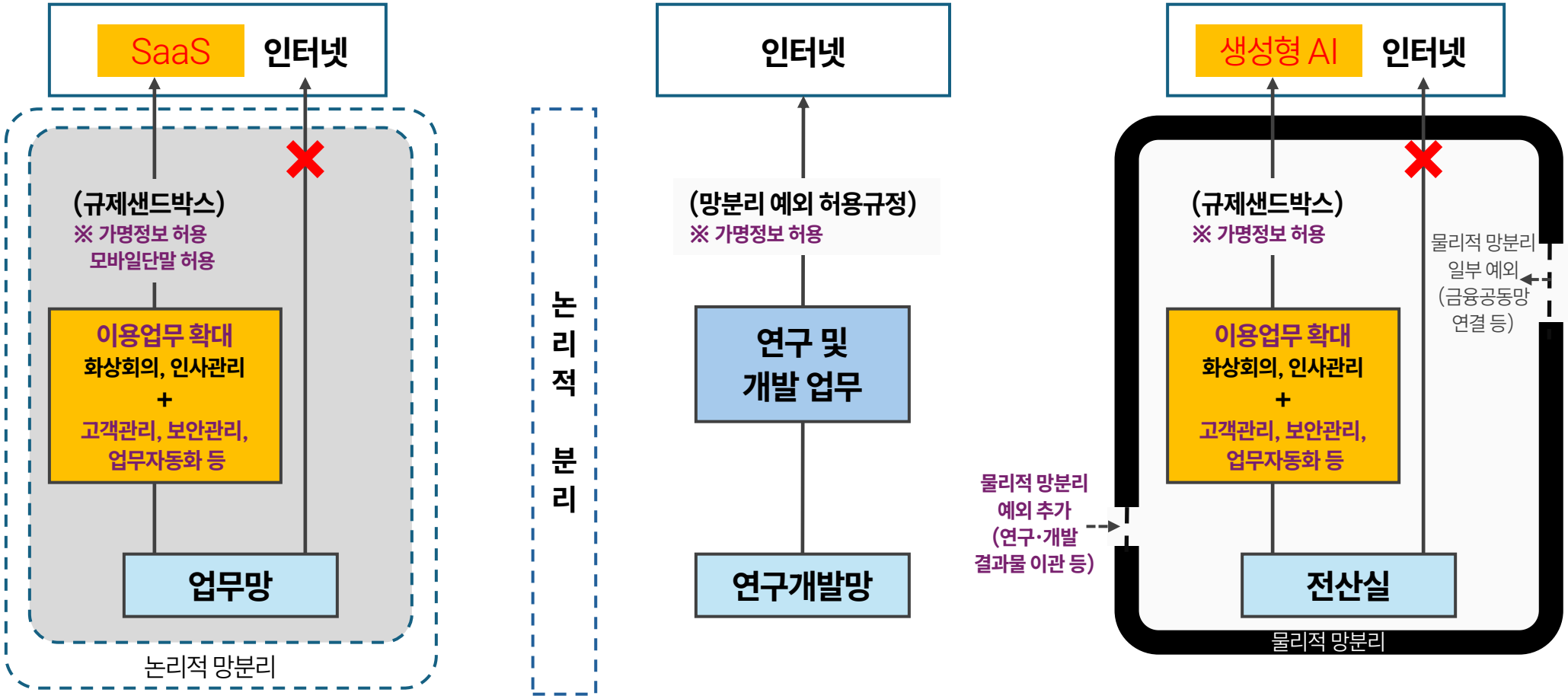


- 구글, 페이스북 등 글로벌 기업 및 국내 대기업의 성공적인 스마트워크 도입 사례 급증
- 쾌적하고 깔끔한 스마트 오피스 환경 관심
- 언제 어디서나 사용 가능한 유연한 근무에 대한 니즈 발생

IT업무환경 정책 변화

- 신기술 활용을 위한 정책 개선 (생성형 AI, SaaS 이용 등)
- 변화하는 보안 규제 : 자율보안-결과책임 원칙

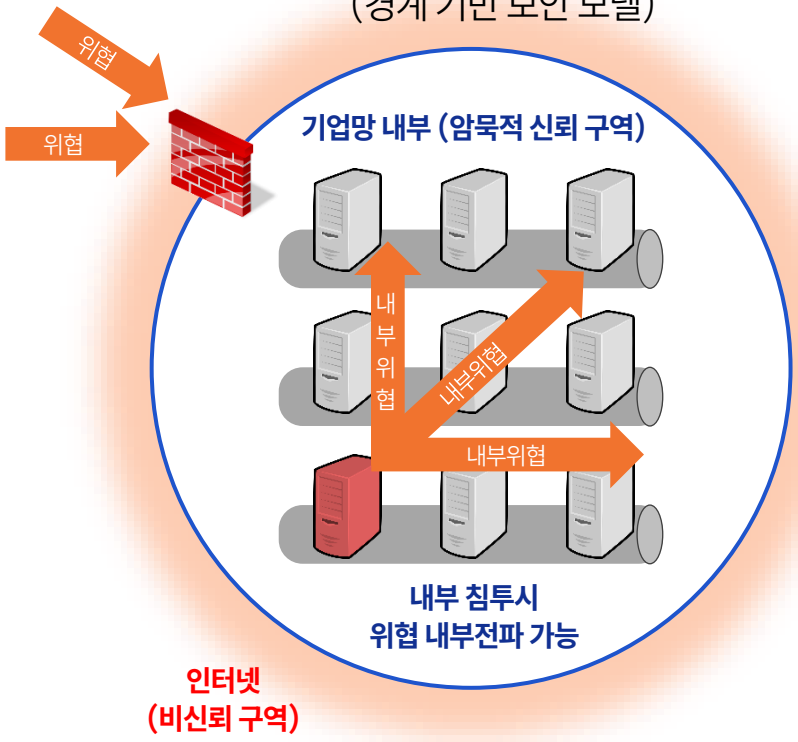
금융분야 망분리 개선안



보안에 대한 인식 변화

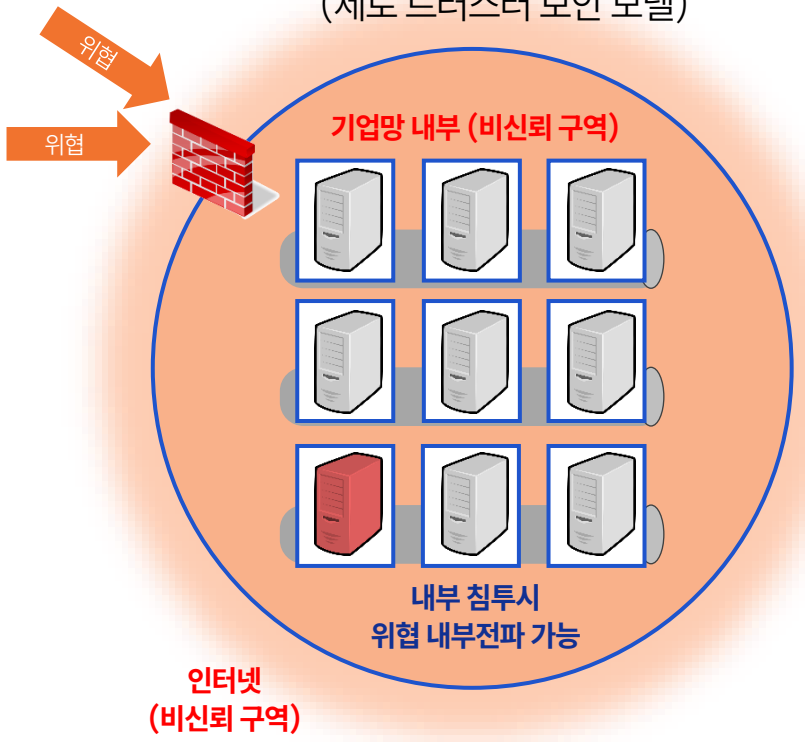
- 제로트러스트 보안 체계 전환의 필요성
- 새로운 보안 개념 : Never Trust, Always Verify

< 제로트러스트 도입 전>
(경계 기반 보안 모델)



- 경계를 기준으로 한번 인증된 기기나 사용자, 트래픽은 모두 허가

< 제로트러스트 도입 후>
(제로 트러스터 보안 모델)



- 네트워크 혹은 물리적 위치, 기기에 상관 없이 '무신뢰' 원칙

Zero Trust VDI

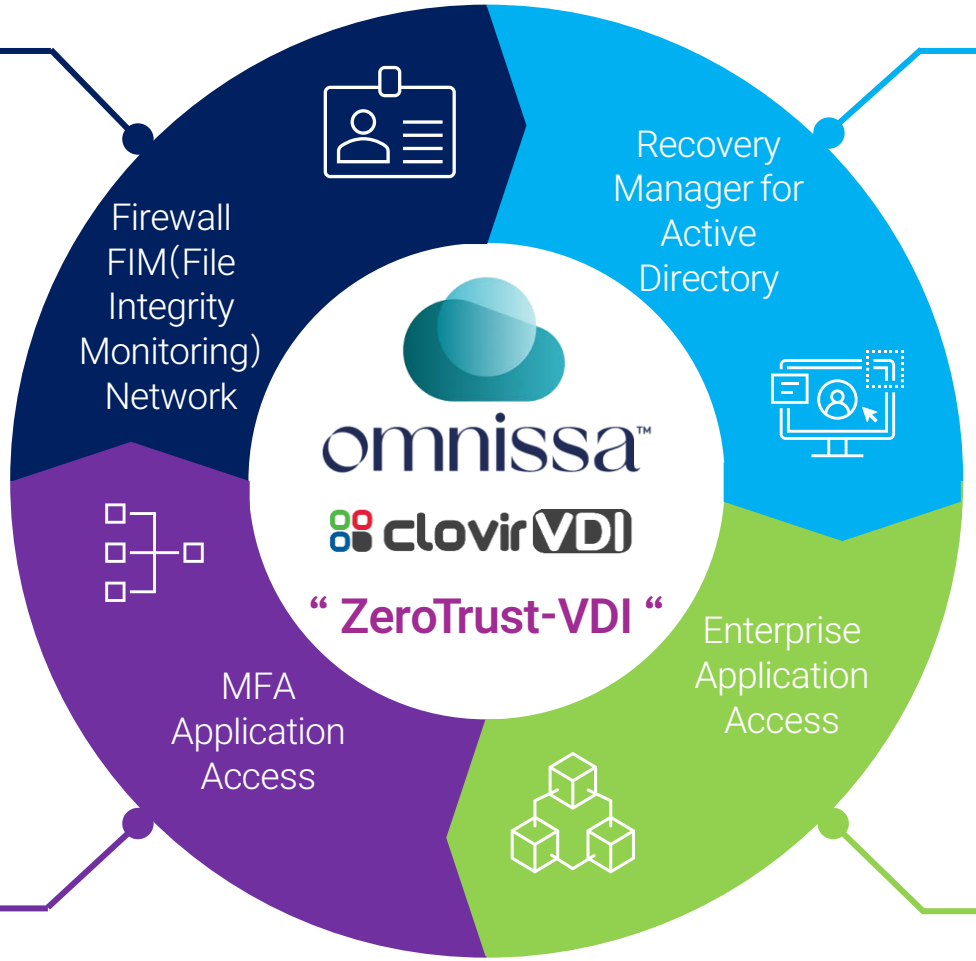
CIO Summit 2025

- 보안적으로 안전한 VDI 환경 제공

Network Micro-Segmentation

- VM간 방화벽 세분화 관리
- 파일 위변조 검사 기능
- Multi-Factor 및 Access 정책 관리
- VDI 접속시 2차 인증 기능

MFA(Multi-Factor Authentication)



Active Directory 위협 탐지, 복구

- ZeroTrust 네트워크 접속 솔루션
- VDI 외부 접근에 대한 보안 관리
- Active Directory 위협 탐지 & 복구
- 다양한 Multi Domain 백업 지원

Enterprise Application Access

Zero Trust VDI

- VDI의 다양한 서비스 카탈로그 기능을 제공하고 업무 데이터는 중앙에서 보관

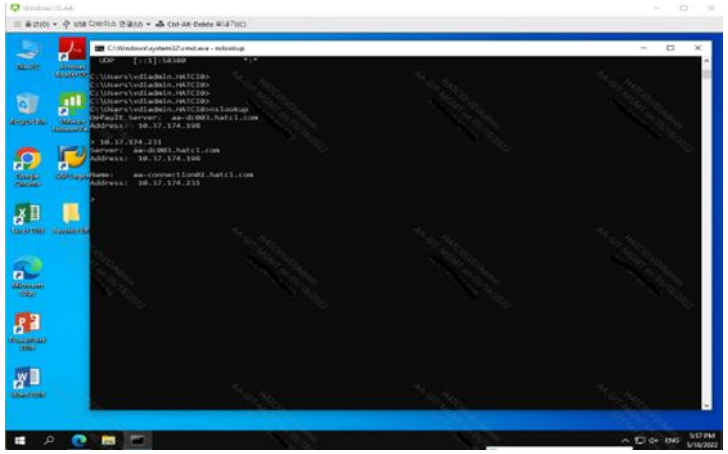


Zero Trust VDI

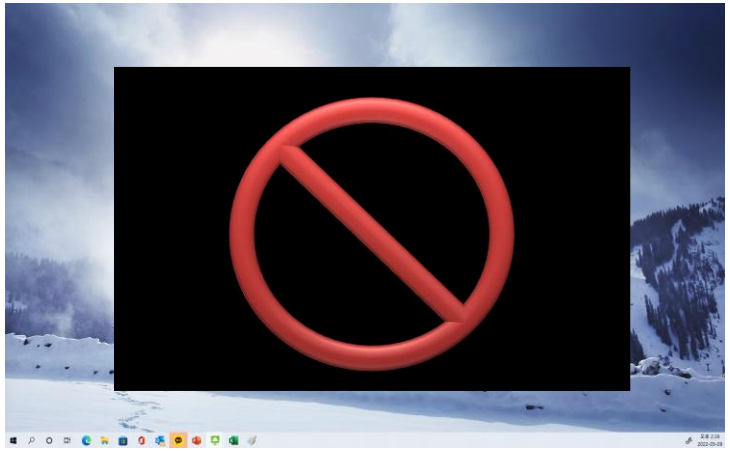
CIO Summit 2025

- 자료 유출 방지 - 사용자의 데스크톱 및 앱 가상화 환경에 대해 보안을 강화하여 자료 유출을 최소화

디지털 워터마크

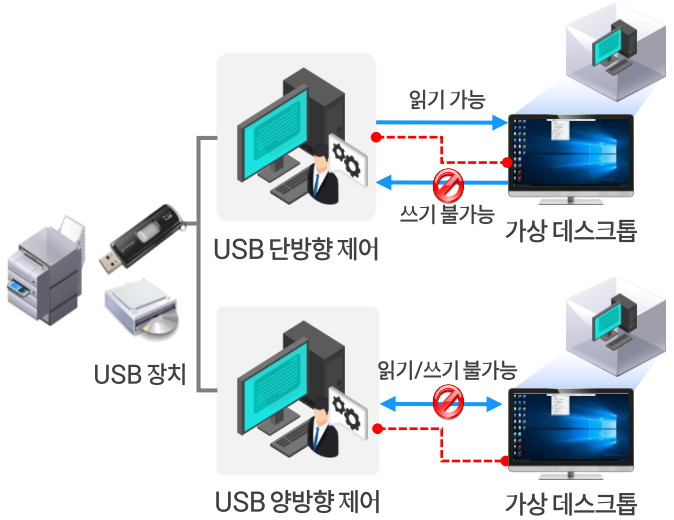


캡쳐 방지

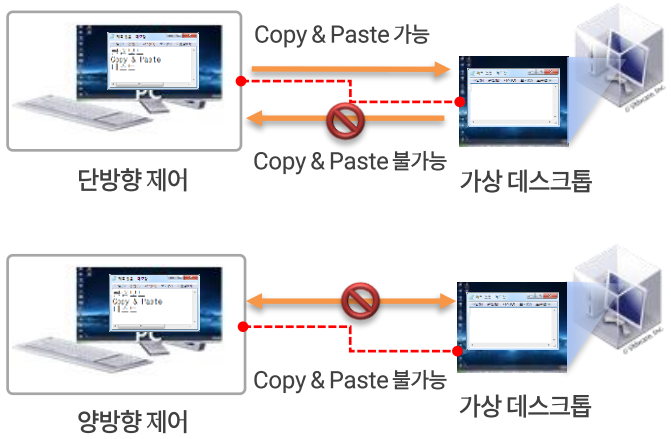


보안 강화

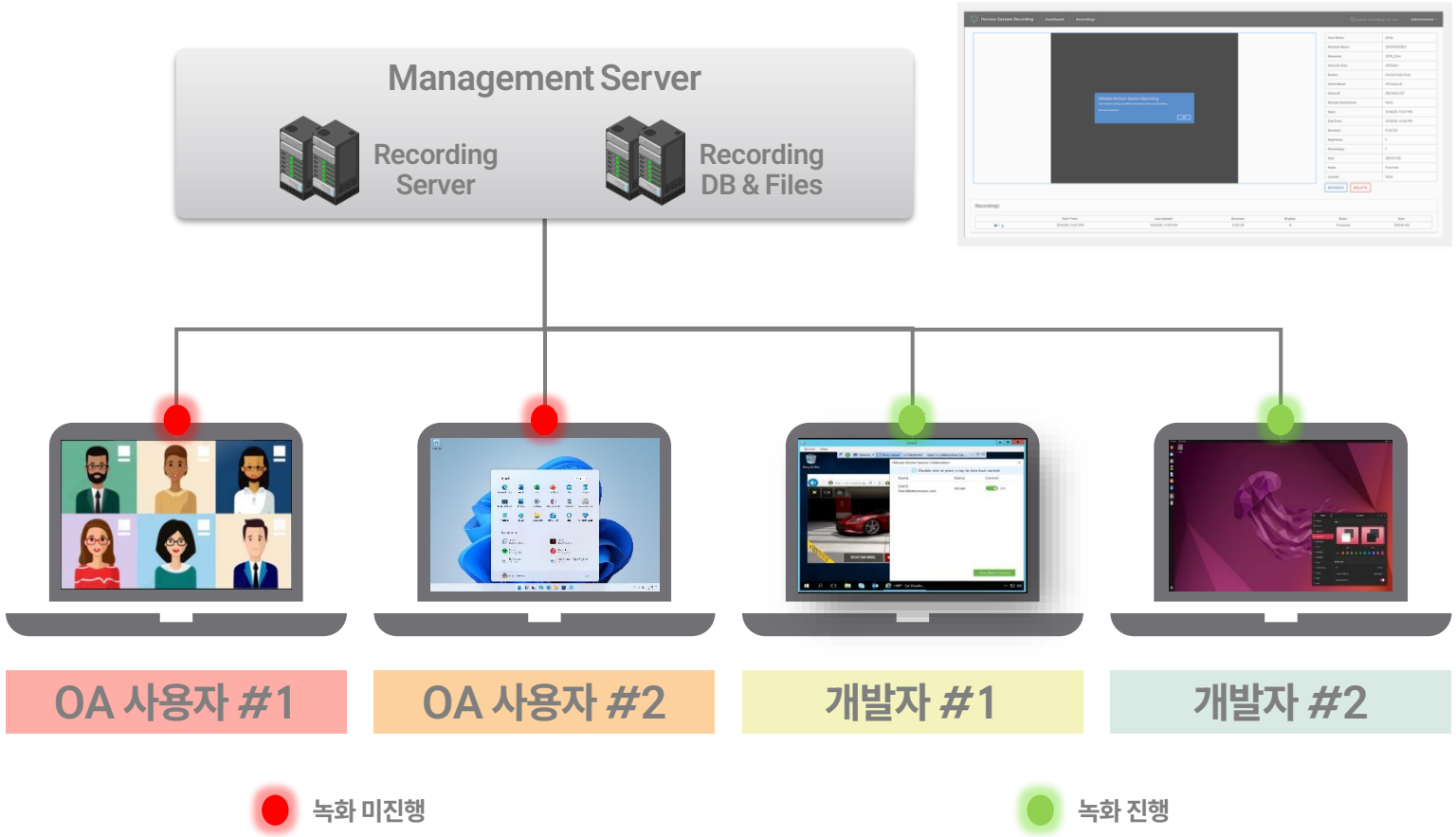
USB 제어



복사/붙여넣기 제어



- Session Recording - 사용자의 데스크톱 및 앱 가상화 세션을 기록하여 행위를 모니터링



[VDI 적용 이전의 설계환경 및 고민]

- 개발자를 위한 보안이 강화된 Windows OS 및 Linux OS 환경 필요
- 외주 개발자들의 행위에 대한 로깅이 필요
- OA 사용자와 차등 정책 적용 필요
- 내부 개발자와 외부 개발자에 대한 차등 정책 필요

[VDI 적용 이후 도입효과]

- OS별/ 버전별로 필요한 각각의 이미지를 부여
- Session Recording 기능을 활용하여 외주 개발자는 세션에 대한 로깅 진행
- 내부 개발자와 외부 개발자는 각각 다른 정책을 적용하여 보안 등급을 분리

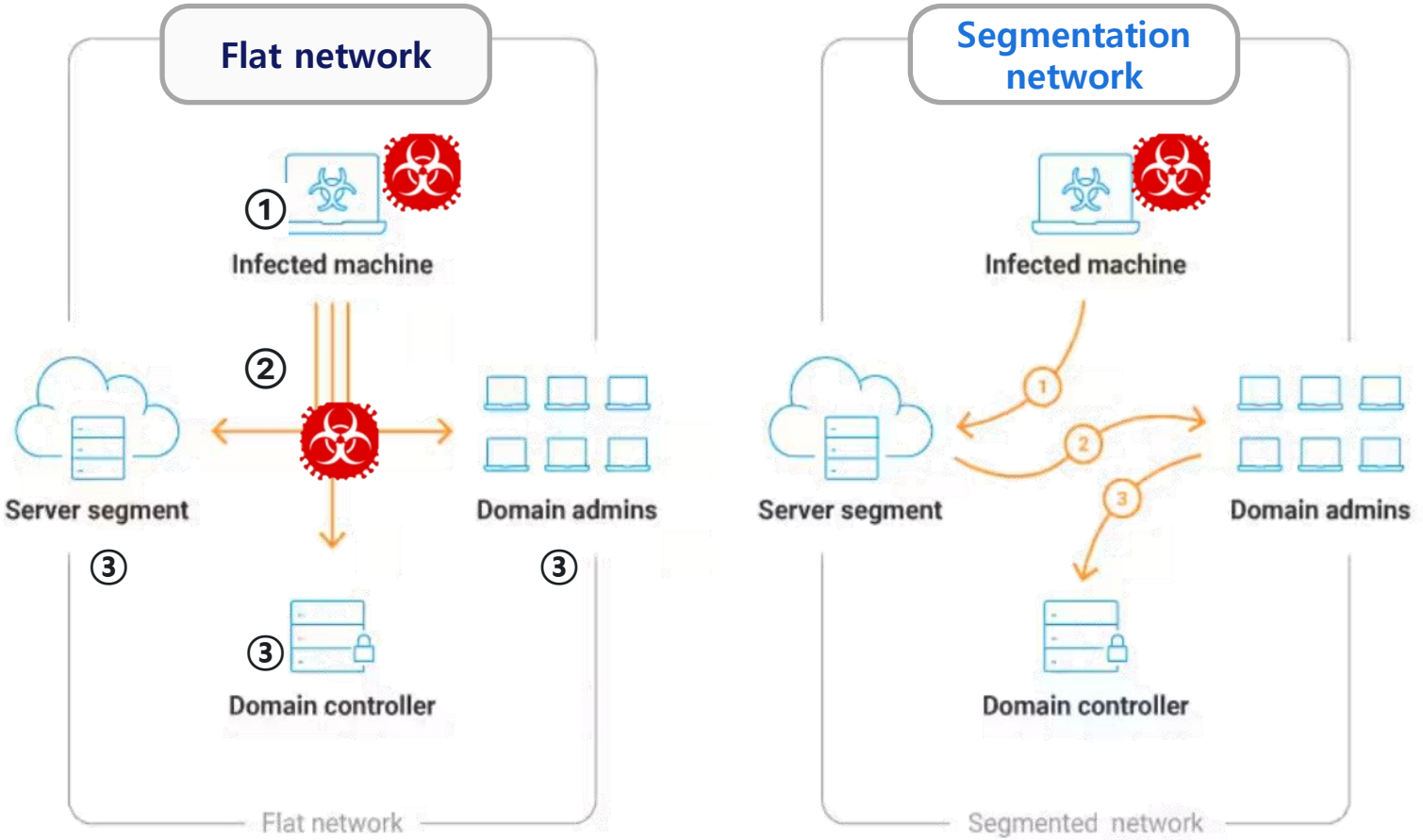
- Micro Segmentation 필요성과 효과

[사이버 공격 킬체인]

① 네트워크 초기 감염

② 측면 이동 수행

③ 침해 확산



[세그멘테이션을 통하여]

❶ 정책위반사항 모니터링

❷ 측면이동 공격 차단

➔ 침해 확산 방어

❸ 중요 애플리케이션 보안

- 소프트웨어적인 망분리와 주요 애플리케이션에 대한 구역화로 보안 강화

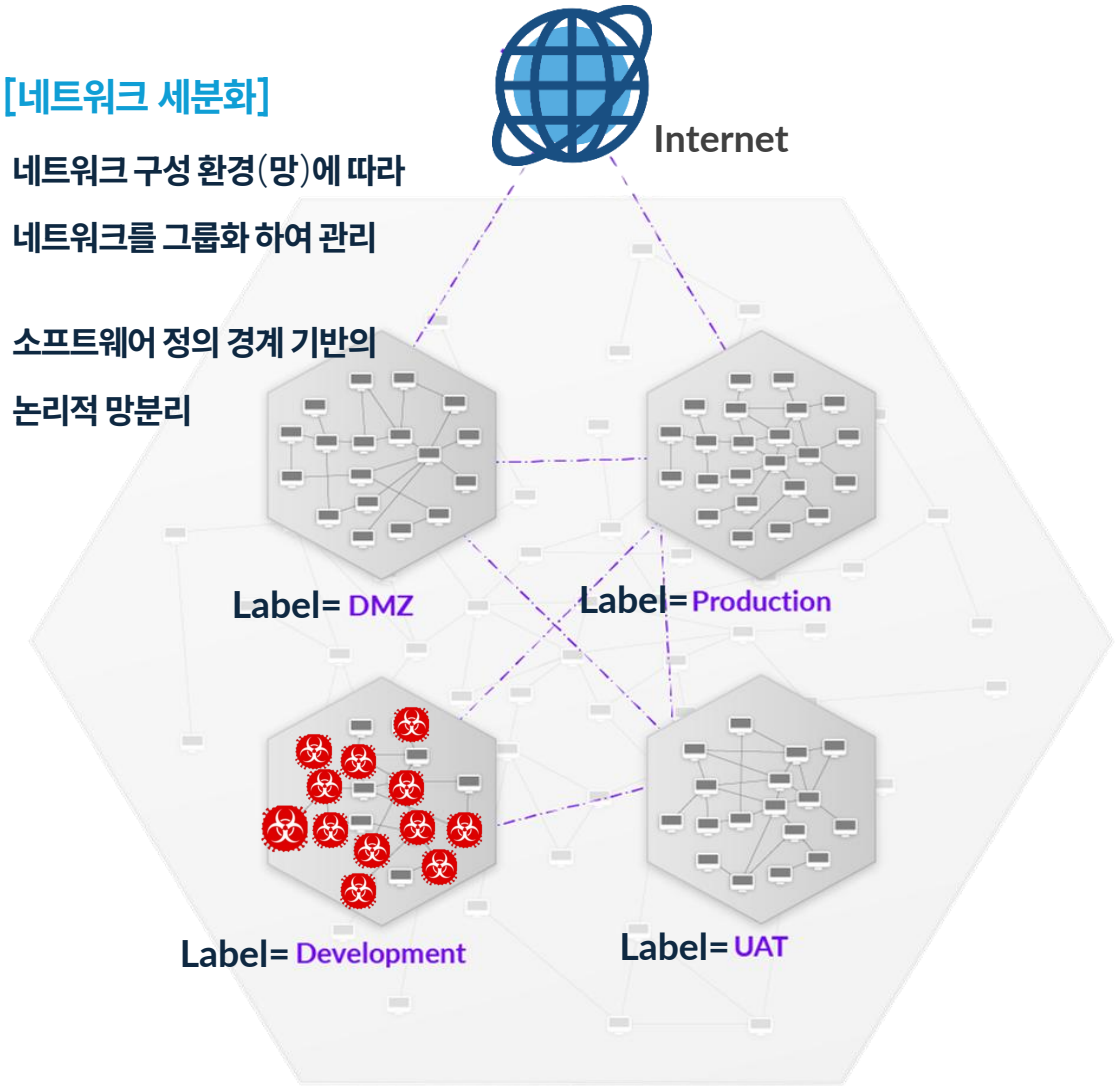
[네트워크 세분화]

네트워크 구성 환경(망)에 따라

네트워크를 그룹화 하여 관리

소프트웨어 정의 경계 기반의

논리적 망분리

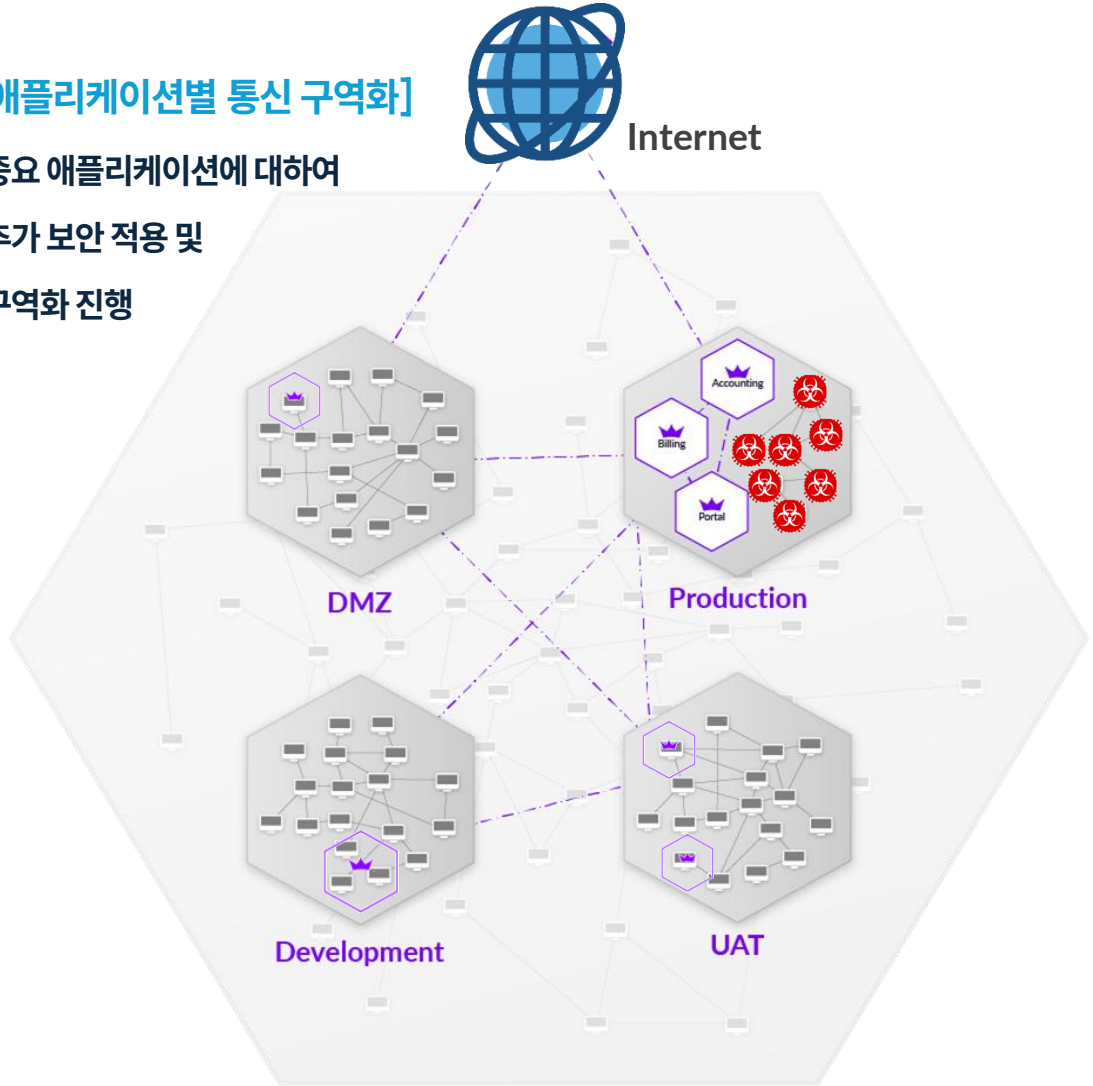


[애플리케이션별 통신 구역화]

중요 애플리케이션에 대하여

추가 보안 적용 및

구역화 진행



Zero Trust VDI

CIO Summit 2025

- 소프트웨어적인 망분리와 주요 애플리케이션에 대한 구역화로 보안 강화

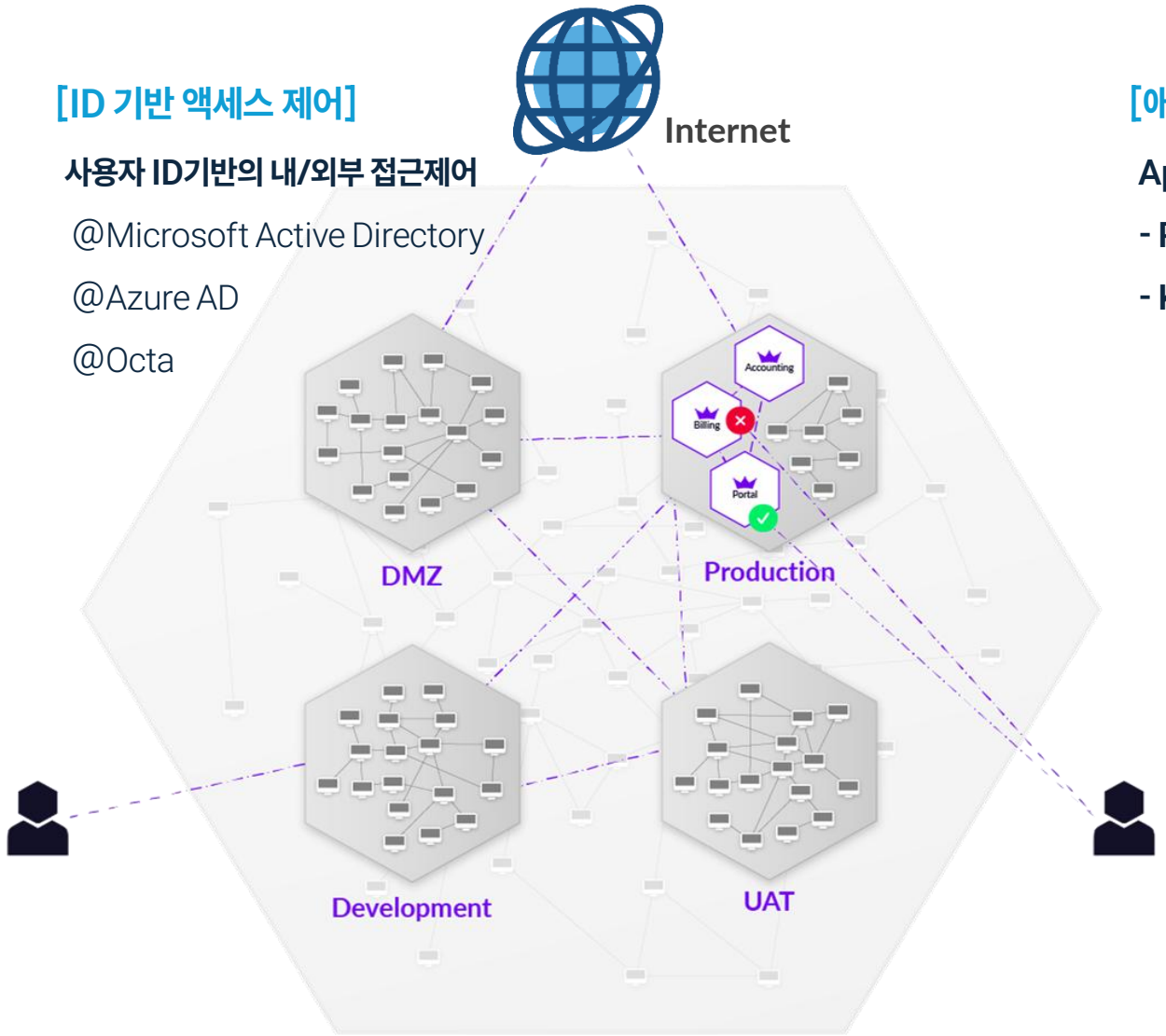
[ID 기반 액세스 제어]

사용자 ID기반의 내/외부 접근제어

@Microsoft Active Directory

@Azure AD

@Octa

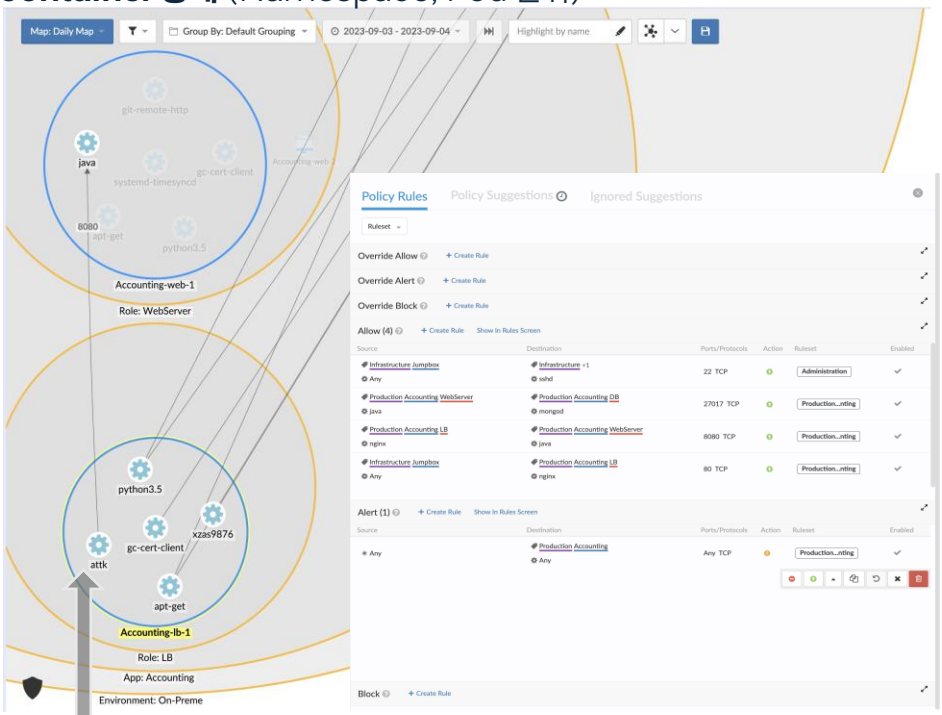


[애플리케이션별 통신 구역화]

Application 간 흐름 통제

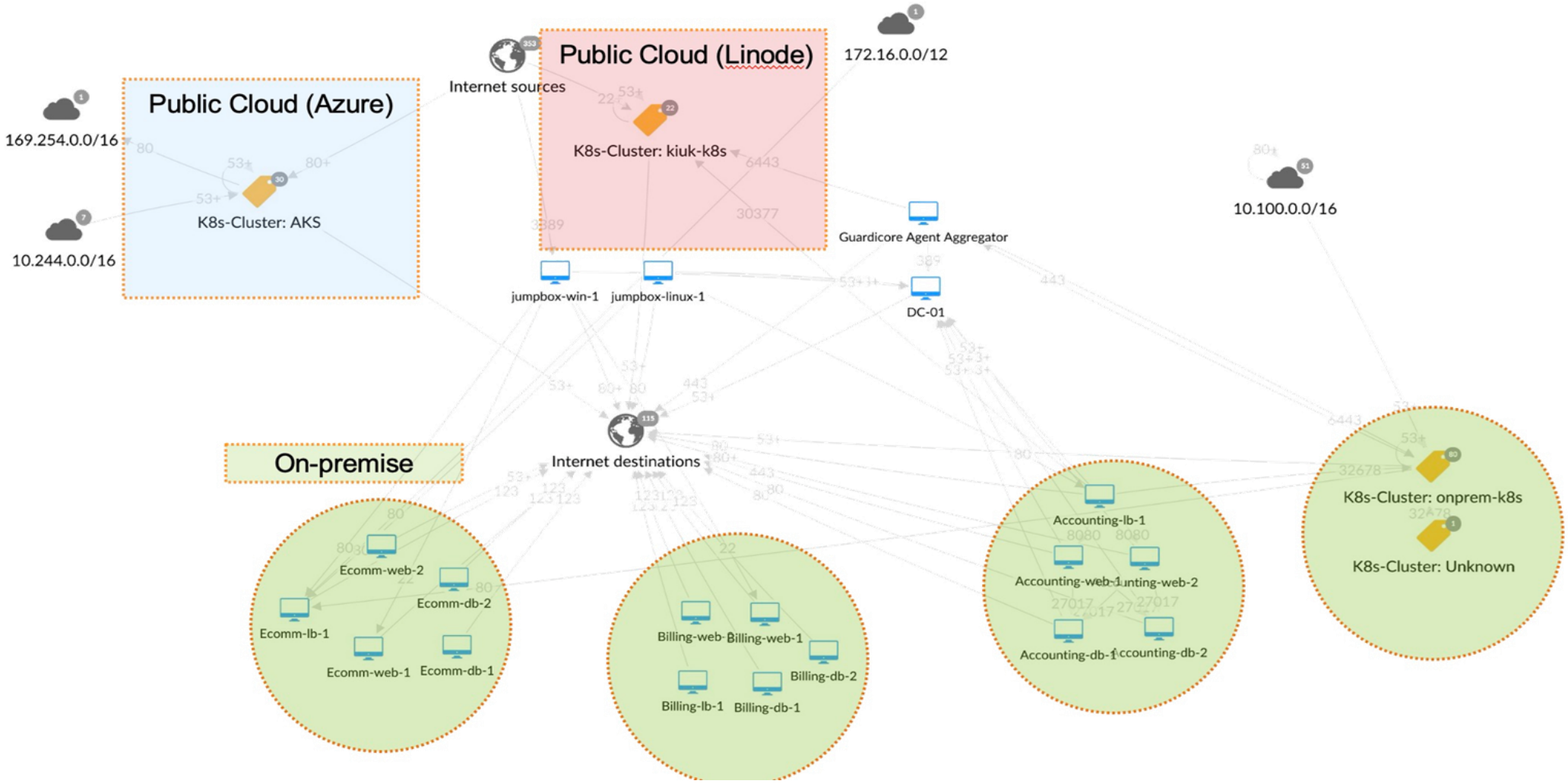
- Process 단위 통제 지원

- K8s-container 통제 (Namespace, Pod 단위)



Application Process Layer

- 모든 자산에 대한 Visibility & Enforcement



- 마이크로 세그멘테이션 기대효과



네트워크 가시성 확보

운영버든 및 오버헤드 감소
비식별 자산정보 확인



모든 인프라에 대한 지원

모든 인프라 환경에
동일한 정책 적용 및 운용



AI기반 정책 추천

현 시점에 맞는 정책 추천
및 완벽한 정책 완성



효율적인 운영 관리

고객의 자산 환경
단순화 및 효율적 관리

▪ 2차 인증 보안 플랫폼 필요성

해킹은 인증도용으로 시작

"국내 데이터 유출 사고 최초 공격 방법으로 '사용자 인증 정보 도용(약 20%)'에 가장 많아"

"2022년 국내 주요 기업 평균 해킹 피해액 43억 3400만원"

-IBM시큐리티 '데이터 유출 비용 연구 보고서' 2022

이용자 **ID/PW 유출 시**에도 생체인증, OTP를 활용한 **추가 인증 절차** 통과시에만 시스템 접속

보안정보 내부자 유출이 70%

"연간 주요 기업 정보 유출 피해액 56조 2000억원"

"산업 주요 자료 접근 및 유출 10명 중 9명이 기업 내부자"

-전국경제인연합회 2022,10
- 경찰청 국가수사본부 2021.11

생체인증 Motp 도입으로 이용자 간 **인증 정보(ID/PW) 공유 등 보안 위규 방지**, 로그인 **로그 관리** 등한 접속 기록 저장

비밀번호 정책의 낮은 실효성

"3개월에 한번씩 비밀번호 변경 권고하는 보안 정책?"

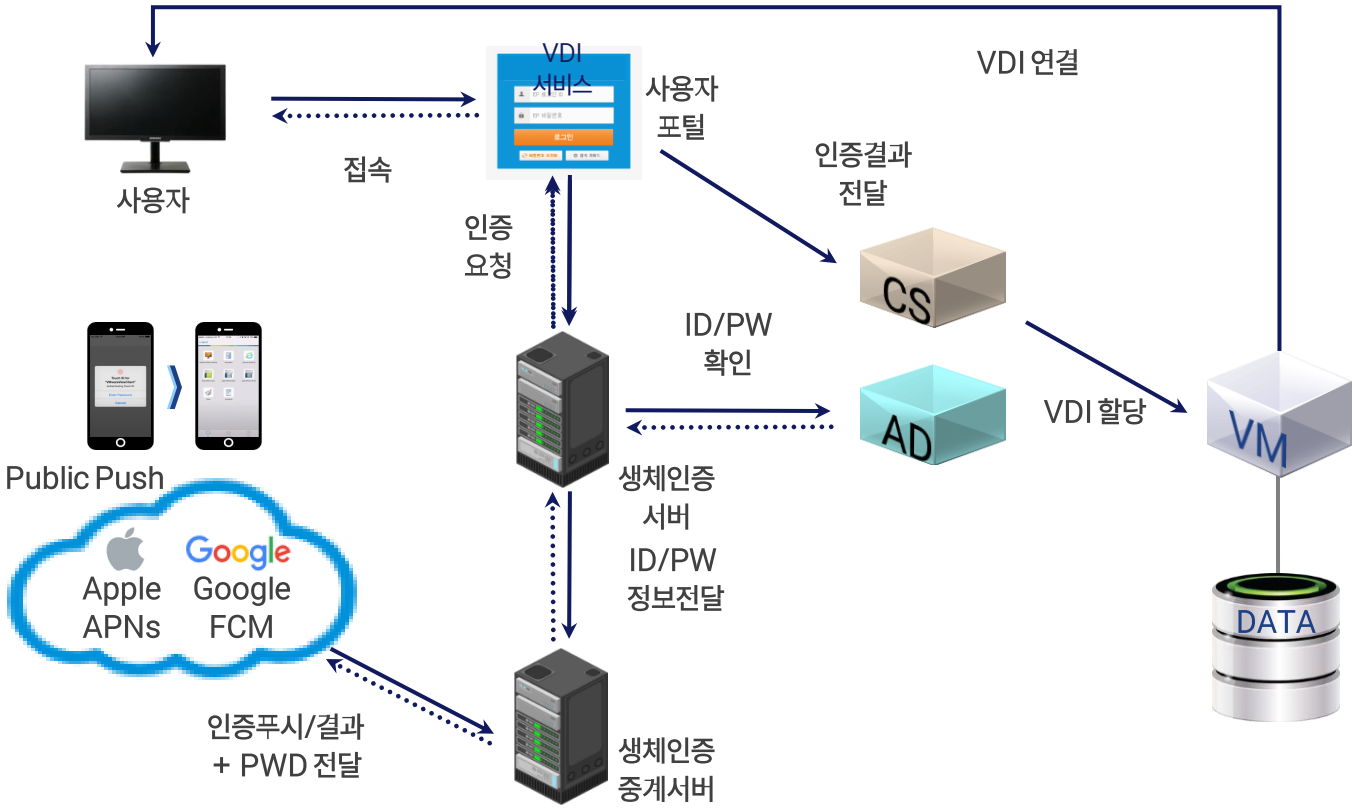
"비밀번호 자주 변경할 시 자꾸 잊어 결국 기억하기 쉬운 취약한 비밀 번호를 사용"

-영국 통신전자보안그룹 CESG, 2016

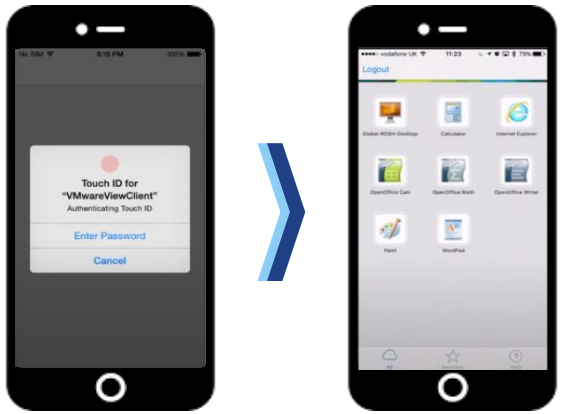
비밀 입력 필요 없는 **FIDO(생체인증)**와 30s/60s마다 바뀌는 **OTP(One Time Password)**통해 편리하고 안전한 로그인

Zero Trust VDI

- 업무시스템의 ID/PW 기반의 로그인 방식에 다양한 2차 인증(OTP, 생체인증, PUSH, QR인증 등)을 적용하여 사용자가 언제 어디서나 안전하게 업무시스템에 접근하도록 지원하는 2차 인증 보안 플랫폼



▶ 모바일에서 접속 시 등록된 지문 또는 안면 인식을 통한 편리성 제공



▪ 2차 인증 보안 플랫폼 장점 및 기대효과

멀티 인증방식 제공
FIDO인증, OTP 등 사용자의 사용환경에 따른 다양한 인증방식을 선택하여 제공

통합인증 구현
웹 애플리케이션, VPN 등 다수의 시스템에 대한 통합 인증 체계 마련

가장 쉽고 편리한 인증
도입 후 바로 적용이 가능하며 사용자 포탈 지원

검증된 솔루션
300여개 이상의 고객사의 업무시스템 추가 인증용으로 운영 중

조회 및 리포팅
관리자, 사용자별로 상세한 정보 조회가 가능하며 관련 리포팅 제공

보안 강화
데이터 암호화, 통신구간 암호화로 스니핑 차단 AES256, SHA2, PBKDF2 적용

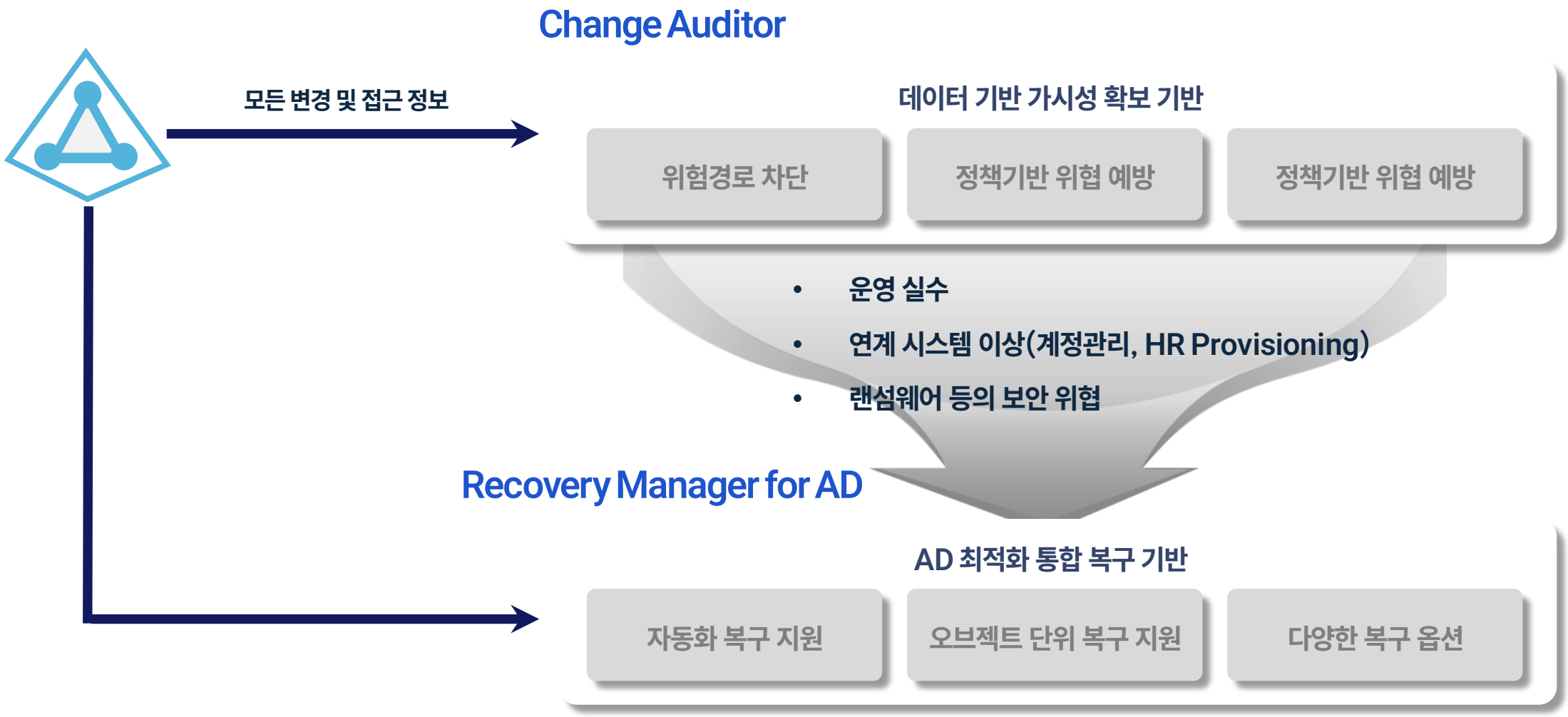
업무 연속성 확보
사용 불가 시에 다양한 비상대처 인증 수단으로 전환하여 원활한 접속 가능

관리 효율성
다양한 관리기능을 웹 기반으로 최소한의 업무로 최대의 관리업무 제공

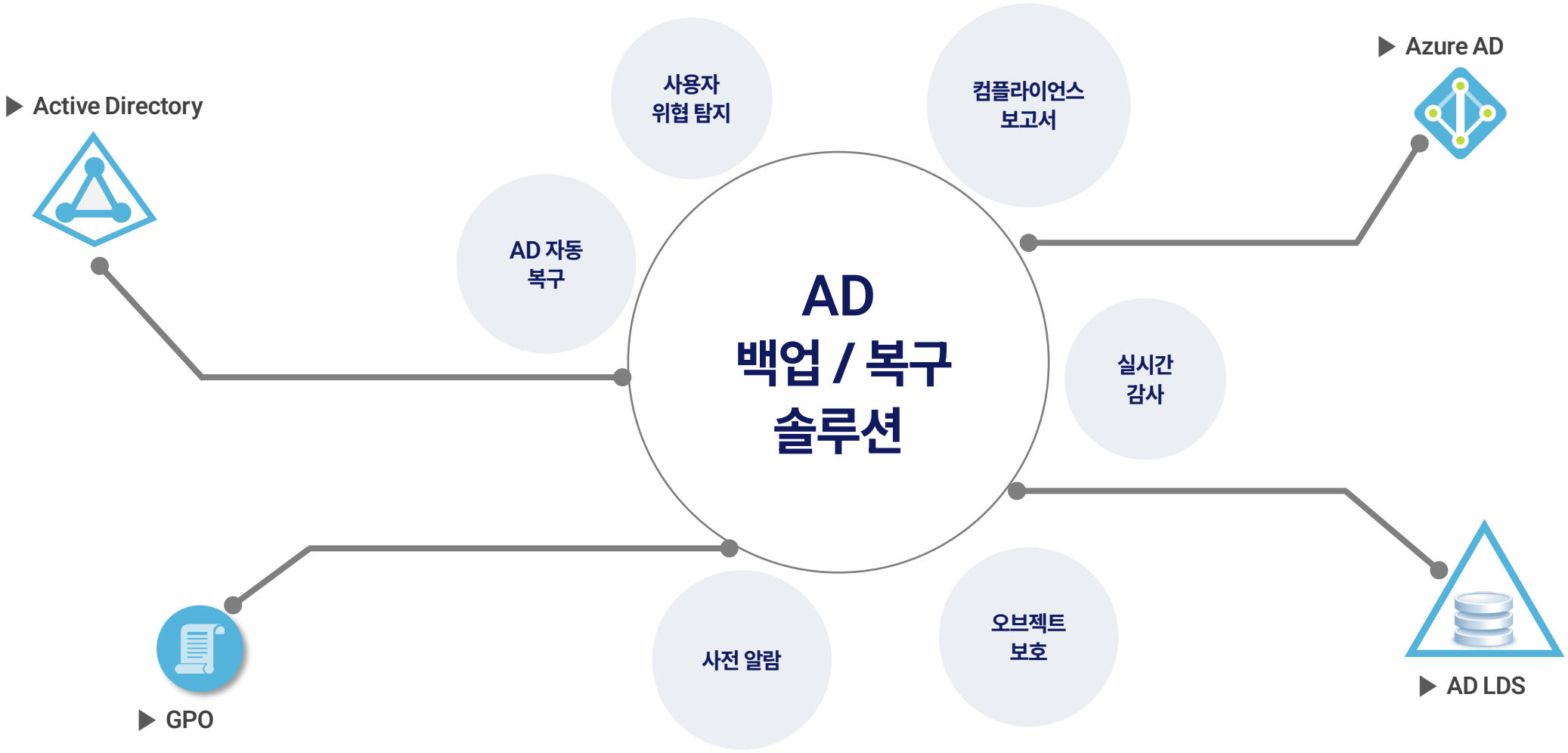
접속 이력 관리
발급업무에 대한 효율성 향상과 발급 이력 조회 기능 제공

비대면 발급시스템
재택근무, 원격근무 등 언택트 업무환경을 위한 시스템 구축

- AD 보안 및 복구 전략


Change Auditor
모든 변경 및 접근 정보
데이터 기반 가시성 확보 기반
위험경로 차단
정책기반 위협 예방
정책기반 위협 예방
운영 실수
연계 시스템 이상(계정관리, HR Provisioning)
랜섬웨어 등의 보안 위협
Recovery Manager for AD
AD 최적화 통합 복구 기반
자동화 복구 지원
오브젝트 단위 복구 지원
다양한 복구 옵션

- Object 단위로 신속한 Active Directory 백업 및 복구



▪ AD 백업/복구 솔루션 장점 및 기대효과

감사정보의 안전한 보존
별도의 DB에 저장되어 관리자로부터 관리 분리

정확하고 상세한 감사정보
강력한 검색, 필터링 및 정밀한 감사 설정 가능

실시간 이벤트 처리
심각한 보안 사고 시 즉시 탐지 및 대응

자체 감사 이벤트 생성
네이티브(Native) 이벤트에 의존하지 않고 고유 이벤트 생성 및 제공

자동 AD 복구
침해 시 AD를 이전 시점으로의 신속한 데이터 복구 지원

중요 데이터 보호 강화
권한 있는 그룹, GPO 및 민감한 사서함을 포함하여 AD, Exchange 및 Windows 파일 서버 내의 중요한 데이터에 대한 변경으로부터 보호

감사 세부 정보의 정규화
사용 불가 시에 다양한 비상대처 인증 수단으로 전환하여 원활한 접속 가능

변경 사항에 대한 가시성
온프레미스 또는 클라우드에 관계없이 모든 변경 사항에 대한 가시성 확보

보안 위협 모니터링
자격증명 도용 및 AD 데이터베이스 복사본과 같은 악용을 감사 및 차단

빠르고 간편한 설치 및 운영
모든 서버를 중앙에서 관리하여 에이전트 자동 배포 및 관리가 가능

▪ AD 백업/복구 솔루션 장점 및 기대효과

감사정보의 안전한 보존
별도의 DB에 저장되어 관리자로부터 관리 분리

정확하고 상세한 감사정보
강력한 검색, 필터링 및 정밀한 감사 설정 가능

실시간 이벤트 처리
심각한 보안 사고 시 즉시 탐지 및 대응

자체 감사 이벤트 생성
네이티브(Native) 이벤트에 의존하지 않고 고유 이벤트 생성 및 제공

자동 AD 복구
침해 시 AD를 이전 시점으로의 신속한 데이터 복구 지원

중요 데이터 보호 강화
권한 있는 그룹, GPO 및 민감한 사서함을 포함하여 AD, Exchange 및 Windows 파일 서버 내의 중요한 데이터에 대한 변경으로부터 보호

감사 세부 정보의 정규화
사용 불가 시에 다양한 비상대처 인증 수단으로 전환하여 원활한 접속 가능

변경 사항에 대한 가시성
온프레미스 또는 클라우드에 관계없이 모든 변경 사항에 대한 가시성 확보

보안 위협 모니터링
자격증명 도용 및 AD 데이터베이스 복사본과 같은 악용을 감사 및 차단

빠르고 간편한 설치 및 운영
모든 서버를 중앙에서 관리하여 에이전트 자동 배포 및 관리가 가능

■ 원격 접속 서비스의 고려사항 및 해결방안

보안성

- 공개된 VPN장비의 IP / Port에 대한 공격 발생
- 증가하는 어플라이언스 취약점 공격
- Supply chain attack, Lateral movement, DDoS 공격
- 선 연결/후 인증 방식의 접속보안 취약점

✓Identify 기반으로 제로 트러스트 모델 지원

✓**애플리케이션 단위의 마이크로 세그먼테이션을 통한 보안 등급별 접속 권한 관리**

✓In-bound 트래픽 구성으로 공격 노출 최소화 (블랙 클라우드 구성으로 내부인프라 스캔 방지)

편의성

- 정책 추가/변경 시, 추가 보안설정 or 별도 S/W 설치
- 신규/증설 시 물리서버 및 네트워크 구성 변경 필요
- 증가하는 클라우드 서비스에 대한 지원 미흡
- VPN 구성 및 운영에 일정기간 소요

✓사용자 단말에 S/W 설치 불필요 (agent/agentless 제공)

✓관리자가 클라우드에서 애플리케이션을 신속하게 생성, 배포 및 확장하도록 지원

✓라이선스 계약만으로 손쉽게 즉시 확대 적용

성능

- 순간적인 대량 접속자 발생시 시스템 성능 저하 및 서비스 중단
- 파일 전송 시 속도 저하 및 끊김 문제
- 해외 등에서의 사용자 경험지수 낮음

✓최대 클라우드 인프라로 시스템 성능 문제 해결

✓**TCP 최적화, 경로 최적화 등 다양한 가속 서비스 연동으로 사용자 속도 만족도 제공**

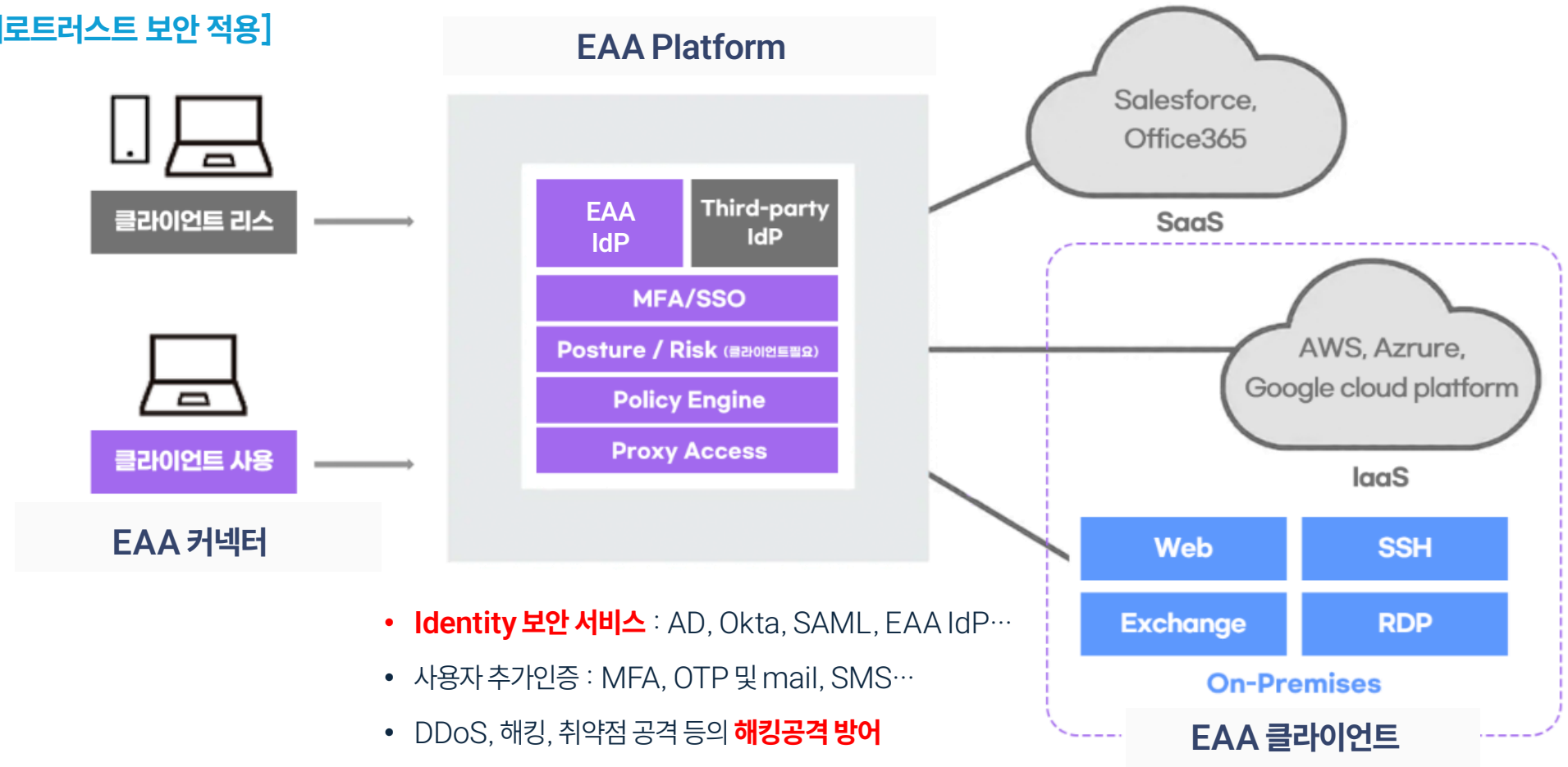
✓해외 등에서의 원격접속 성능이 크게 향상

Zero Trust VDI

CIO Summit 2025

- 클라우드 내의 ID 인식 프록시로 시간과 장소에 상관없이 사용자가 원하는 애플리케이션에 안전하게 접속할 수 있는 빠르고 안전한 원격 보안 접속 서비스를 제공

[원격접속 및 제로트러스트 보안 적용]



- **Identity 보안 서비스** : AD, Okta, SAML, EAA IdP…
- 사용자 추가인증 : MFA, OTP 및 mail, SMS…
- DDoS, 해킹, 취약점 공격 등의 **해킹공격 방어**
- 경로 최적화를 통한 **가속기능** 기본 제공

▪ EAA 솔루션 장점 및 기대효과

원격 보안 접속 강화
방화벽, 보안 그룹의 모든 인바운드 트래픽 차단하고
인터넷에서 기업 인프라가 보이지 않게 구성

애플리케이션 기반
사용자에게 전체 네트워크가 아닌
애플리케이션 별 정확한 접속 권한 부여

언제 어디서나 접속
클라우드 내의 ID 인식 프록시로 언제든
사용자가 원하는 애플리케이션에 안전하게 접속

멀티 클라우드의 유연성
안전한 단일 포털을 통해 AWS, Azure,
Google Cloud와 인프라 전반에서 접속 제어

다양한 인증 방식
간편하고 안전한 멀티 팩터 인증(MFA)으로
무단 접근 최소화

편리한 운영
네트워크 또는 인프라를 변경 없이 인력 변경을
적용하고 사용자 별 접속 허용 가능

똑똑한 의사 결정
사용자, 디바이스 등에 대한 정보를 실시간으로
수집하여 접속 허용 여부에 대한 정확한 판단

신속한 대처
단일 포털을 통해 단 몇 분만에
새로운 애플리케이션 & 사용자 설정

사용자 활동 확인
모든 사용자의 정보 및 수행 정보 기록으로
컴플라이언스 준수

비용 및 복잡성 감소
클라우드 전송 서비스로 간소화되어
가상 또는 물리적 어플라이언스 관리 불필요