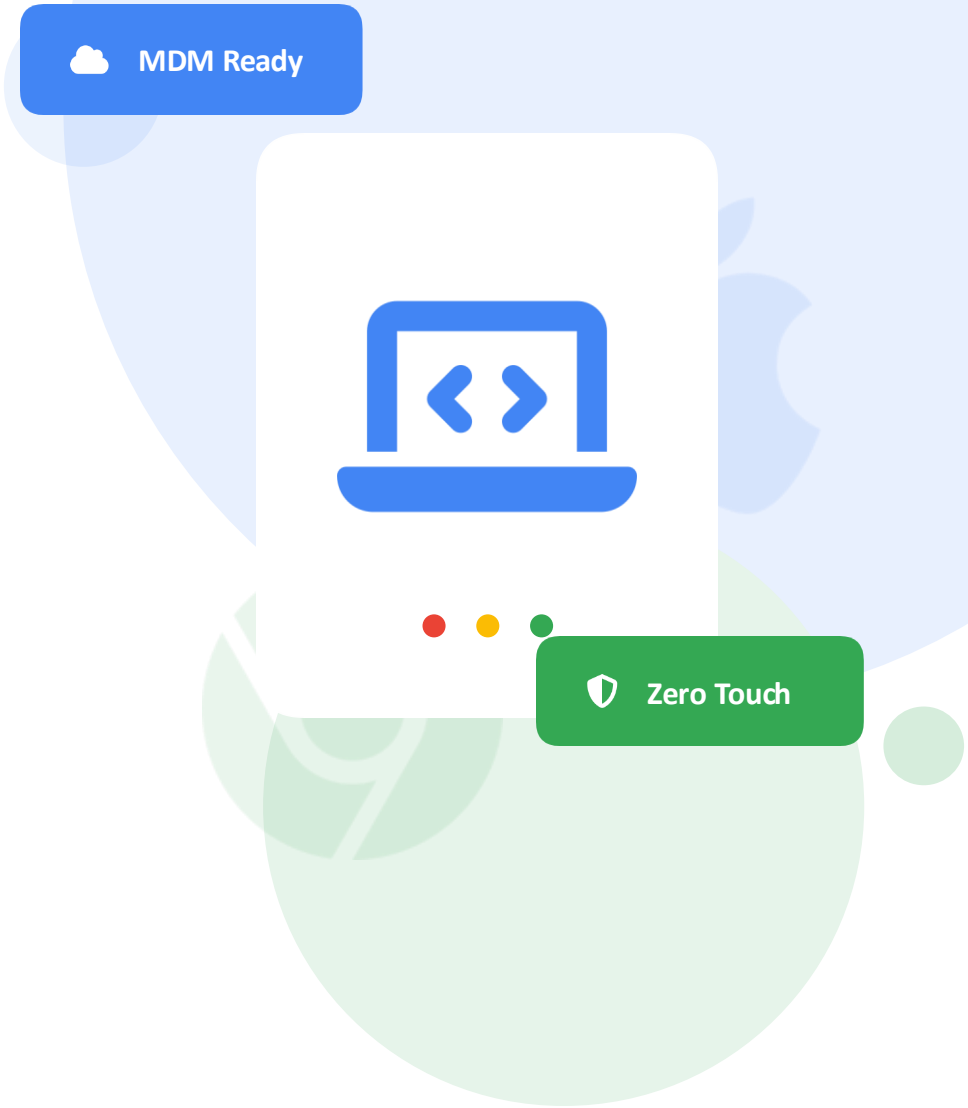
Deployment Strategy

Mac & Chrome OS

DEP로 배포 지옥 탈출하기

Doyoung Park



Doyoung Park

Security Engineer

Flipster, Security Team

Core Competencies

Enterprise Security

전사 보안 정책 수립 및 보안 엔지니어링을 통한 안정적인 보안 환경 구축

Automation & Engineering

반복적인 보안 업무 자동화 및 인프라 엔지니어링을 통한 운영 효율성 극대화

Deployment Strategy

사용자 경험(UX) 개선을 통한 Seamless한 업무 환경 제공

> "보안은 강력해야 하지만, 사용자는 그것을 느끼지 못해야 합니다."

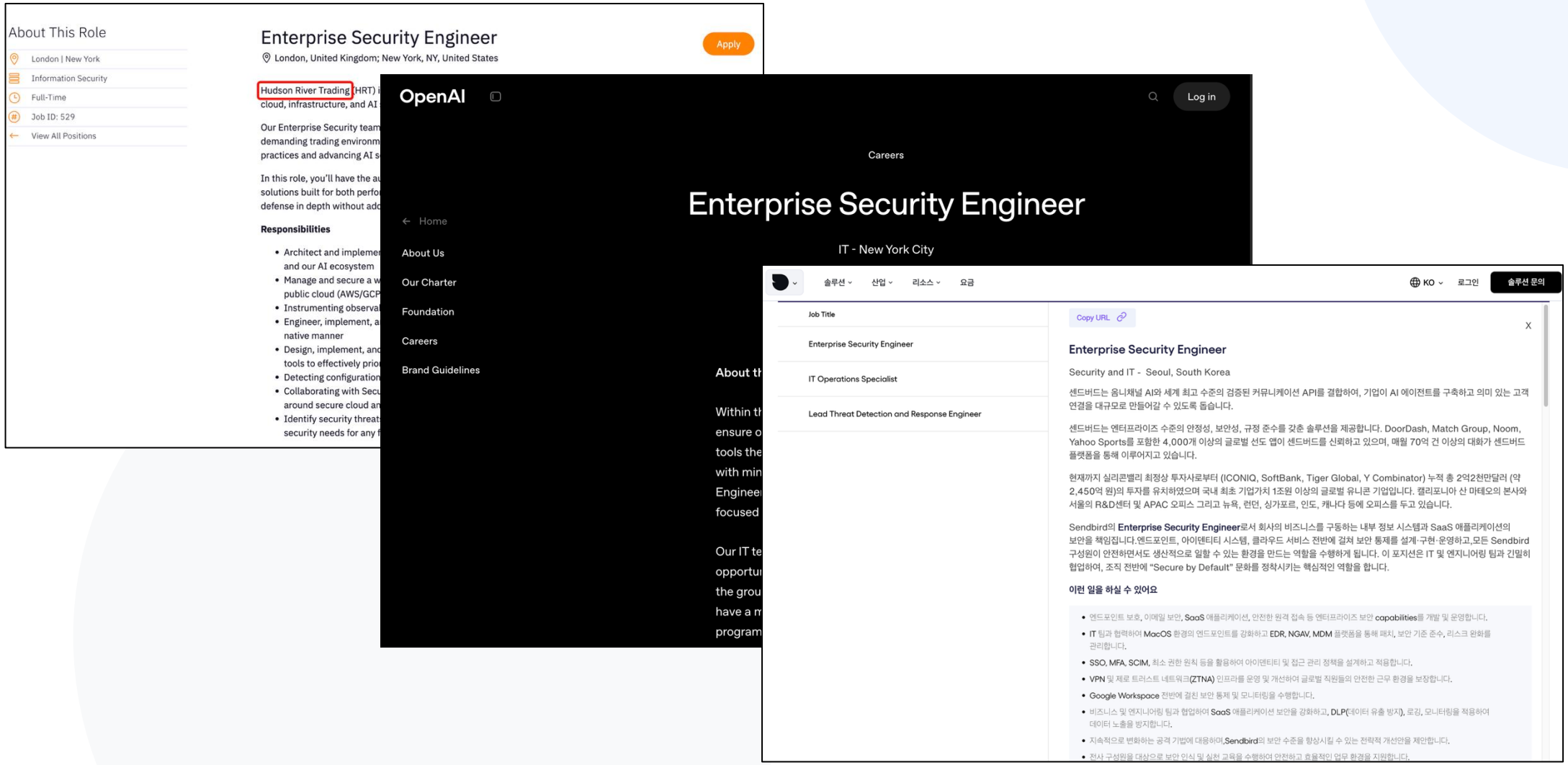
Role Definition

Enterprise Security Engineer

Policy | Operations | Automation | Deployment

Professional Path

Careers



About Company

Flipster

Crypto Derivatives Exchange

글로벌 암호화폐 파생상품 거래소로서
빠른 실행 속도와 강력한 보안을 자랑합니다.
전 세계 사용자들에게 최적의 트레이딩 환경을 제공합니다.

Global Market

전 세계 사용자 대상 서비스

ISO 27001

정보보호 경영시스템 인증

VARA in Dubai

규제 준수 및 라이선스

200+ Members

글로벌 임직원 및 엔지니어

Our Strengths

Company Advantages

Work Smart,
Work Securely

우리는 물리적인 제약 없이 전 세계 어디서나 일할 수 있는 환경을 제공합니다.
자동화를 통해 효율성을 극대화하고, 빠른 실행력을 바탕으로 혁신을 만들어냅니다.

Security Focus

사용성을 해치지 않는 보안

Automation

반복 업무 자동화 및 엔지니어링

Agile & Fast

빠른 의사결정과 실험 정신

Remote-first

시공간 제약 없는 협업 문화

원격이라 좋을 것 같지만 우리는 보안을 다뤄야 하는

환경의 차이

Office Based

On-premise Environment

- 네트워크 신뢰 기반 (Trust Network)
- NAC(접근 제어) 적용 용이
- 물리적 통제 및 자산 관리 가능
- 사내망 내부 = 안전지대

VS

Remote Based

Distributed Environment

- 네트워크 불신 기반 (Zero Trust)
- NAC 적용 및 통제 어려움
- 디바이스 자체 신뢰(Device Trust) 핵심
- 공용 와이파이 등 통제 어려운 외부 위협 노출 대응

Pain Points

원격 보안에 대한 부재 NAC 배제

기존의 네트워크 중심 보안 통제가 불가능한 환경에서 발생한 주요 문제점들입니다.

무제한 접근

Google Factor만 있으면 전 세계 어디서나, 어떤 랩탑으로든 회사 네트워크에 접근이 가능합니다.

Endpoint 미설치

보안 에이전트 설치 없이도 접속이 허용되어, 검증되지 않은 기기가 내부망에 진입할 수 있습니다.

가시성 부재

FileVault(디스크 암호화)나 OS 버전 등 기기의 중요 보안 파라미터가 설정되어 있는지 확인이 불가능합니다.

MDM 설치 저항

당시 낮은 보안 인식으로 인해 사용자들이 MDM 설치를 감시로 오인하거나 거부감이 있었습니다.

SSO(Okta)의 한계

SSO 도입은 접근 기기 수만 줄였을 뿐, 배포의 일관성이나 기기 자체의 무결성은 해결하지 못했습니다.

불명확한 가이드

실제 맥북을 수령한 뒤 사용자가 무엇을 설치하고 설정해야 하는지 명확한 프로세스가 부재했습니다.

Solution Strategy

원격 보안을 위한 개선

1차 시도: SSO (Okta)

접근 제어 중심의 해결책

⚠ 접근 기기 수 감소

인가된 사용자만 접근 가능하지만, 기기의 상태는 확인 불가

✕ 배포 일관성 부족

사용자마다 환경 설정이 제각각이며 중앙 관리가 어려움

? "무엇을 해야 하나요?"

기기 수령 후 초기 세팅 가이드 부재로 인한 사용자 혼란

→

Recommended

최종 해결책: DEP & Zero Touch

기기 무결성 및 자동화 중심

✓ 수령 즉시 정책 자동 적용

ABM 기반 Zero Touch로 전원 ON과 동시에 MDM 등록

보안 파라미터 강제화

FileVault, OS 버전 등 필수 보안 설정 강제 적용

Seamless User Experience

로그인만 하면 모든 설정 완료, 사용자 개입 최소화

Part 2

Device Enrollment Program (DEP) on macOS

macOS | Zero Touch | MDM | Security

Process Overview

Mac Device Enrollment Program Flow

법인 구매

구매팀에서 Apple 기기 법인 구매 (ABM 등록)

Wi-Fi 연결

기기 활성화를 위한 인터넷 연결 필수

Profile 배포

MDM 설치를 위한 Profile 자동 다운로드 및 설치

완료

보안 설정 적용 및 필수 소프트웨어 자동 설치

Core Concept

“전원을 켜고 인터넷에 연결되는 순간, Apple 서버가 우리 회사 MDM으로 전달”

Mac 배포의 핵심: ABM & DEP

ABM + DEP 등록

기기 구매 시 법인을 통해 구입한다면
"이 기기는 Flipster의 소유다"라고
Apple 서버에 영구적으로 등록됩니다

ADE 자동 할당

Automated Device Enrollment를 통해
사용자가 별도 설치를 하지 않아도
MDM 서버 정책을 자동으로 수신합니다

Setup Assistant

Siri 설정, Apple ID 로그인 등
불필요한 단계를 스킵(Skip)하고
바로 로그인 화면으로 진입합니다

Setup Strategy

Mac DEP 적용 : Admin Side

필수 선행 사항

성공적인 DEP 도입을 위한 준비 단계

ABM 계정 및 MDM 연동

Apple Business Manager 계정 생성 및 사내 MDM 서버와의 토큰 교환/연동 필수

법인 구매 라우팅 (Routing)

GA/구매팀과 협업하여 Apple 공인 리셀러를 통해 구매하도록 프로세스 일원화

DEP 자동 할당 규칙 설정

구매한 기기의 시리얼이 ABM에 등록되면 즉시 MDM 서버 자동 할당 설정

Key Points

운영 및 관리 포인트

효율적인 기기 관리를 위한 설정

기기 수령/반납 프로세스

사용자 입사(Onboarding) 시 자동 배포 및 퇴사(Offboarding) 시 원격 초기화 절차 확립

그룹 및 태그 관리

부서(Dev, HR 등) 및 직군에 따라 차등화된 프로파일/앱 설치 정책 적용을 위한 그룹핑

Stage 배포 운영 환경

OS 업데이트나 보안 정책 변경 전, 일부 기기에 먼저 배포하여 안정성 검증

Deployment Strategy

Mac DEP 적용 : User Side

Zero Touch

신규 입사자 (New User)

언박싱부터 업무 시작까지 10분

전원 ON & Wi-Fi 연결

인터넷 연결 즉시 Apple 서버가 기기 인식 및 등록 시작

자동 등록 (Remote Management)

복잡한 설정 없이 프로파일이 자동 설치되며 정책 적용

회사 계정 로그인

SSO 로그인 한 번으로 앱 설치 및 보안 설정 자동 완료

Migration

기존 입사자 (Current Member)

지속적인 컴플라이언스 준수

로그인 시 상태 점검

Okta(login), MDM 통해 기기 보안 상태 확인

누락 정책 재적용

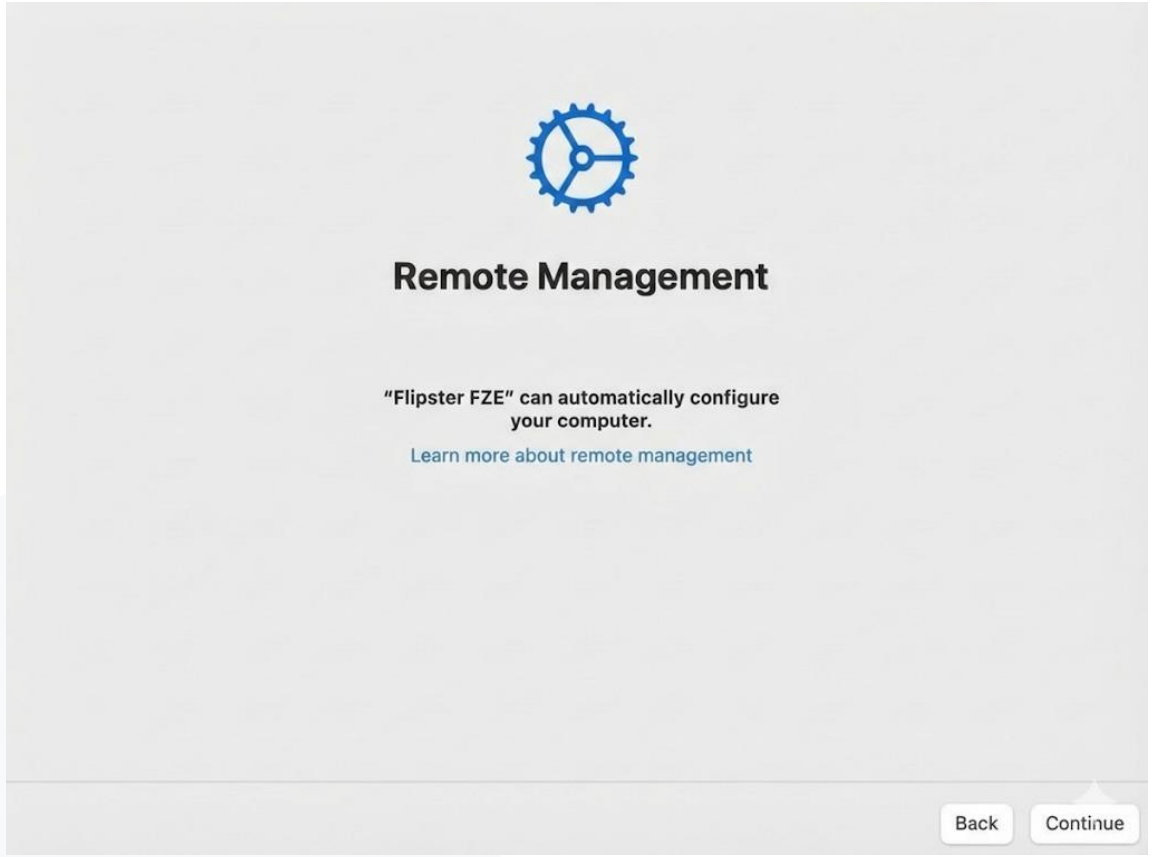
삭제된 앱이나 변경된 설정 발견 시 자동으로 강제 재적용

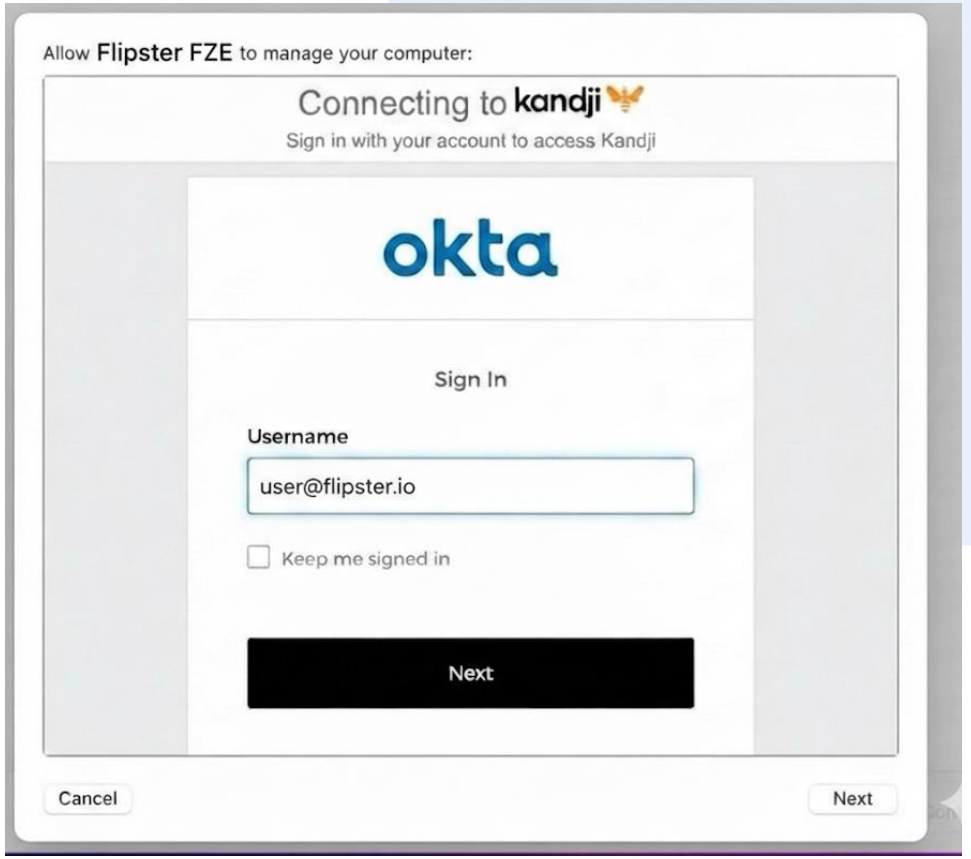
기기 변경 부담 최소화

기기 변경 시 업무공백 최소화

Deployment Strategy

Mac DEP 적용 : User Side





Deployment Strategy

Kandji 장점

직관적인 UI

- 깔끔하고 현대적인 UI
- Context 100% Sharing
- 실시간 상태 모니터링

IDP 연동 친화성

- device assignment 자동화
- 부서별 자동정책 적용 (Assignment Map)
- Device trust condition access

앱 배포

- Apple id 없이 app store 앱 배포
- Version 관리
- Self service를 이용한 app 자율성 보장

Part 3

Chrome OS..?

Cloud-first Endpoint

Cloud Native

Security

Efficiency

Google Way

Mac OS vs Chrome OS

Mac OS

Powerful Productivity

- 강력한 생산성 및 네이티브 앱
- 별도 보안 솔루션(EDR/MDM) 필수
- 초기 세팅 및 유지보수 요구
- 통제 어려움

VS

Chrome OS

Cloud First Security

- 로그인 즉시 완벽한 환경 동기화
- OS 자체 보안으로 AV / EDR 불필요
- 자동 업데이트 및 자동 포맷 지원
- Browser 외 CLI 사용 제한

Why Chrome OS?

Chrome OS 도입의 3가지 핵심 장점

Cloud First

- 로그인 즉시 Google 환경 동기화
- OS 기본설정(Wi-Fi, 즐겨찾기 등) 자동 배포 지원
- 언제 어디서나 동일한 업무 환경 제공

Security

- 별도의 AV / EDR 불필요
- 기기 분실 시 데이터 100% 보존 (Google Drive)
- 로그아웃 시 로컬 데이터 자동 삭제 및 포맷 지원

Efficiency

- 비용 절감
- 안드로이드 Application 호환 (VPN 등)
- 중단 없는 자동 업데이트 관리

The Google Way

Chrome OS 배포 전략

Google Admin Console

별도의 MDM 서버가 필요하지 않습니다.
단일 콘솔에서 모든 기기와 사용자를 통합 관리합니다.

Device Policy

로그인 전 기기에 적용되는 시스템 설정입니다.

- Wi-Fi 및 네트워크 설정
- OS 업데이트 버전 관리
- 기기 timeout 관리

User Policy

로그인 후 사용자의 계정에 따라오는 설정입니다.

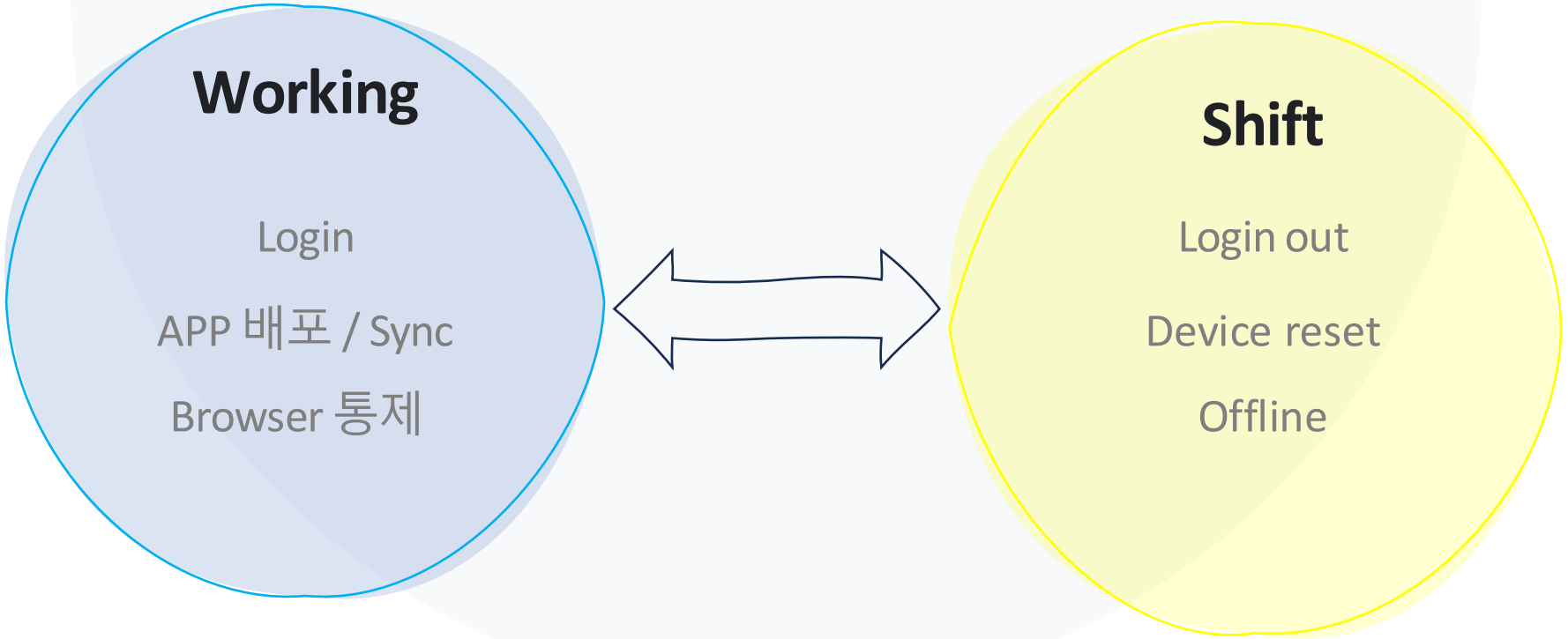
- app 배포 및 Browser extension 관리
- 관리되는 북마크 및 홈페이지
- 로그인 도메인 제한

Browser Policy

Chrome 사용 시 Group/Org에 따라오는 설정입니다.

- Browser 내 캡쳐 제한
- Screen sharing 금지
- Copy and paste 제한

Chrome OS device cycle



Deployment Process

Chrome OS Zero Touch Flow

구매

시리얼 자동 등록

프로비저닝

전원 ON & Wi-Fi 연결
"조직 관리 기기" 확인

로그인

Google Workspace(IDP)
계정 로그인

완료

바탕화면 진입 후
세팅 자동 완료

Impact & Results

도입 효과: 사용자와 보안팀 모두의 승리

Newbie (신규 입사자)

1hr → 10min

기기 세팅 소요 시간 단축

*"우와, 진짜 로그인만 하니까 다 되네요?
바로 업무 시작할 수 있어서 너무 편해요!
장비를 교체 받았는데, 제가 해야 할 일이 없나요?"*

- 복잡한 매뉴얼 없이 즉시 업무 환경 구성
- 초기 세팅 스트레스 및 대기 시간 제거
- 일관된 사용자 경험(UX) 제공

Security Team

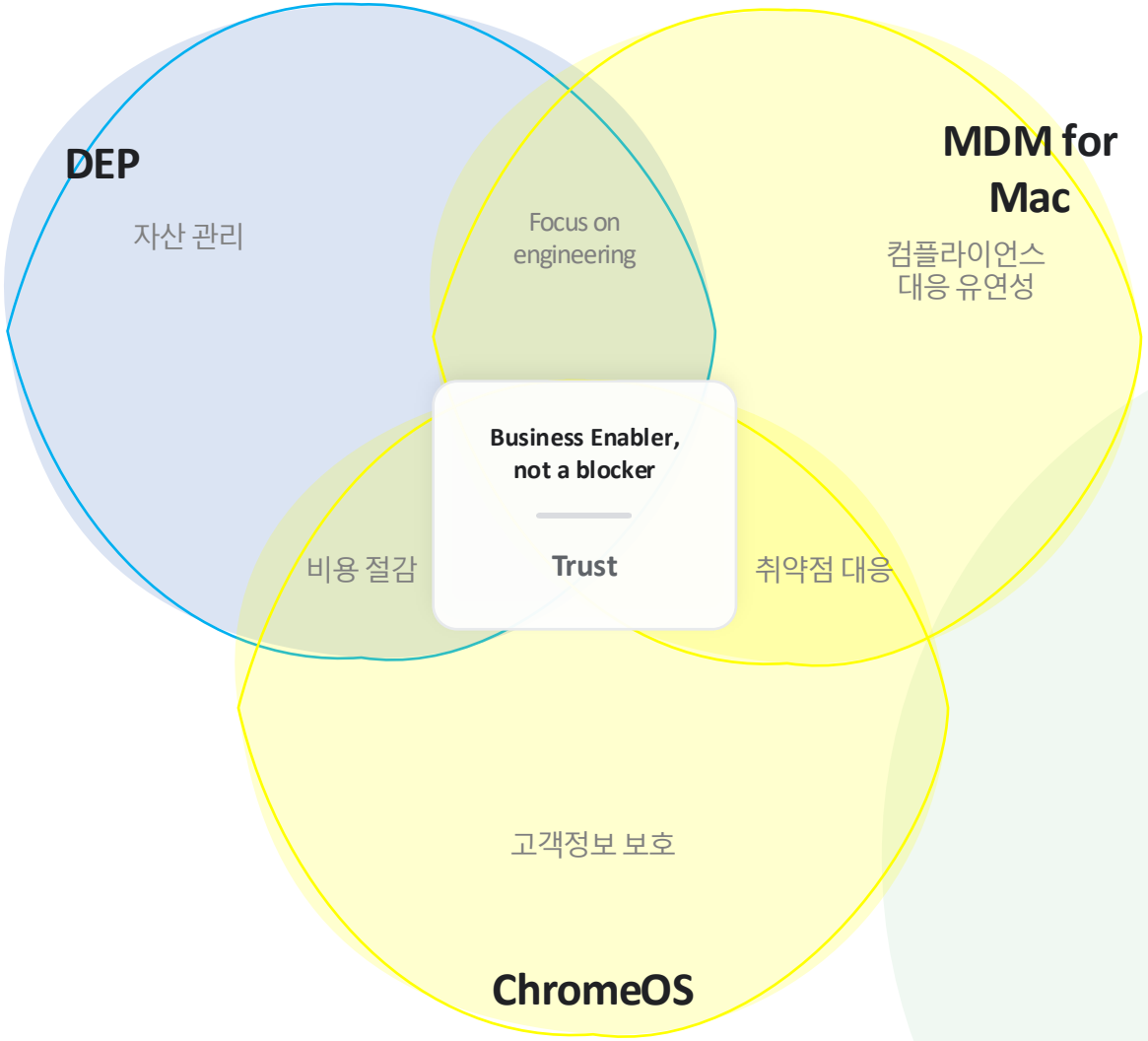
↘ 90%

단순 배포/세팅 문의 감소

"보안팀은 이제 엔지니어링에 집중합니다."

- 반복 업무 감소로 엔지니어링 집중 환경 조성
- 도난/분실 시 Remote Lock 등 보안성 강화
- 빠른 자산 파악 및 취약점 대응 속도 증가

Deployment Strategy: Key Takeaways



Q & A

질문을 받습니다.

Doyoung Park