중소형 병원 하이브리드 클라우드 보안 아키텍처

김이박 병원 예약 · 진료정보 · 관제 시스템

AWS 운영계 | 온프레미스 EMR | GCP DR | Wazuh 관제

김다정, ○○○, ○○○

목차

1. 요구사항 분석 및 설계 방향
2. AWS 인프라 설계 및 구축
3. 온프레미스 GCP 인프라 설계 및 구축
4. 보안관제 설계 및 구축
5. 비용 효과
6. QnA

고객의 모호한 요구

"진료기록은 외부에 노출되지 않게 관리 해주세요."

"온라인 예약 시스템이 필요해요."

“오류나 장애가 나도 예약 업무는 멈추지 않았으면 해요..”

”요즘 개인정보 유출 사고가 많던데, 우리 병원은 괜찮을까요?”

”비용은 가능한 합리적이었으면 좋겠어요.”

고객의 모호한 요구

"진료기록은 외부에 노출되지 않게 관리 해주세요."

"온라인 예약 시스템이 필요해요."

“오류나 장애가 나도 예약 업무는 멈추지 않았으면 해요..”

”요즘 개인정보 유출 사고가 많던데, 우리 병원은 괜찮을까요?”

”비용은 가능한 합리적이었으면 좋겠어요.”

고객의 모호한 요구

"진료기록은 외부에 노출되지 않게 관리 해주세요."

"온라인 예약 시스템이 필요해요."

“오류나 장애가 나도 예약 업무는 멈추지 않았으면 해요..”

”요즘 개인정보 유출 사고가 많던데, 우리 병원은 괜찮을까요?”

”비용은 가능한 합리적이었으면 좋겠어요.”

고객의 모호한 요구

"진료기록은 외부에 노출되지 않게 관리 해주세요."

"온라인 예약 시스템이 필요해요."

“오류나 장애가 나도 예약 업무는 멈추지 않았으면 해요..”

”요즘 개인정보 유출 사고가 많던데, 우리 병원은 괜찮을까요?”

”비용은 가능한 합리적이었으면 좋겠어요.”

고객의 모호한 요구

"진료기록은 외부에 노출되지 않게 관리 해주세요."

"온라인 예약 시스템이 필요해요."

“오류나 장애가 나도 예약 업무는 멈추지 않았으면 해요..”

”요즘 개인정보 유출 사고가 많던데, 우리 병원은 괜찮을까요?”

”비용은 가능한 합리적이었으면 좋겠어요.”

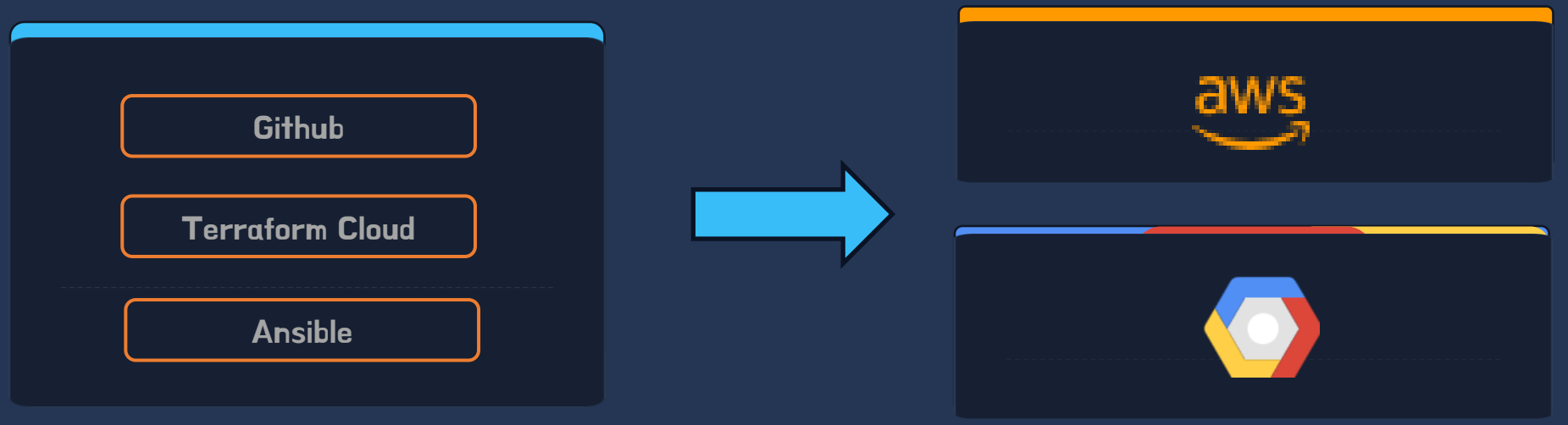
프로젝트 한 줄 정의

중소형 병원의 예약 · 진료정보 · 관제 시스템을 하이브리드 클라우드로 설계했습니다.

대외 서비스	민감 의료정보	장애 대응	보안 운영 관제
AWS 운영	온프레미스 EMR/DB	GCP DR	Wazuh / Grafana / Prometheus

프로젝트 표준 및 협업 거버넌스

짜깁기식 구축을 넘어, 거버넌스와 IaC 표준 정립



IaC 원칙
클라우드 리소스는 Terraform Cloud 기준으로 생성 변경

협업 원칙
GitHub 브랜치와 PR로 변경 이력 관리

명명 규칙
서비스 환경 역할이 드러나도록 리소스 이름 통일

역할분담

AWS 인프라

김다정 팀장

AWS 운영계 인프라와 **병원 예약 EMR 서비스 개발**을 총괄

- AWS 클라우드 인프라 설계 및 구축
- 병원 예약 EMR 서비스 개발

온프레미스 GCP

○○○

온프레미스 의료정보 환경과 GCP를 잇는 **하이브리드 아키텍처** 구축

- 온프레미스 GCP 설계 및 구축
- 하이브리드 아키텍처 설계 및 구축

SIEM 관제

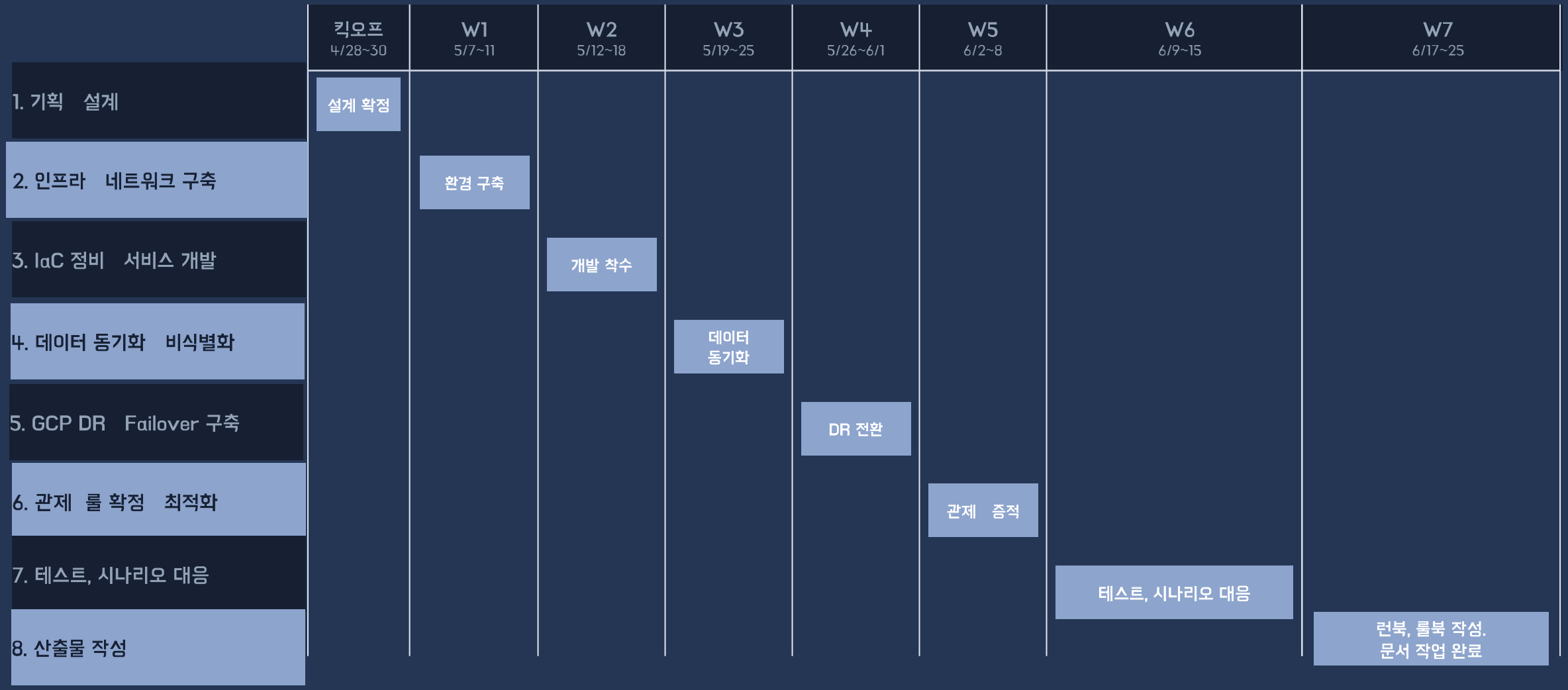
○○○

Wazuh 기반 **보안관제 복구 아키텍처**와 클라우드 인프라 구축

- 보안 모니터링 복구 아키텍처 설계
- AWS 클라우드 인프라 설계 및 구축

프로젝트 일정(WBS)

2026.04.28~2026.06.25 (약 2개월)




CLOUDFLARE
aws
Pubic subnet
NAT
ALB
WAF
private subnet
ECS EC2
ECS EC2
ECS EC2
Wazuh manager
Wazuh Indexer
Grafana
DB Subnet
RDS Proxy
RDS Proxy
RDS Aurora
RDS Aurora
S3
VPN
VPN
libreswan

AWS 인프라,
예약 진료정보 시스템 개발

담당자 김다정

환자

요구사항에 따른 구현

예약 인증

SFR-001

예약시스템 기능

초진, 재진, 입원 및 수술 등 전 과정에 대한 **예약 및 알림 기능**을 구현

- ✓ 예약/예약 취소
- ✓ 실시간 자동 알림
- ✓ 예약/상태/변경 조회

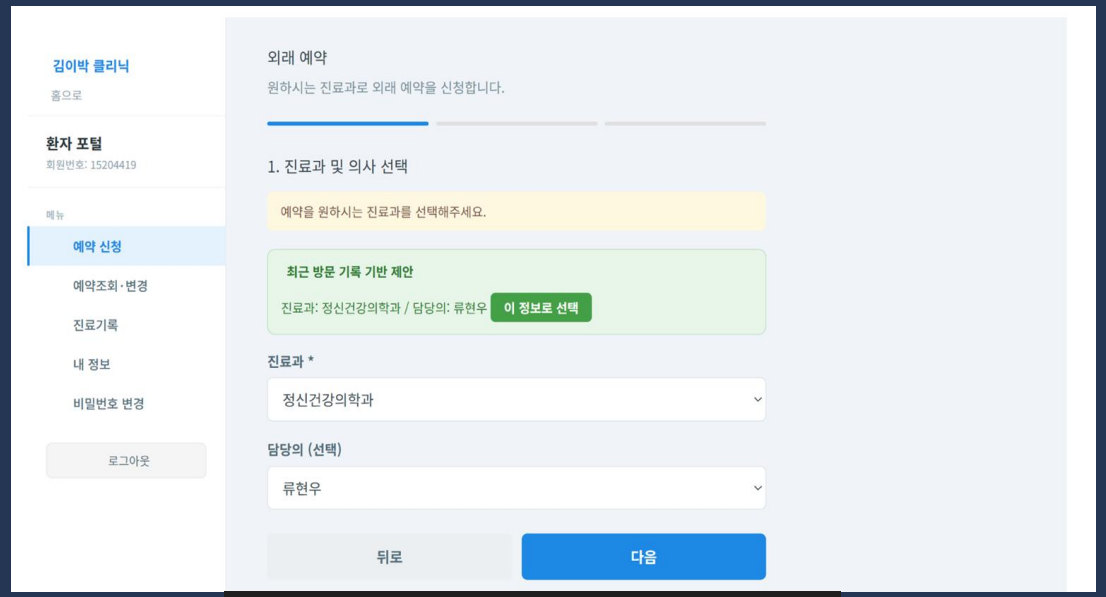
SFR-002

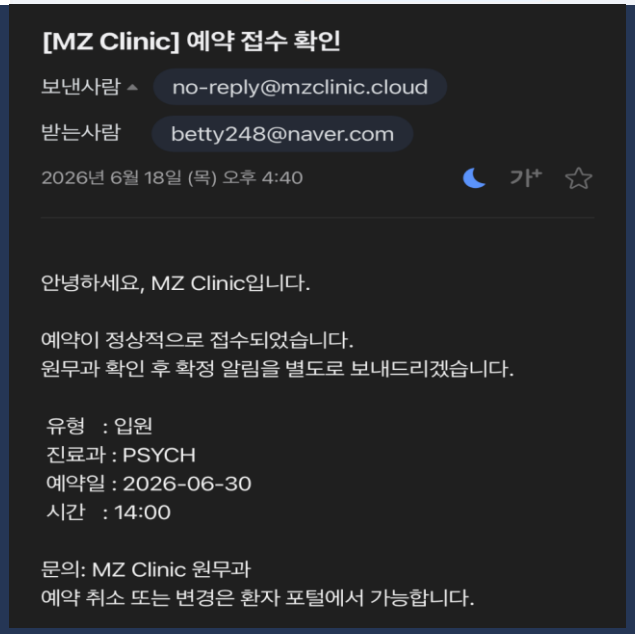
사용자 인증 및 권한관리

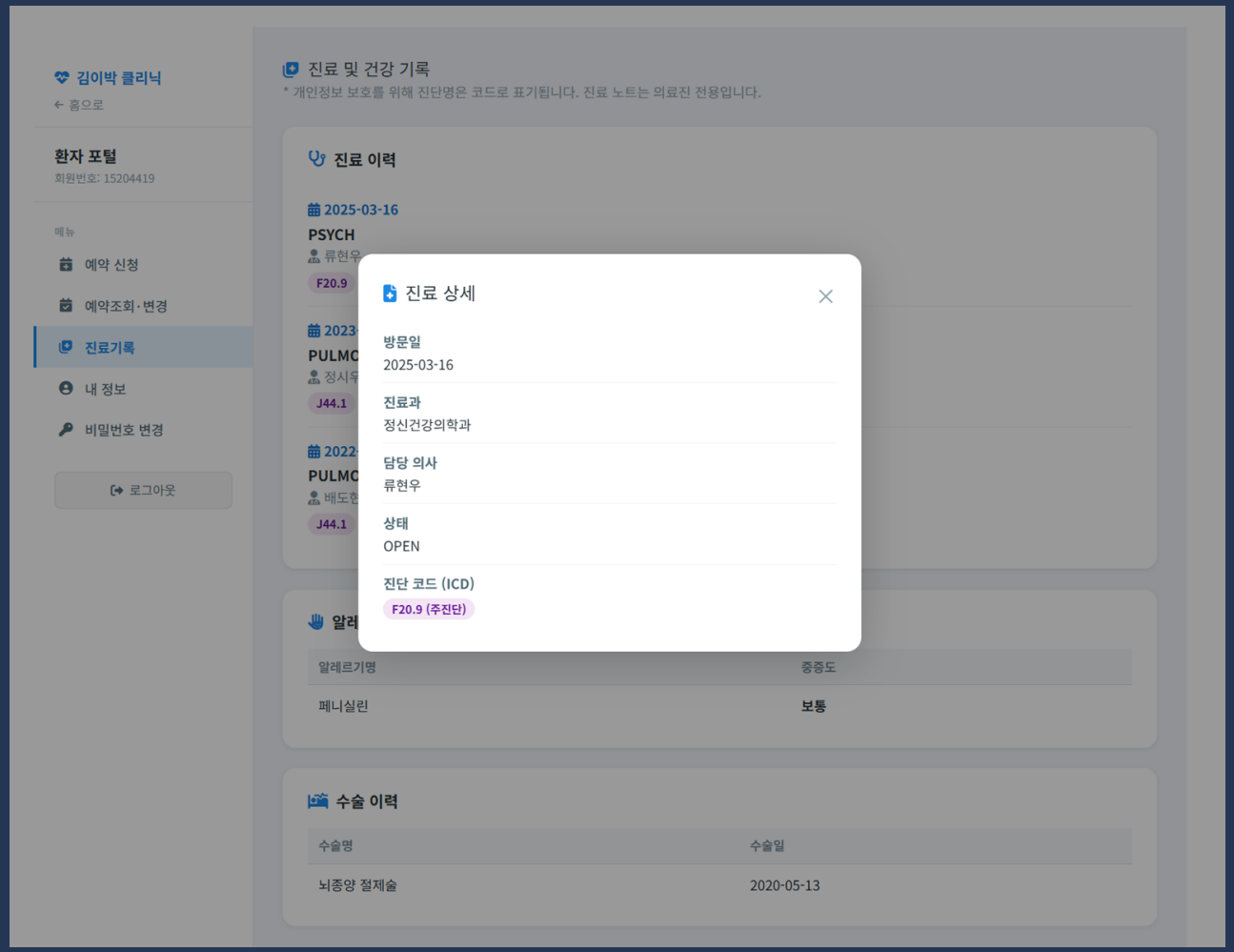
데이터 보호를 위해 **역할 기반 접근제어 (RBAC)**와 다중 인증(MFA)을 적용

- ✓ 역할 기반 접근제어(RBAC)
- ✓ 2단계 인증(MFA) 의무화
- ✓ 최소권한 원칙

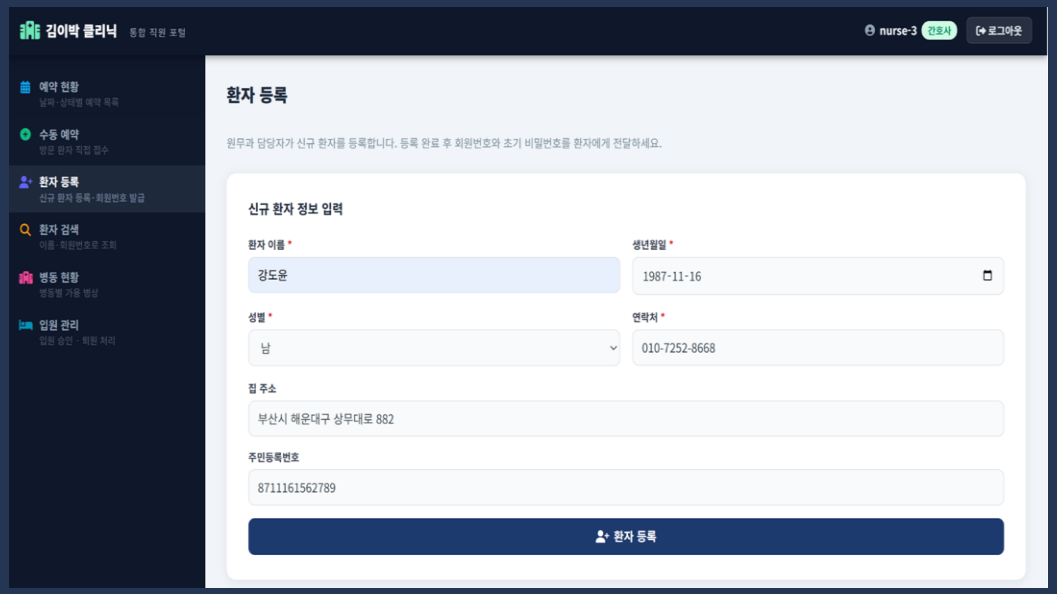
환자: 예약 등록 및 진료 기록 확인

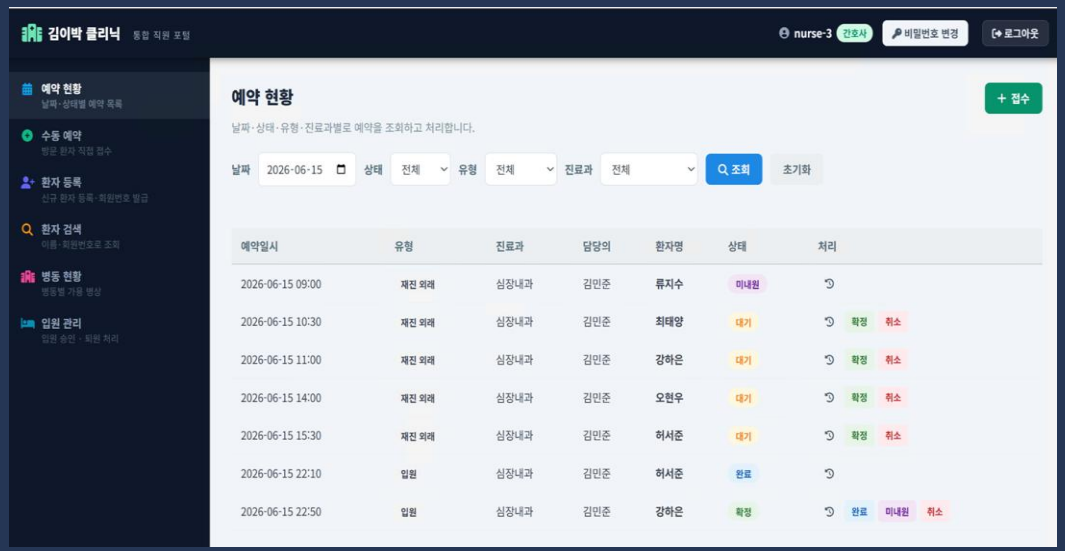


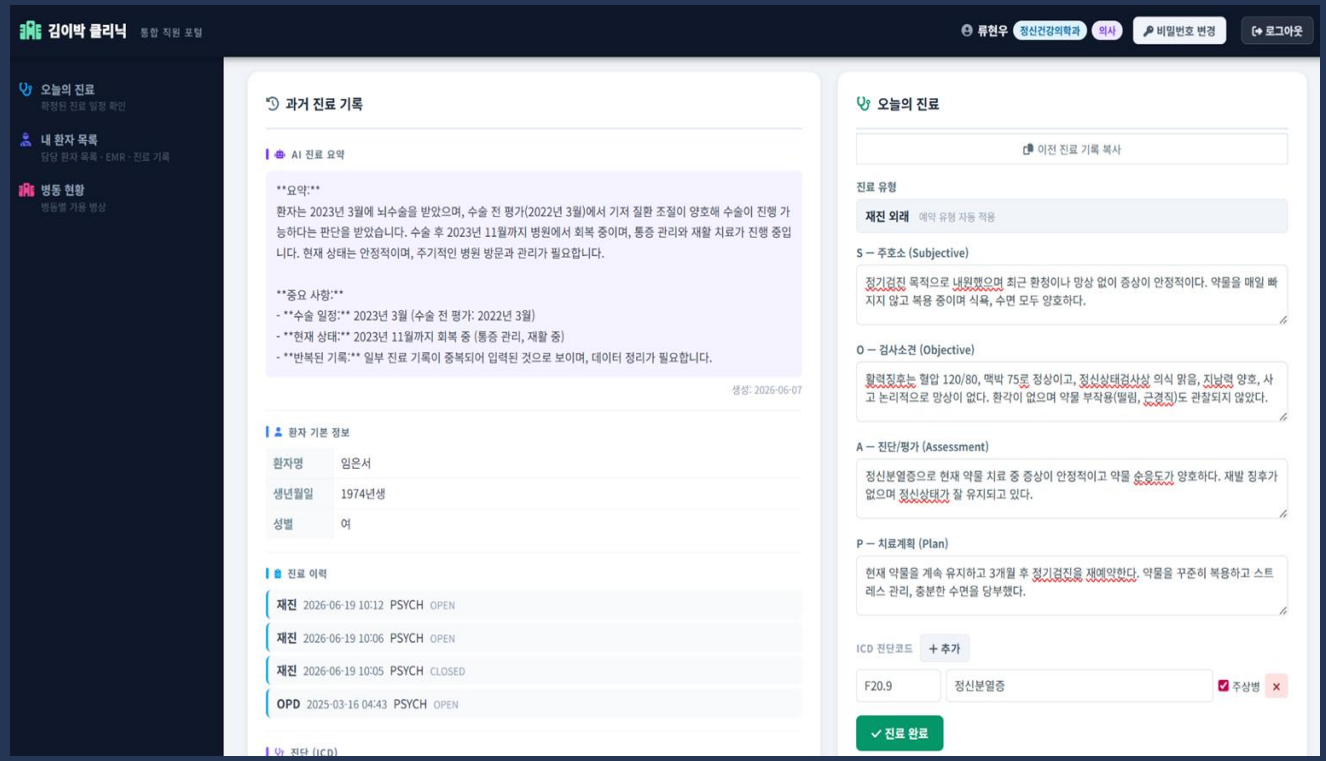




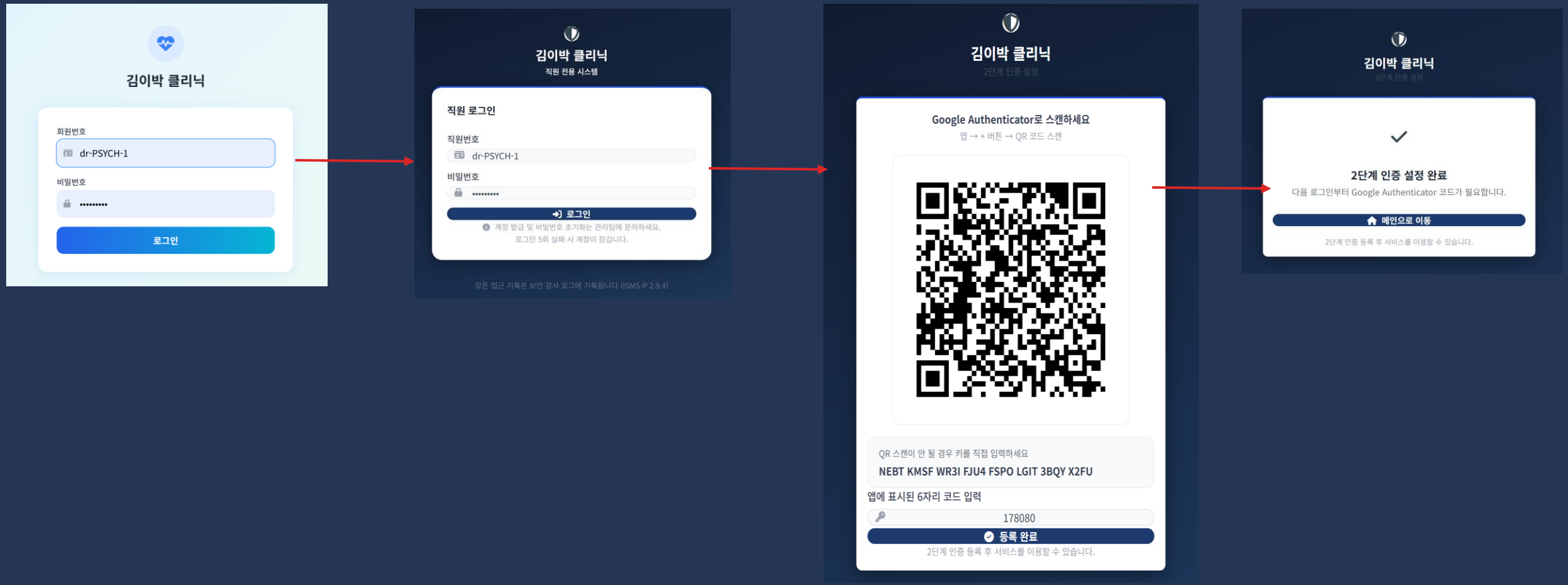
간호사: 초진 환자 등록 및 진료 관리 / 의사: 진료 등록 및 퇴원 지시



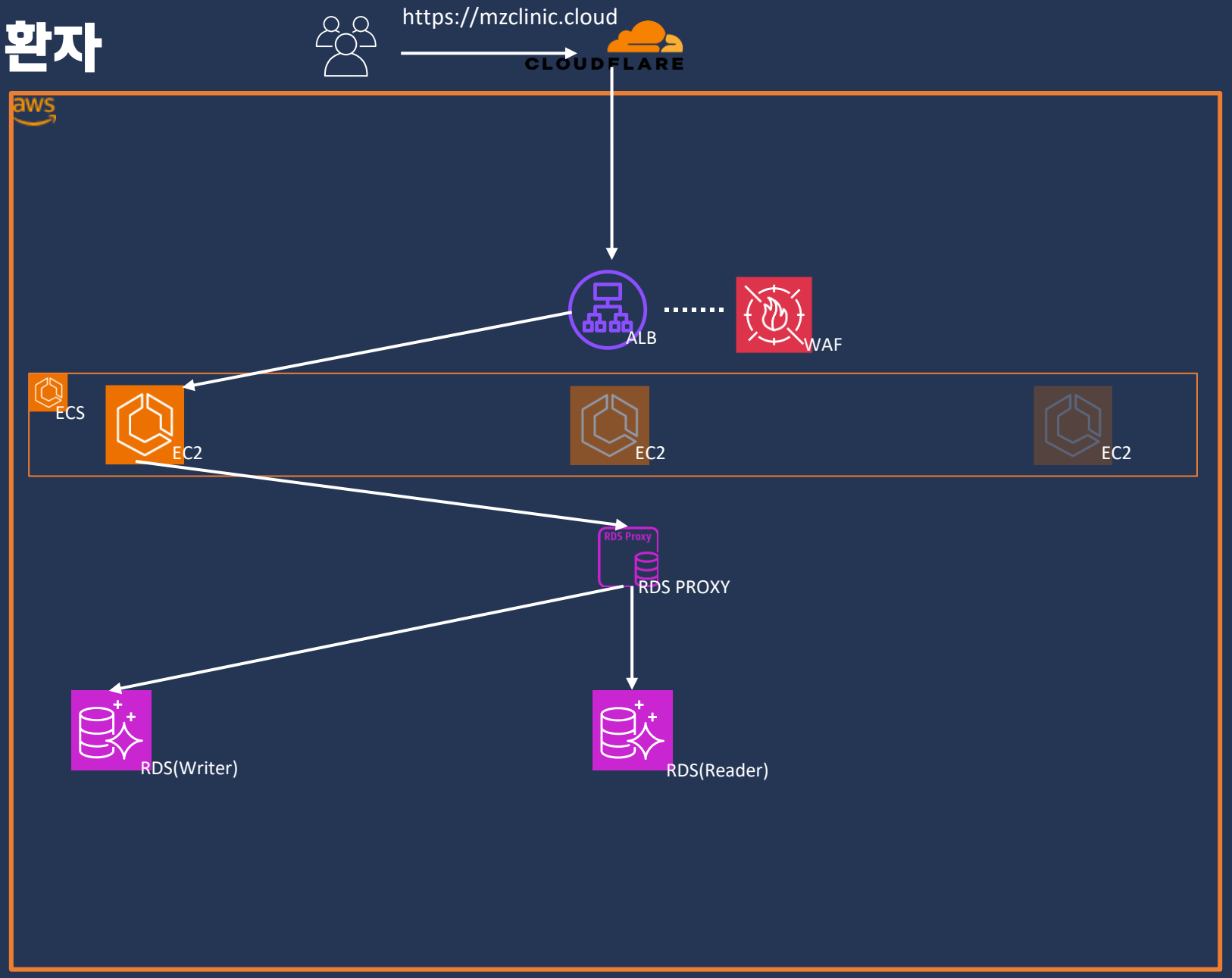




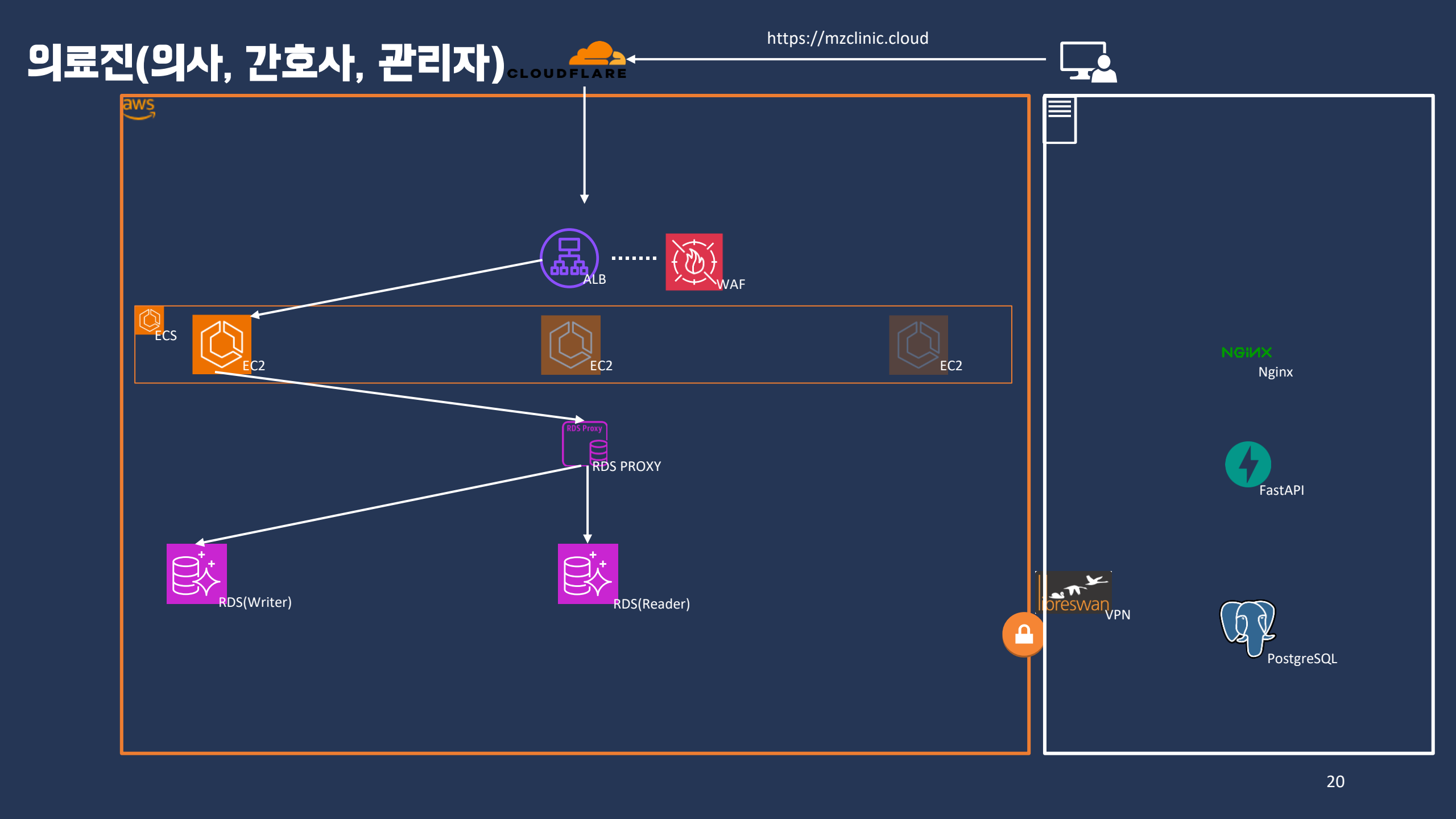
다중인증(MFA)


김이박 클리닉
회원번호
dr-PSYCH-1
비밀번호
로그인
김이박 클리닉
직원 전용 시스템
직원 로그인
직원번호
dr-PSYCH-1
비밀번호
로그인
계정 발급 및 비밀번호 초기화는 관리팀에 문의하세요.
로그인 5회 실패 시 계정이 잠깁니다.
모든 접근 기록은 보안 감사 로그에 기록됩니다 (ISMS-P 2.9.4)
김이박 클리닉
2단계 인증 설정
Google Authenticator로 스캔하세요
앱 → + 버튼 → QR 코드 스캔
QR 스캔이 안 될 경우 키를 직접 입력하세요
NEBT KMSF WR3I FJU4 FSPO LGIT 3BQY X2FU
앱에 표시된 6자리 코드 입력
178080
등록 완료
2단계 인증 등록 후 서비스를 이용할 수 있습니다.
김이박 클리닉
2단계 인증 설정 완료
다음 로그인부터 Google Authenticator 코드가 필요합니다.
메인으로 이동
2단계 인증 등록 후 서비스를 이용할 수 있습니다.

환자


https://mzclinic.cloud
CLOUDFLARE
aws
ALB
WAF
ECS
EC2
EC2
EC2
RDS Proxy
RDS PROXY
RDS(Writer)
RDS(Reader)

의료진(의사, 간호사, 관리자)



의료진(의사, 간호사, 관리자)

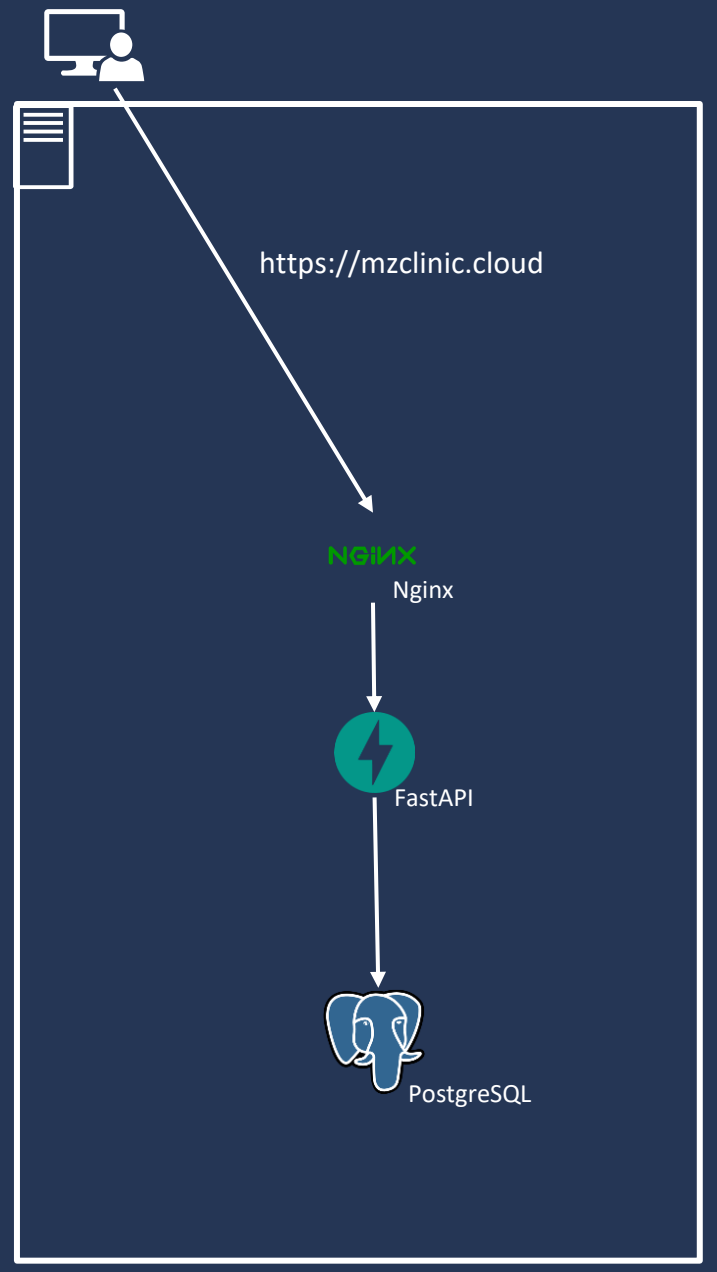
김이박 클리닉

로그인 완료

병원 내부망에서만 접속 가능합니다.

내부 진료 DB 바로가기

당일 진료 현황 대시보드



요구사항에 따른 구현

가용성, 비용분석 자동화

SFR-010

AWS 가용성 구성

예약 시스템의 고가용성을 유지하기 위한

AWS 기본 가용성 구성 아키텍처를 설계

- ✓ AWS 기본 가용성 구성
- ✓ 서비스 중단 최소화
- ✓ 유연한 리소스 확장성

김다정,
개인 프로젝트

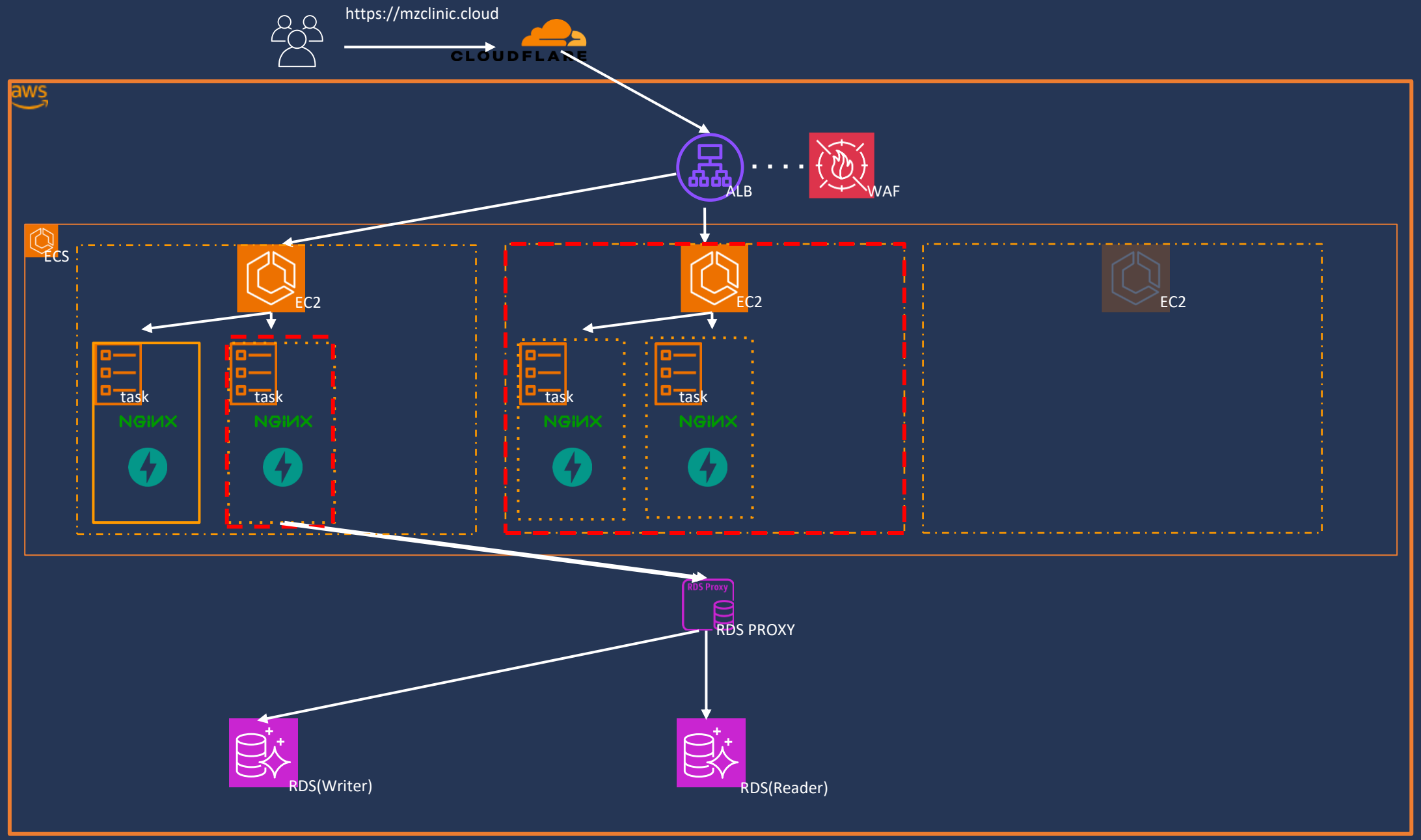
SFR-017

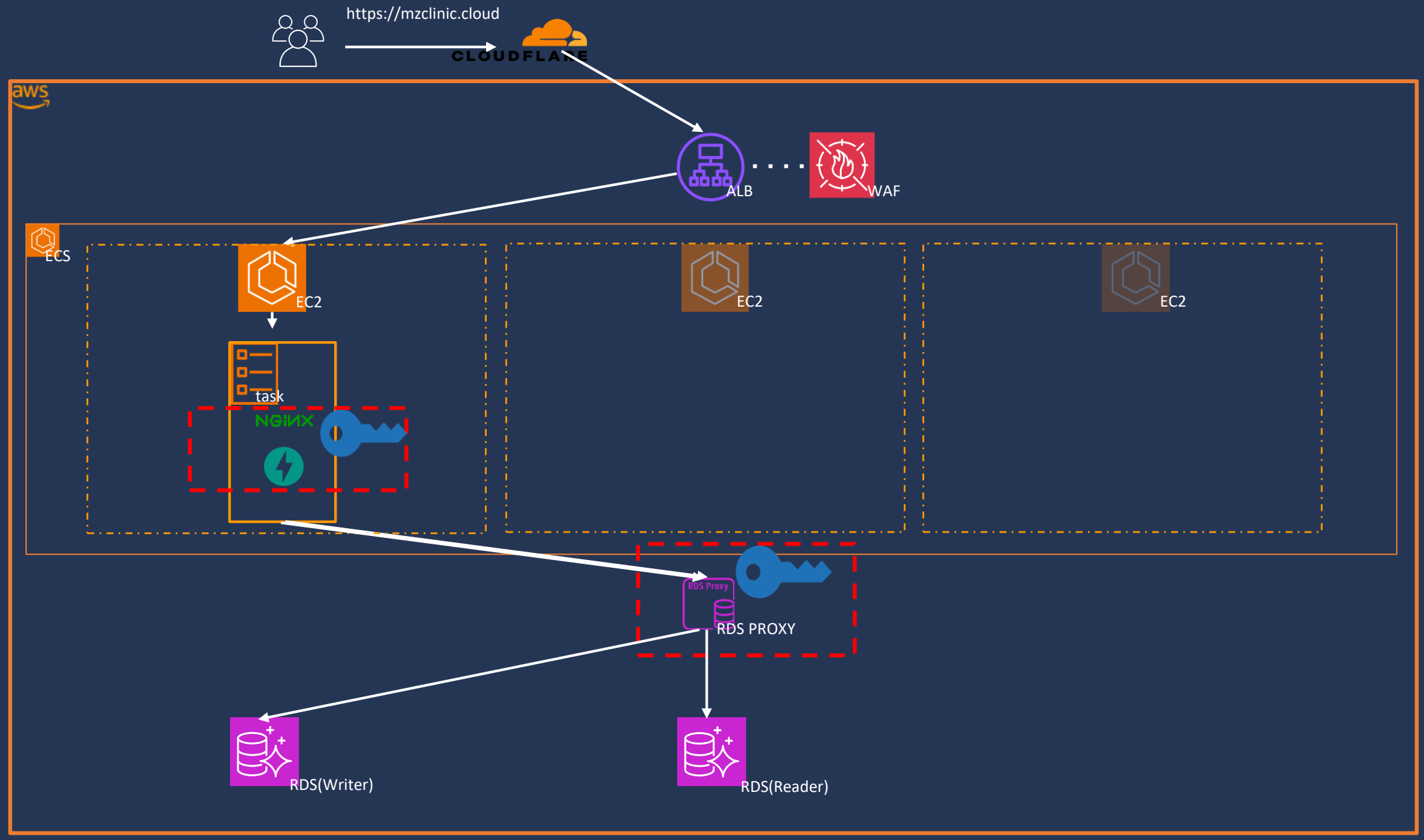
AIOps 비용 분석기

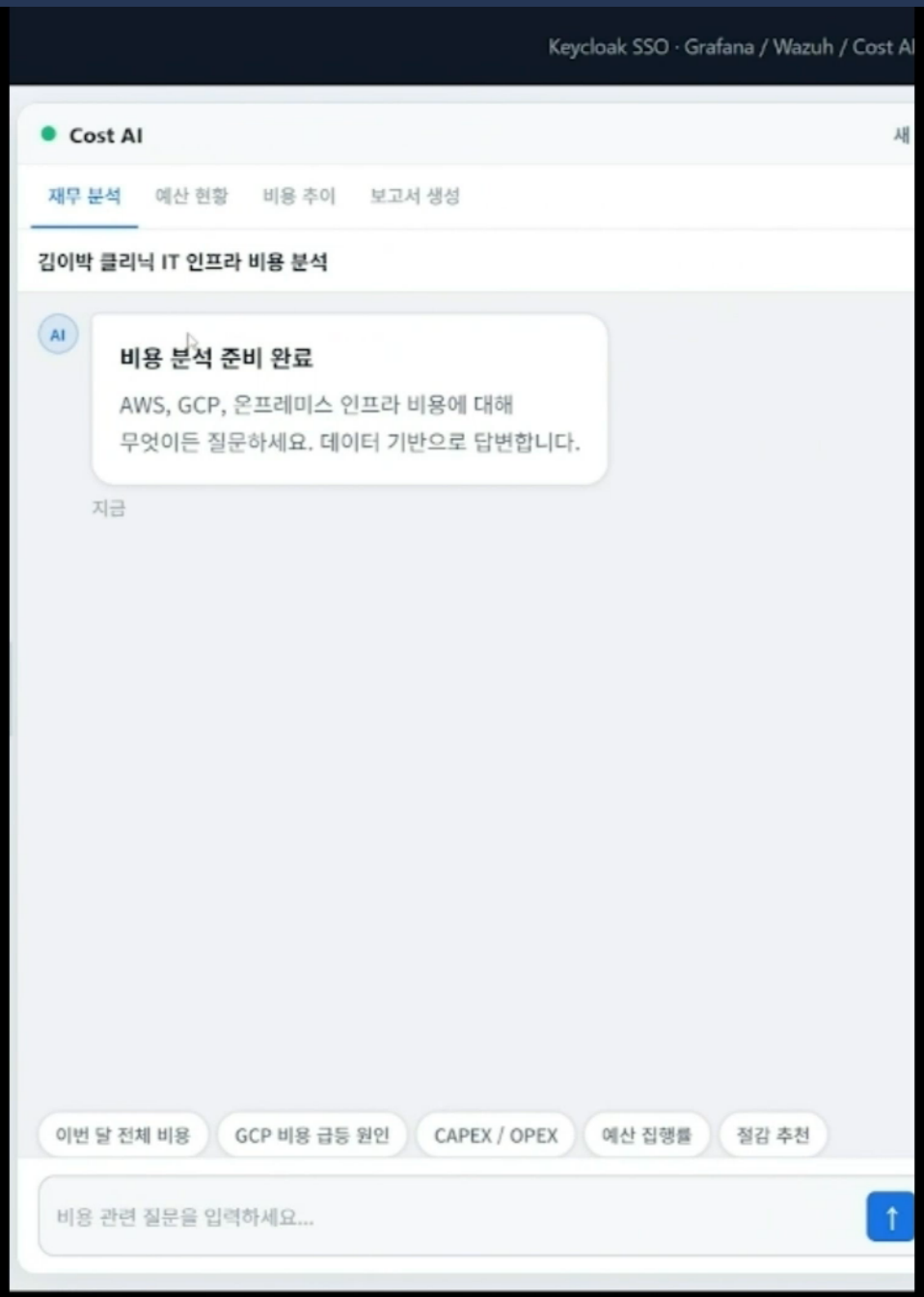
월별 비용 데이터를 통합 수집하고,

AI분석을 통해 비용 분석 및 절감 인사이트 제공

- ✓ AI 챗봇 (RAG)
- ✓ 월간 보고서 자동화
- ✓ 비용 이상 감지/미사용리소스 감지


https://mzclinic.cloud
CLOUDFLARE
aws
ALB
WAF
ECS
EC2
EC2
EC2
task
task
task
task
NGINX
NGINX
NGINX
NGINX
RDS Proxy
RDS PROXY
RDS(Writer)
RDS(Reader)


https://mzclinic.cloud
CLOUDFLARE
aws
ALB
WAF
ECS
EC2
EC2
EC2
task
NGINX
RDS Proxy
RDS PROXY
RDS(Writer)
RDS(Reader)


Keycloak SSO · Grafana / Wazuh / Cost AI
Cost AI
재무 분석
예산 현황
비용 추이
보고서 생성
김이박 클리닉 IT 인프라 비용 분석
AI
비용 분석 준비 완료
AWS, GCP, 온프레미스 인프라 비용에 대해
무엇이든 질문하세요. 데이터 기반으로 답변합니다.
지금
이번 달 전체 비용
GCP 비용 급등 원인
CAPEX / OPEX
예산 집행률
절감 추천
비용 관련 질문을 입력하세요...

AI활용 비용분석

재무 분석 | 예산 현황 | 비용 추이 | 보고서 생성

김이박 클리닉 IT 인프라 비용 분석
AWS · GCP · On-premises

대화 저장 ↓ ● 연결됨

YOU: 5월 리포트의 핵심 내용을 참고해서 6월에는 어떤 변화가 있을지 정리해줘

오전 07:08

AI

완벽합니다! 5월 리포트 핵심 내용을 바탕으로 6월의 변화를 정리해드리겠습니다.

📊 **5월 리포트 핵심 → 6월 변화 분석**

5월 리포트 핵심 문제점

1. **GCP 비용이 131.2% 급증** - 신규 프로젝트 투입 또는 워크로드 확대
2. **AWS EC2 비용이 전체의 43.2% 차지** - 최적화 필요
3. **온프레미스 고정 지출** - 클라우드 마이그레이션 검토 필요

6월 변화 현황

📈 **전체 비용 추이 (5월 vs 6월)**

클라우드	5월	6월	변화	증감율
AWS	1,528,366원	1,527,836원	-530원	**-0.03%**
GCP	196,391원	149,491원	-46,900원	**-23.9%** ⬇️
온프레미스	281,967원	281,967원	0원	**0.0%**
전체 합계	2,006,723원	1,959,294원	-47,429원	**-2.4%** ⬇️

✅ **긍정적 변화**

1. **GCP 비용 감소 (-23.9%)** 🎉
   - 5월의 131.2% 급증 이후 조정
   - Networking: 105,420원 → 80,777원 (-23.4%)
   - Cloud SQL: 53,242원 → 40,458원 (-24.0%)
   - Compute Engine: 34,873원 → 26,070원 (-25.3%)
   - → **5월 권고사항이 효과를 본 것으로 추정**
2. **AWS 비용 안정화**
   - 5월의 7.9% 증가세에서 벗어나 거의 동일 수준 유지
   - EC2: 661,670원 → 663,550원 (안정적)

MZ Clinic · AI Cost Analysis System · Powered by AWS Bedrock

IT 인프라 운영비용 월간 현황 보고

2026년 5월 기준 · AWS / GCP / On-premises

발 신	MZ클리닉 AI 비용분석 시스템 (Powered by AWS Bedrock)
수 신	관리자
기준 월	2026년 5월
발송 일시	2026년 06월 20일 (자동 발송)

본 보고서는 AWS Bedrock AI가 자동 분석·생성한 월간 비용 현황입니다. 수치 이상 발견 시 담당자가 직접 확인하시기 바랍니다.

📎 상세 보고서 PDF가 첨부되어 있습니다. (infra_report_2026_05.pdf)

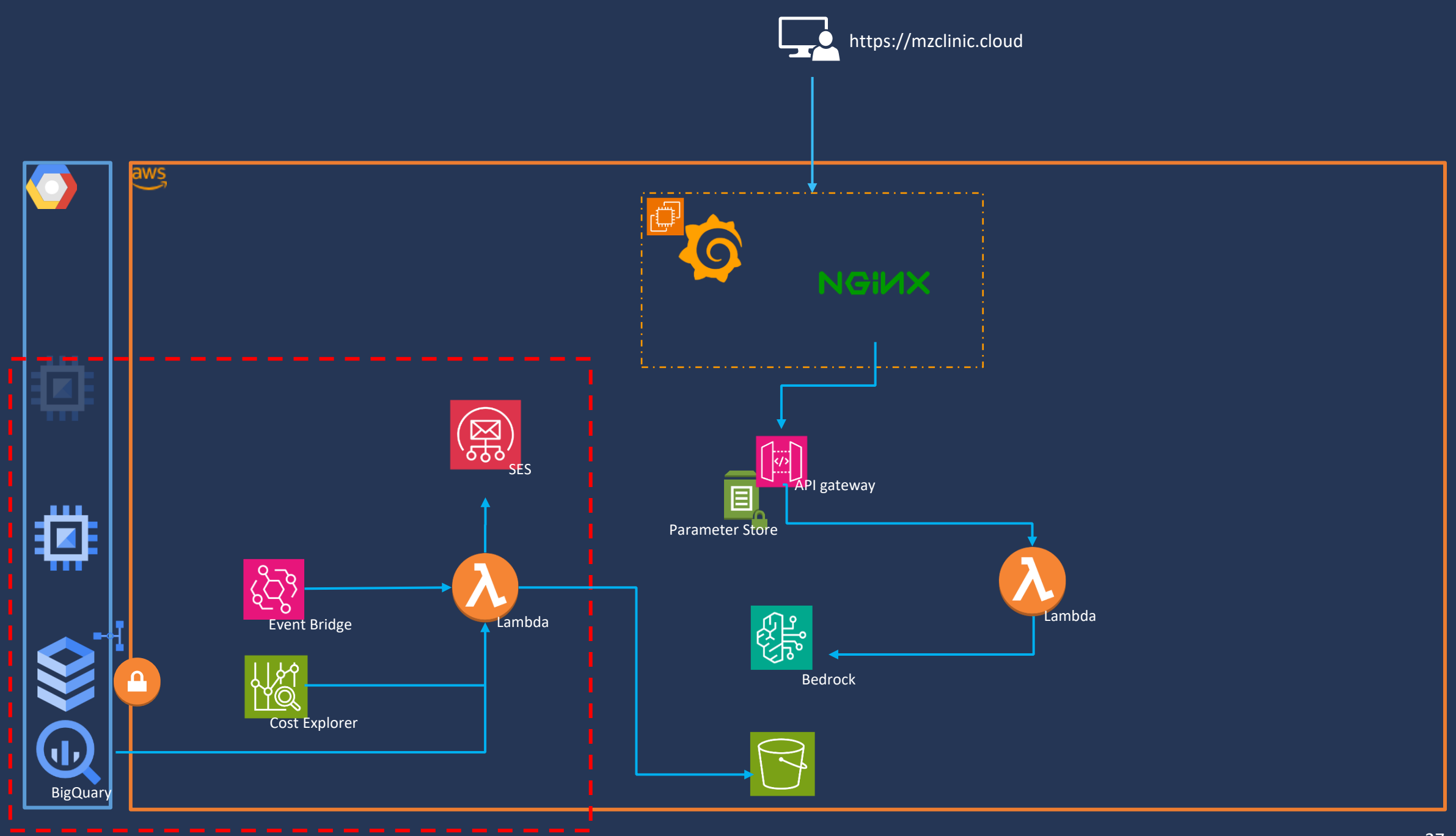
2026년 5월 IT 인프라 비용 현황 보고서

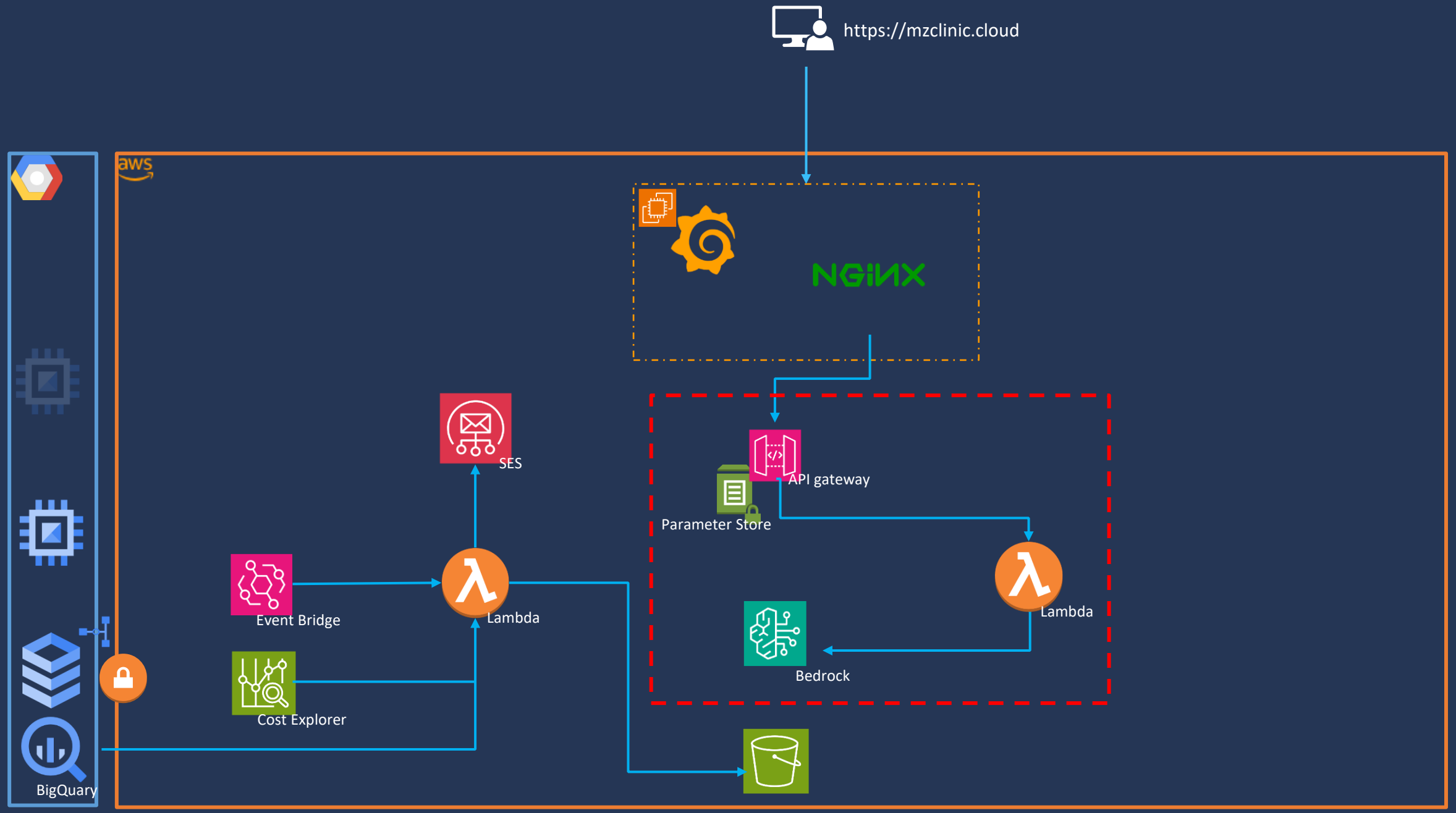
1. 이번 달 비용 요약

구분	5월 비용	전월 대비	비율
AWS	1,528,366원	+7.9%	76.1%
GCP	196,391원	+131.2%	9.8%
온프레미스	281,967원	+0.0%	14.0%

Claude

Amazon Titan


https://mzclinic.cloud
aws
NGINX
SES
API gateway
Parameter Store
Event Bridge
Lambda
Lambda
Bedrock
Cost Explorer
BigQuary


https://mzclinic.cloud
aws
NGINX
SES
API gateway
Parameter Store
Event Bridge
Lambda
Lambda
Bedrock
Cost Explorer
BigQuary

온프레미스 GCP 하이브리드

담당자 ○○○

Why Hybrid Architecture?

왜 하이브리드 아키텍처가 필요했는가?

클라우드도 장애가 날 수 있다

항공 예약 체크인 장애 사례처럼 외부 클라우드 장애는 실제 리스크

AWS 운영계만으로 끝내지 않음

병원 원본 데이터는 더 강한 보호가 필요하다

원본정보 EMR 진단기록 수술기록

온프레미스에 원본 의료정보 보관

장애 시 최소 업무는 계속되어야 한다

AWS 장애 시에도 예약 접수와 긴급 공지는 유지

GCP DR 환경으로 전환, 의료진 접근 환경은 온프레미스만으로 닫힌 구조

요구사항에 따른 구현

데이터 분류 비식별화 AI활용 진료정보 요약

SFR-003

데이터 분류 및 저장 정책

데이터 등급 분류 및 저장 위치 통제

- ✓ 민감도와 업무 목적에 따라 데이터 분류
- ✓ 의료정보는 온프레미스에 저장 관리
- ✓ 예약정보 비식별 통계등은 AWS 운용 가능

SFR-004

비식별화 처리

온프레미스 EMR을 AWS 전송 시

데이터 유형별 비식별화 규칙 적용

Text is not SVG - cannot display

- ✓ 의료정보는 최소 정보만 AWS로 전달
- ✓ 원본 진단명 또는 자유서술 원문 전달 금지
- ✓ 허용 스키마 검증 및 비허용 필드 차단

○○○,
개인 프로젝트

SFR-016

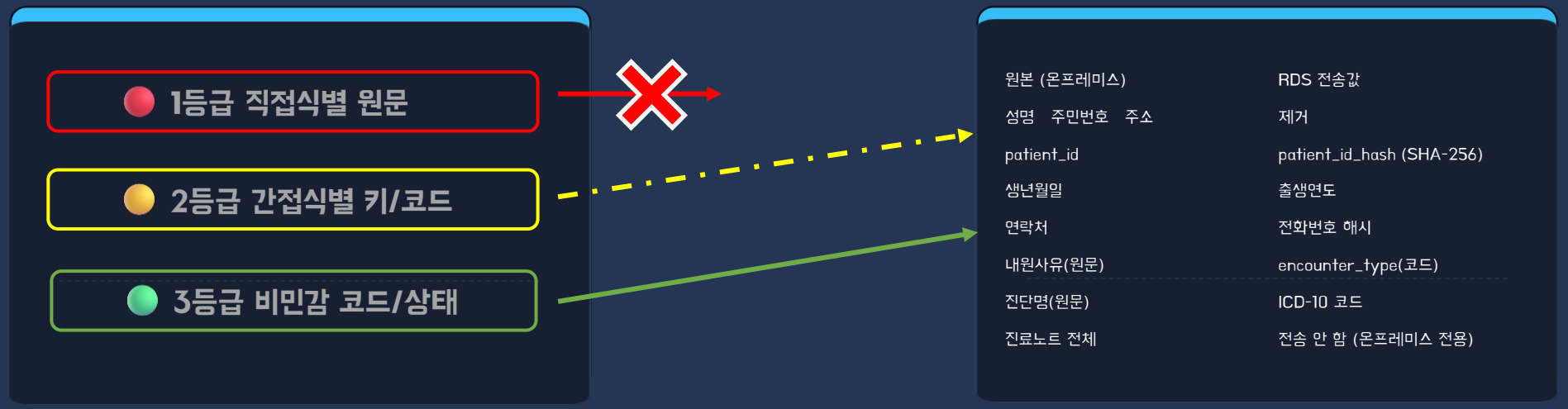
진료정보 요약제공

AI를 통해 환자별 진료정보 요약본을 제공

- ✓ 온프레미스 환경에서 AI를 통한 요약
- ✓ 적절한 모델을 취사선택
- ✓ 증적 자료 요약

데이터 민감도 3등급 분류와 비식별화 전송

3등급 분류 비식별화 전송



patients
개인정보들 (성명, 연락처, 주소, 주민등록 번호 등)

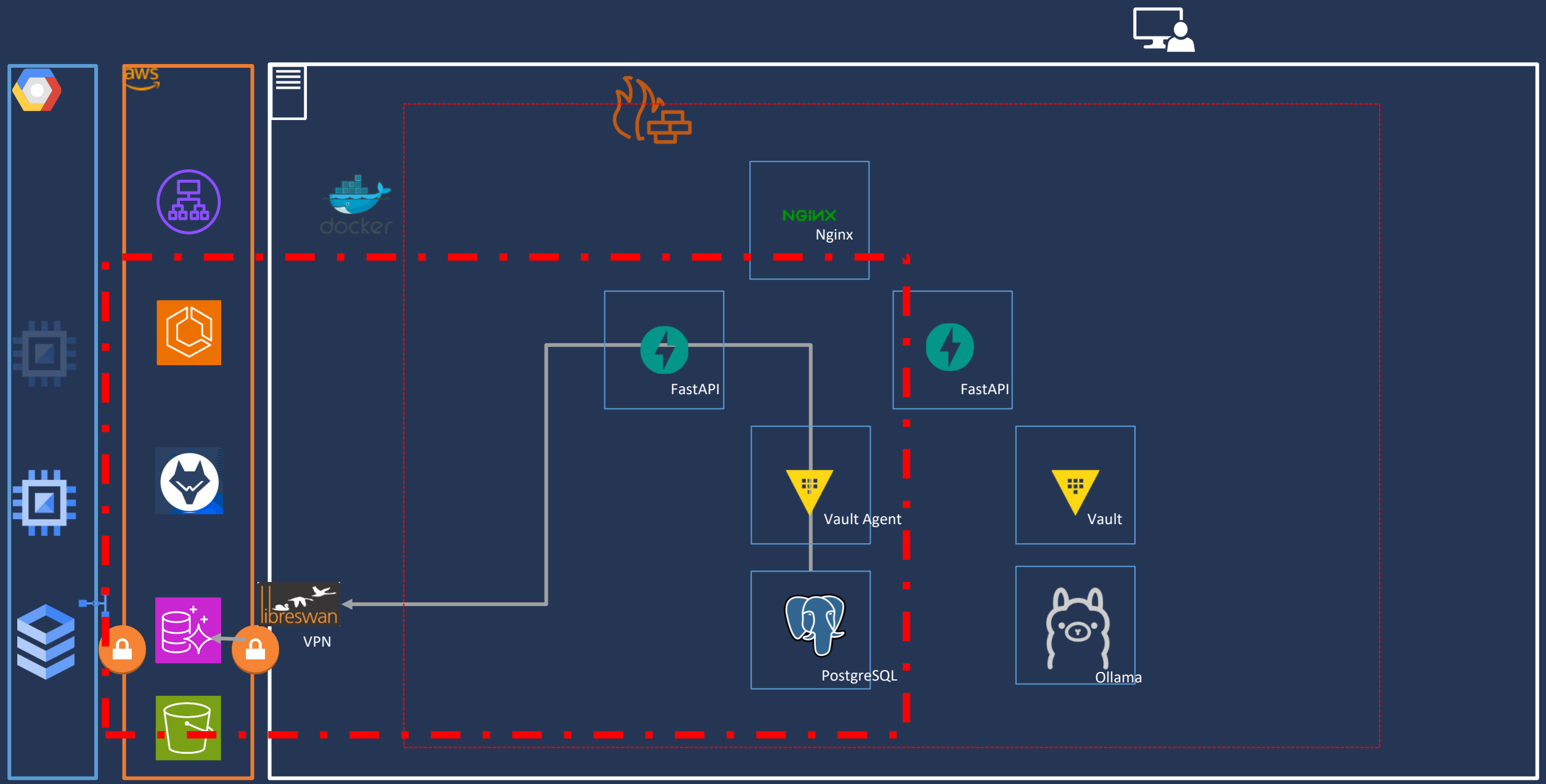
encounter
내원 사유 (자유서술)

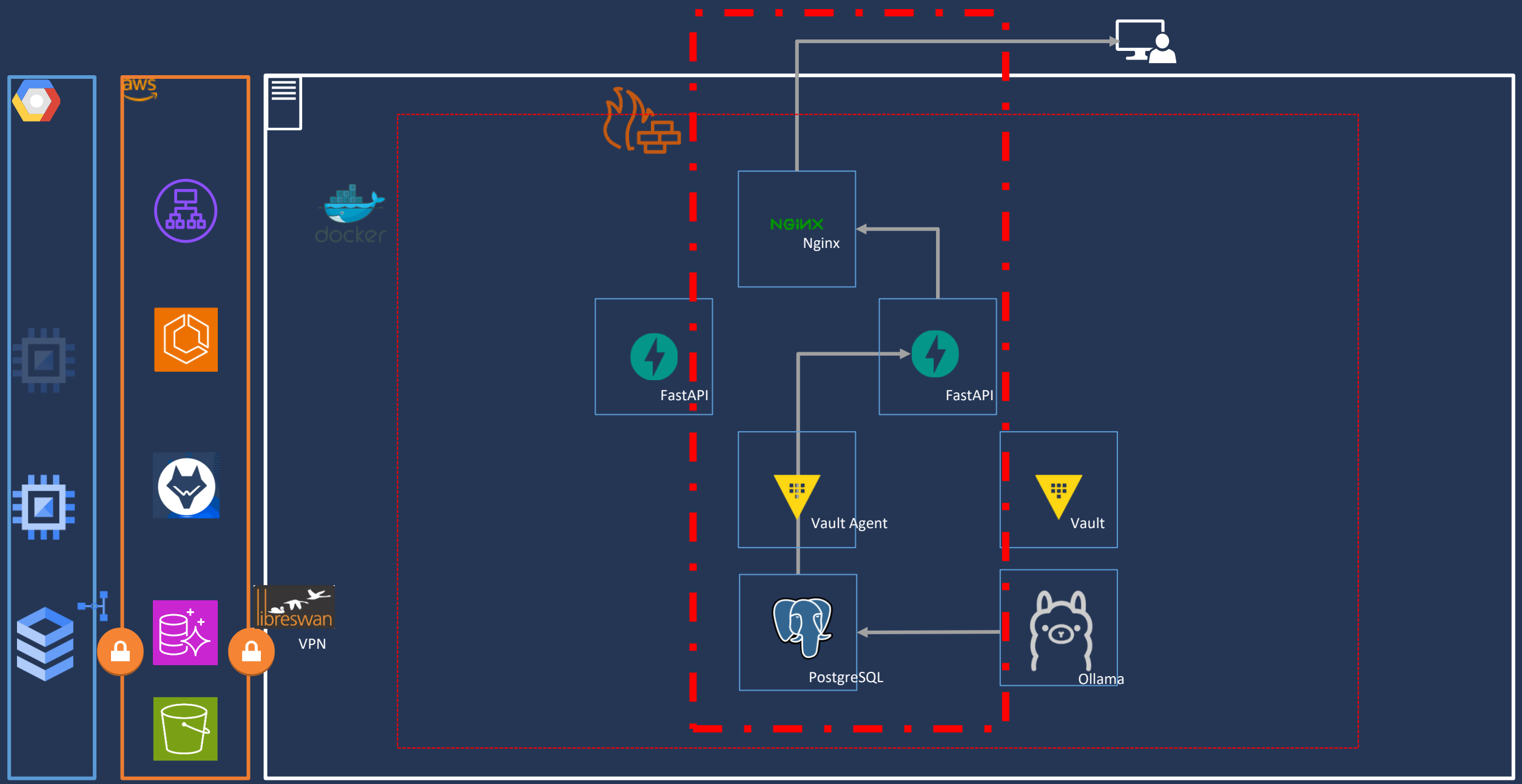
diagnoses
ICD-10진단코드 ,
진단명 원문 (자유서술)

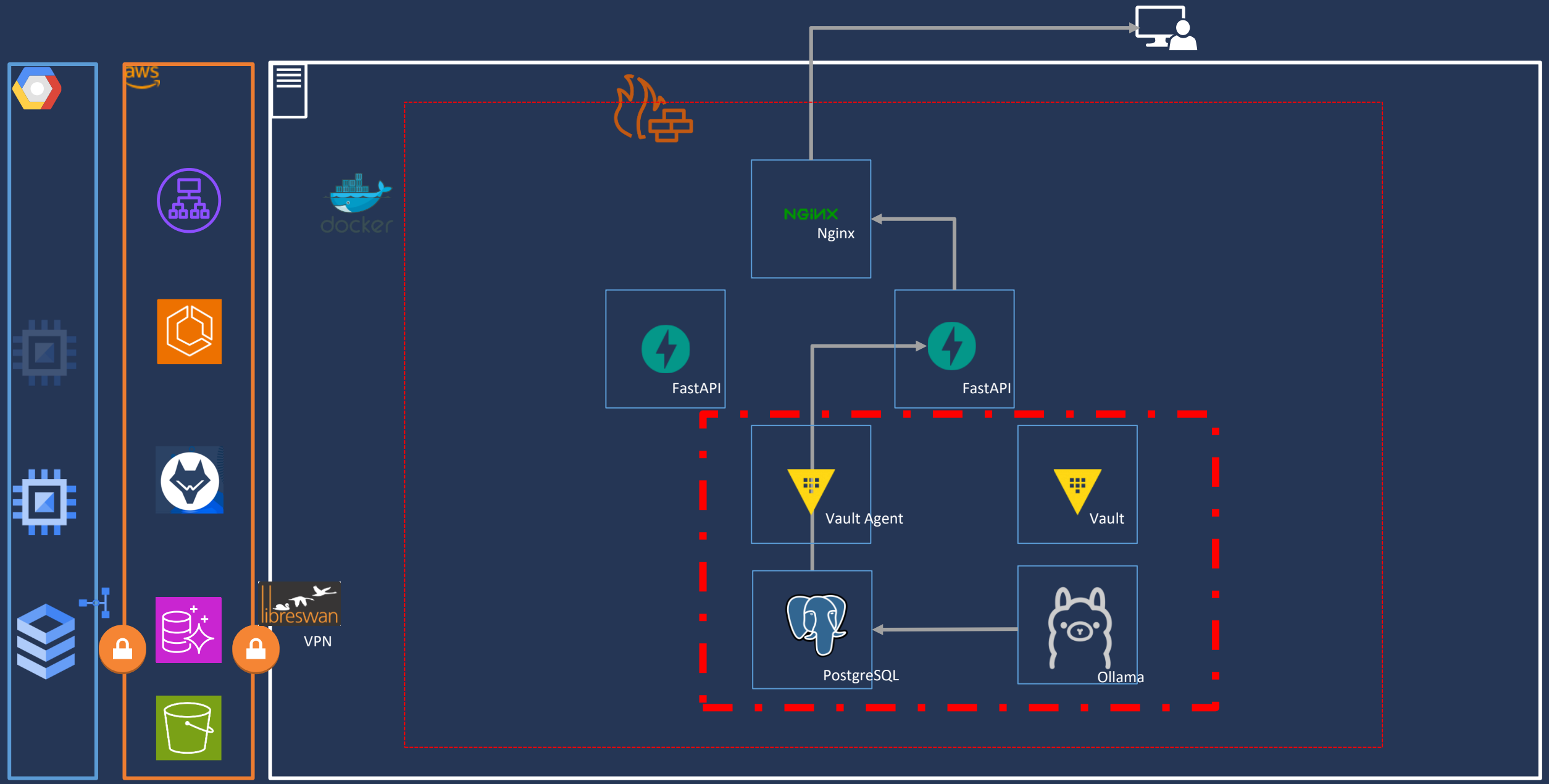
allergies
알레르기 명 원문

surgery_histories
수술명 원문, 수술 분류 코드
수술 소견 (자유서술)

clinic_notes
의무기록 원문


aws
docker
NGINX
Nginx
FastAPI
FastAPI
Vault Agent
Vault
libreswan
VPN
PostgreSQL
Ollama


aws
docker
NGINX
Nginx
FastAPI
FastAPI
Vault Agent
Vault
PostgreSQL
Ollama
libreswan
VPN


aws
docker
NGINX
Nginx
FastAPI
FastAPI
Vault Agent
Vault
PostgreSQL
Ollama
libreswan
VPN

오늘의 진료
확정된 진료 일정 확인

내 환자 목록
담당 환자 목록 · EMR · 진료 기록

병동 현황
병동별 가용 병상

과거 진료 기록

AI 진료 요약

요약:
환자는 2023년 3월에 뇌수술을 받았으며, 수술 전 평가(2022년 3월)에서 기저 질환 조절이 양호해 수술이 진행 가능하다는 판단을 받았습니다. 수술 후 2023년 11월까지 병원에서 회복 중이며, 통증 관리와 재활 치료가 진행 중입니다. 현재 상태는 안정적이며, 주기적인 병원 방문과 관리가 필요합니다.

중요 사항:
- **수술 일정:** 2023년 3월 (수술 전 평가: 2022년 3월)
- **현재 상태:** 2023년 11월까지 회복 중 (통증 관리, 재활 중)
- **반복된 기록:** 일부 진료 기록이 중복되어 입력된 것으로 보이며, 데이터 정리가 필요합니다.

생성: 2026-06-07

환자 기본 정보

환자명	임은서
생년월일	1974년생
성별	여

진료 이력

재진 2026-06-19 10:12 PSYCH OPEN

재진 2026-06-19 10:06 PSYCH OPEN

재진 2026-06-19 10:05 PSYCH CLOSED

OPD 2025-03-16 04:43 PSYCH OPEN

진단 (ICD)

오늘의 진료

이전 진료 기록 복사

진료 유형

재진 외래 예약 유형 자동 적용

S — 주호소 (Subjective)

정기검진 목적으로 내원했으며 최근 환청이나 망상 없이 증상이 안정적이다. 약물을 매일 빠지지 않고 복용 중이며 식욕, 수면 모두 양호하다.

O — 검사소견 (Objective)

활력징후는 혈압 120/80, 맥박 75로 정상이고, 정신상태검사상 의식 맑음, 지남력 양호, 사고 논리적으로 망상이 없다. 환각이 없으며 약물 부작용(떨림, 근경직)도 관찰되지 않았다.

A — 진단/평가 (Assessment)

정신분열증으로 현재 약물 치료 중 증상이 안정적이고 약물 순응도가 양호하다. 재발 징후가 없으며 정신상태가 잘 유지되고 있다.

P — 치료계획 (Plan)

현재 약물을 계속 유지하고 3개월 후 정기검진을 재예약한다. 약물을 꾸준히 복용하고 스트레스 관리, 충분한 수면을 당부했다.

ICD 진단코드 + 추가

F20.9 정신분열증 주상병 ×

✓ 진료 완료

요구사항에 따른 구현

비용 최적화 운영 편의 AI활용 비용분석

SFR-015

키 관리

플랫폼별 독립 시크릿 관리 및 자동 로테이션

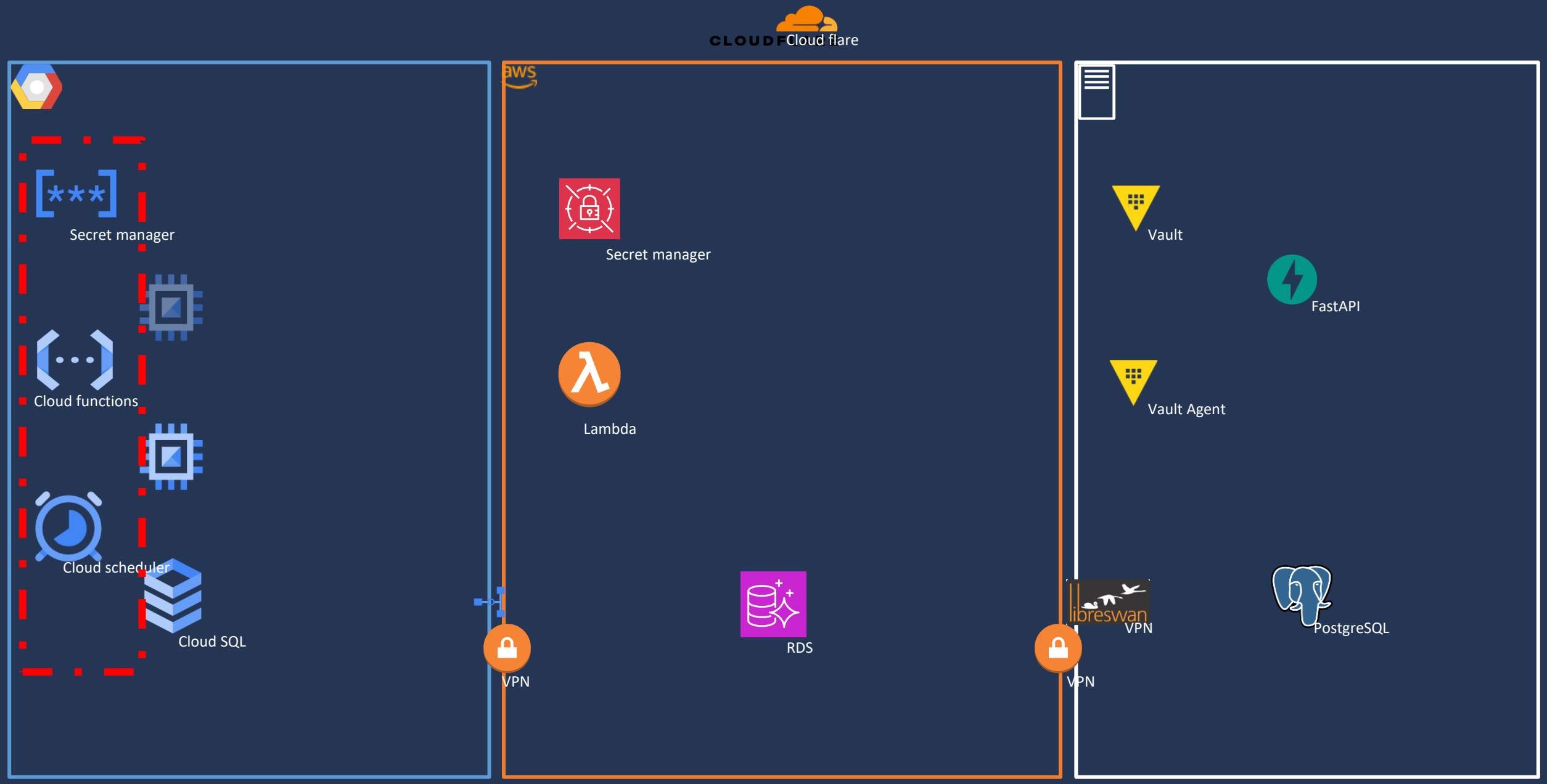
- ✓ Vault
- ✓ Secret Manager
- ✓ Lambda

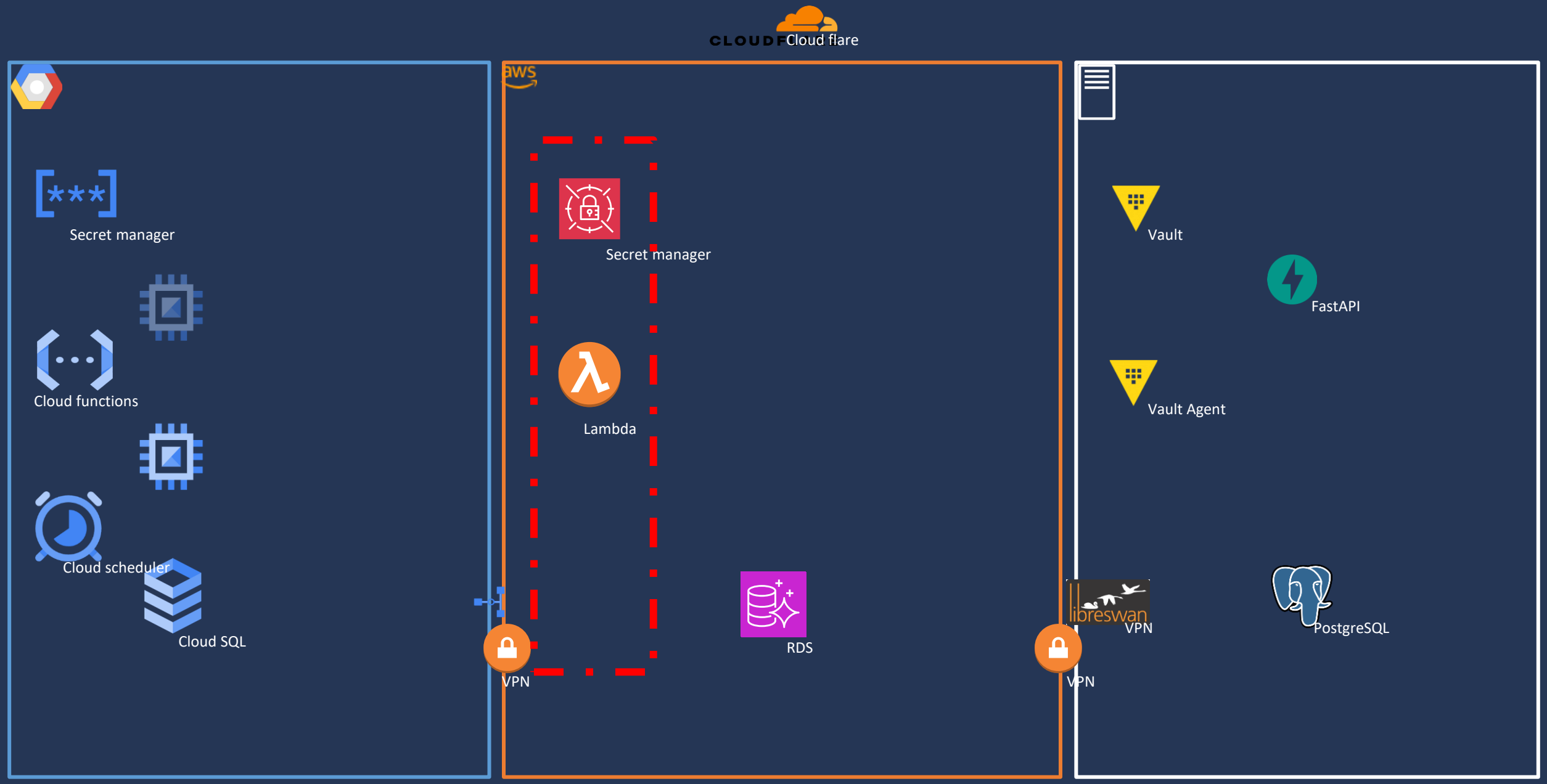
SFR-011

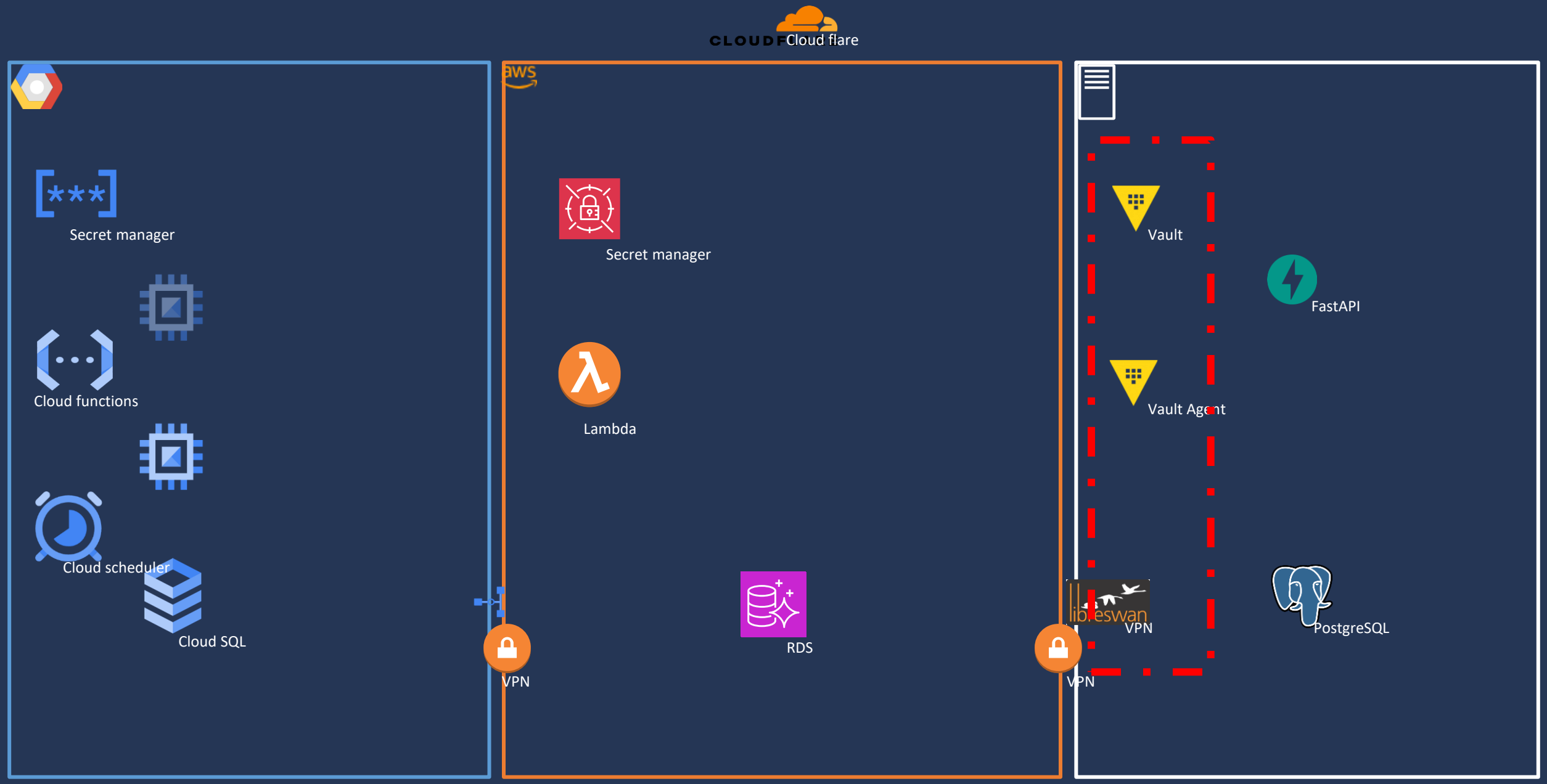
ISMS-P

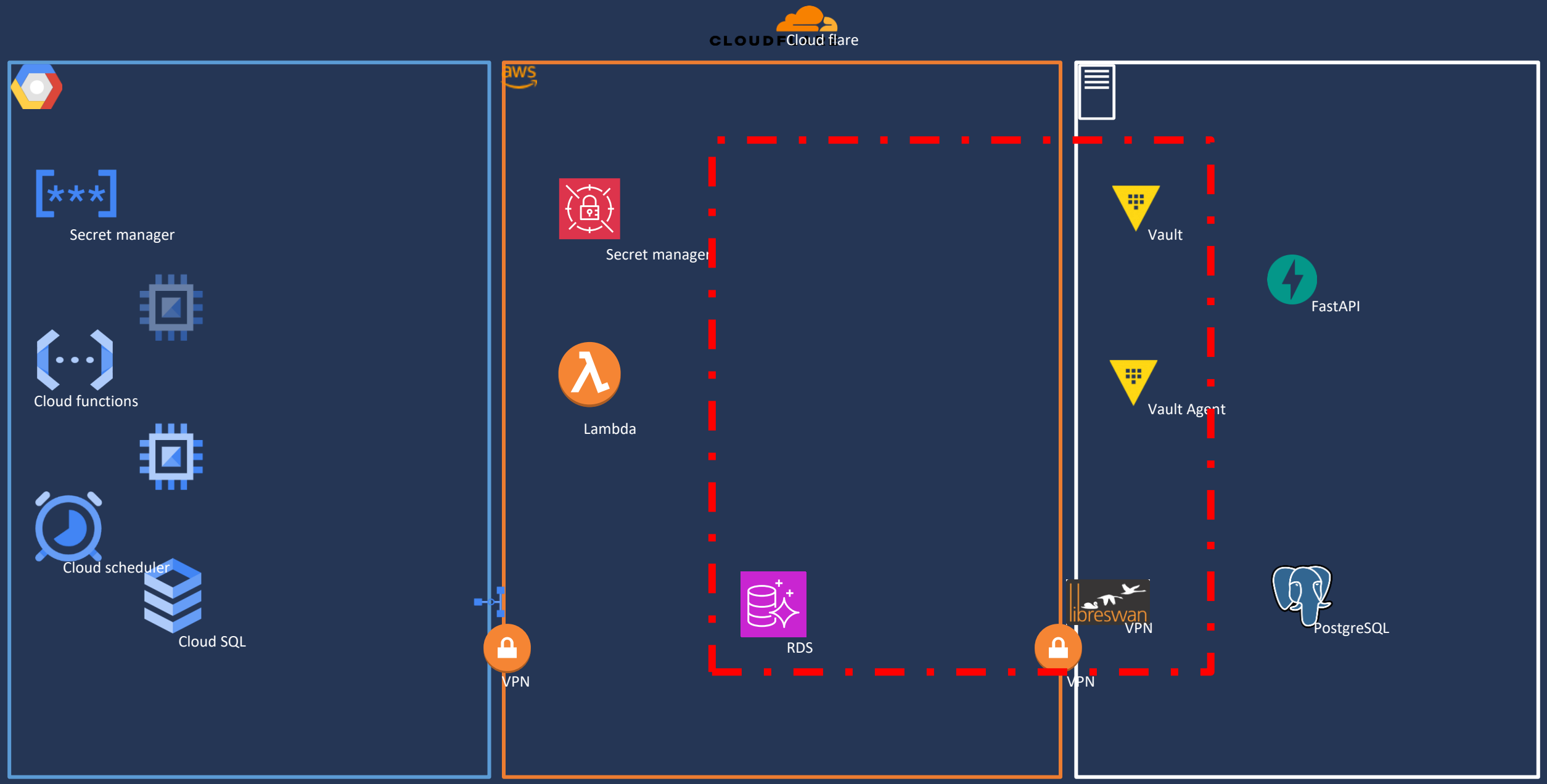
ISMS-P 기준 핵심 통제항목 이행

- ✓ ISMS-P 2.5.4 “시크릿 로테이션 7일”
- ✓ ISMS-P 2.9.4 “로그 보존 365일”
- ✓ ISMS-P 2.9.3 "백업 및 복구관리"


Cloud flare
Secret manager
Cloud functions
Cloud scheduler
Cloud SQL
VPN
Secret manager
Lambda
RDS
VPN
Vault
FastAPI
Vault Agent
libreswan
VPN
PostgreSQL

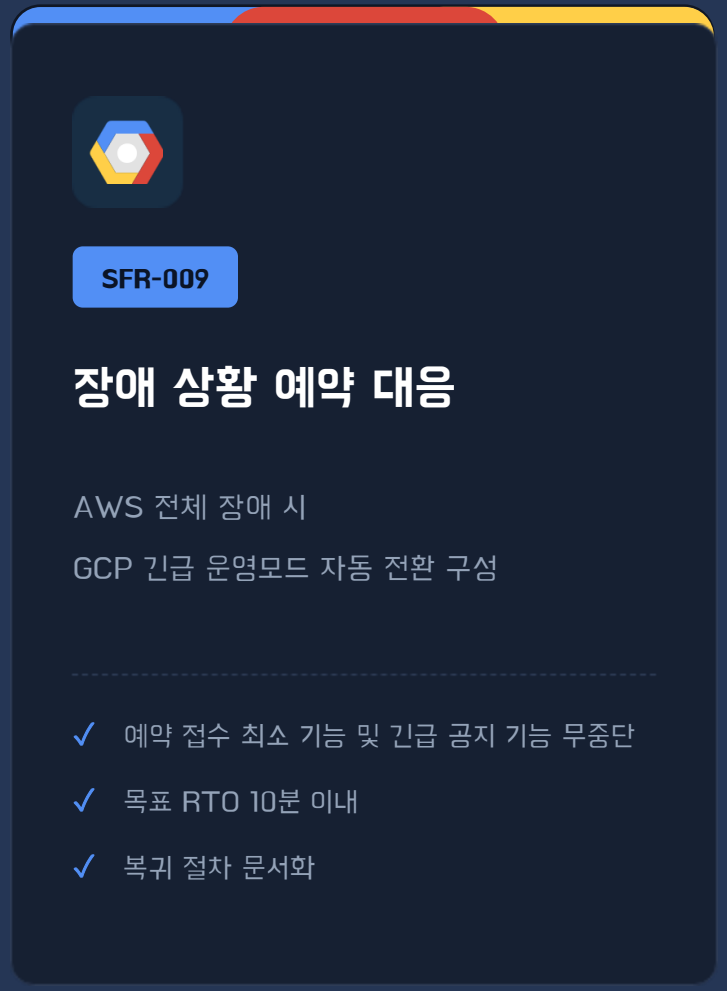

Cloud flare
Secret manager
Cloud functions
Cloud scheduler
Cloud SQL
Secret manager
Lambda
RDS
VPN
VPN
Vault
FastAPI
Vault Agent
libreswan
VPN
PostgreSQL

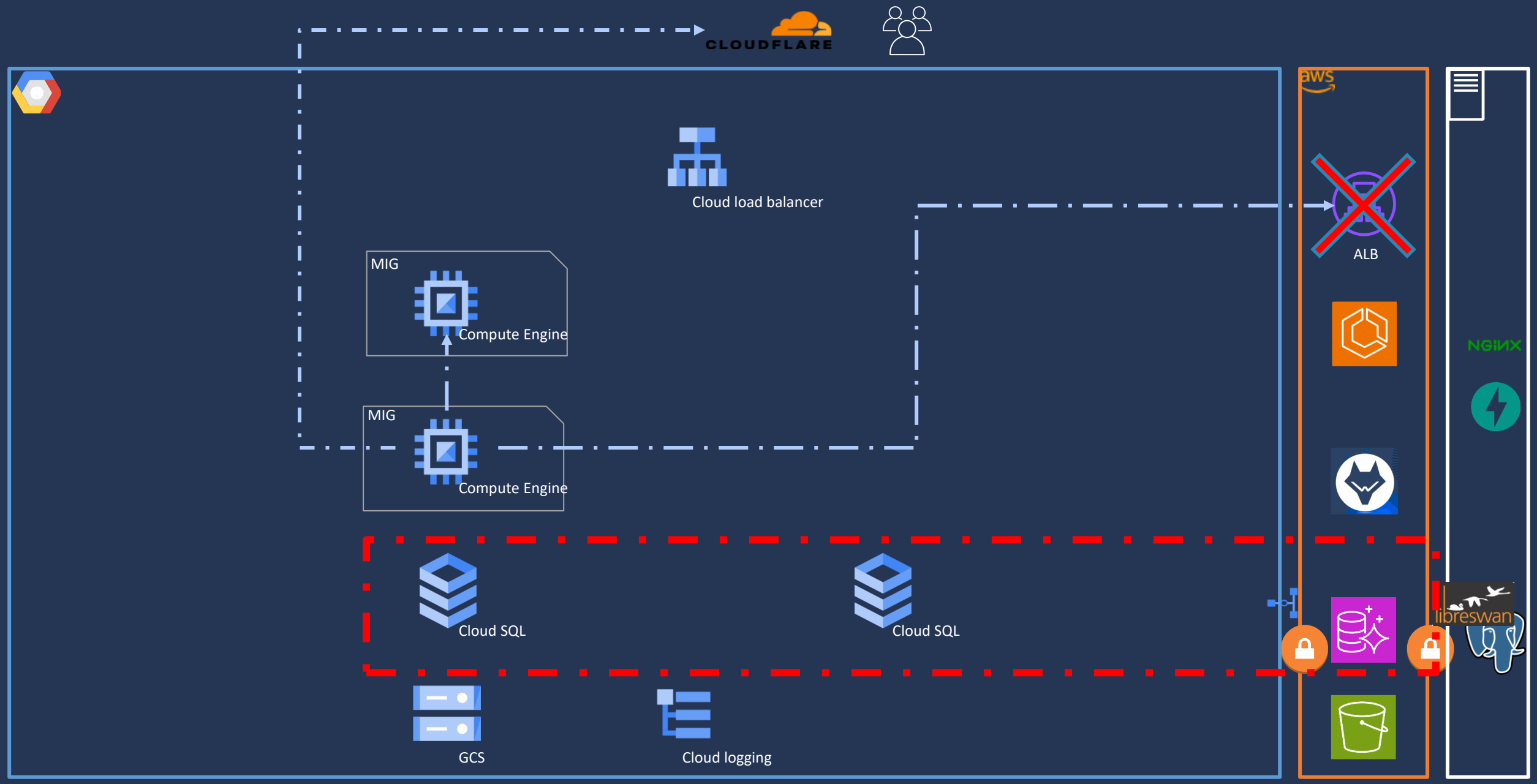

Cloud flare
Secret manager
Cloud functions
Cloud scheduler
Cloud SQL
Secret manager
Lambda
RDS
VPN
VPN
Vault
Vault Agent
FastAPI
VPN
PostgreSQL

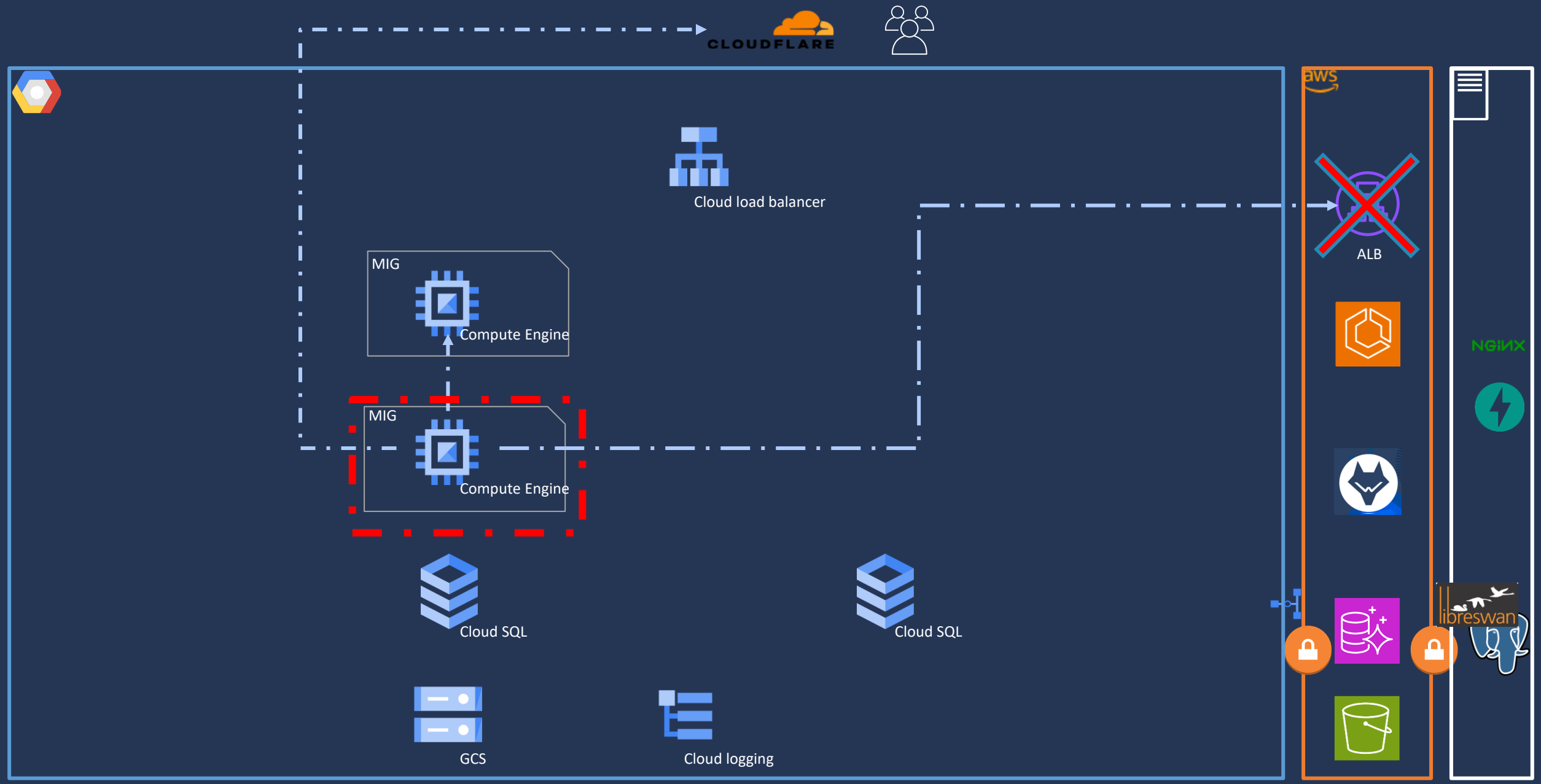

Cloud flare
Secret manager
Cloud functions
Cloud scheduler
Cloud SQL
Secret manager
Lambda
RDS
VPN
VPN
Vault
Vault Agent
FastAPI
libreswan
VPN
PostgreSQL

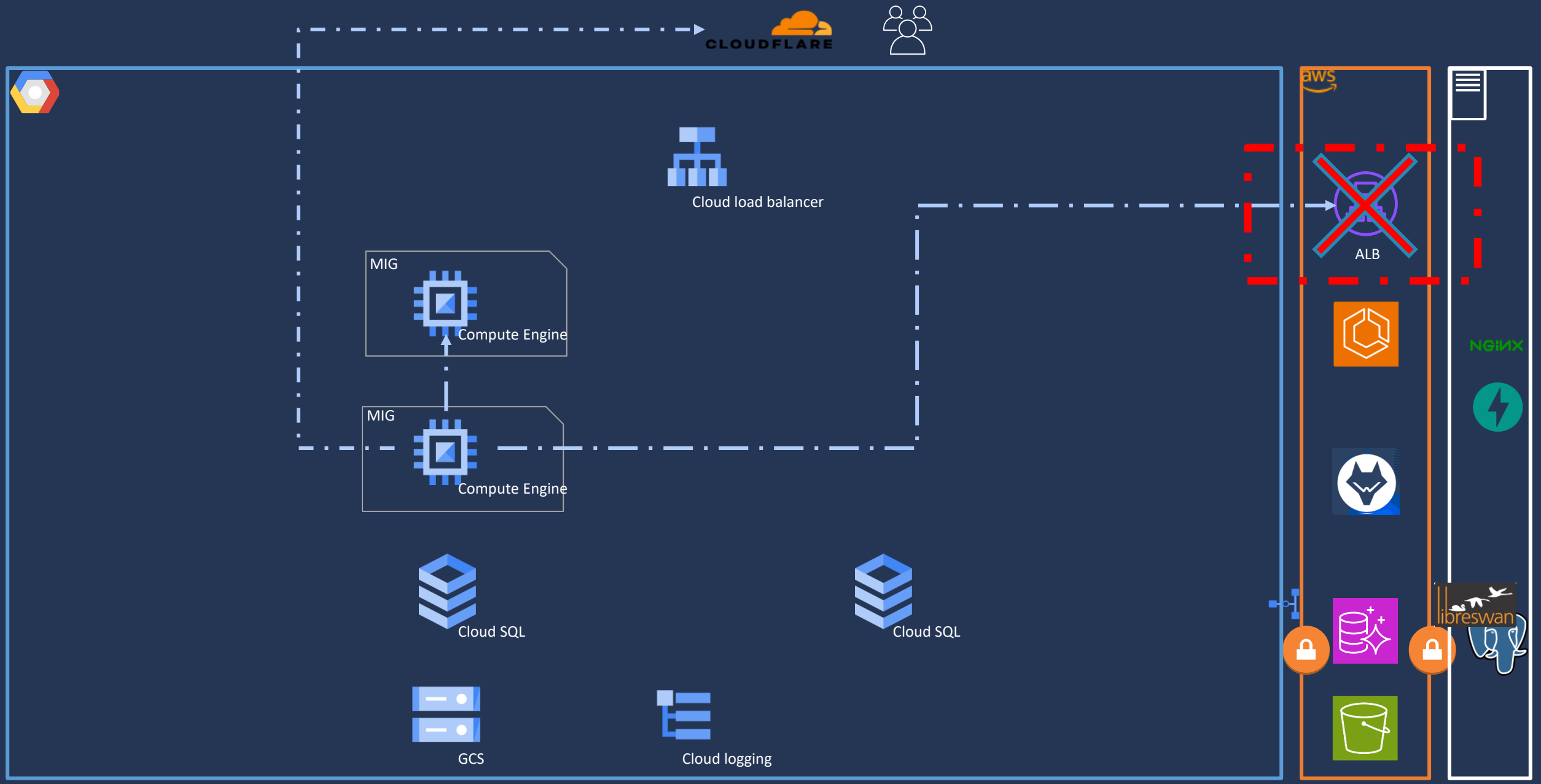
요구사항에 따른 구현

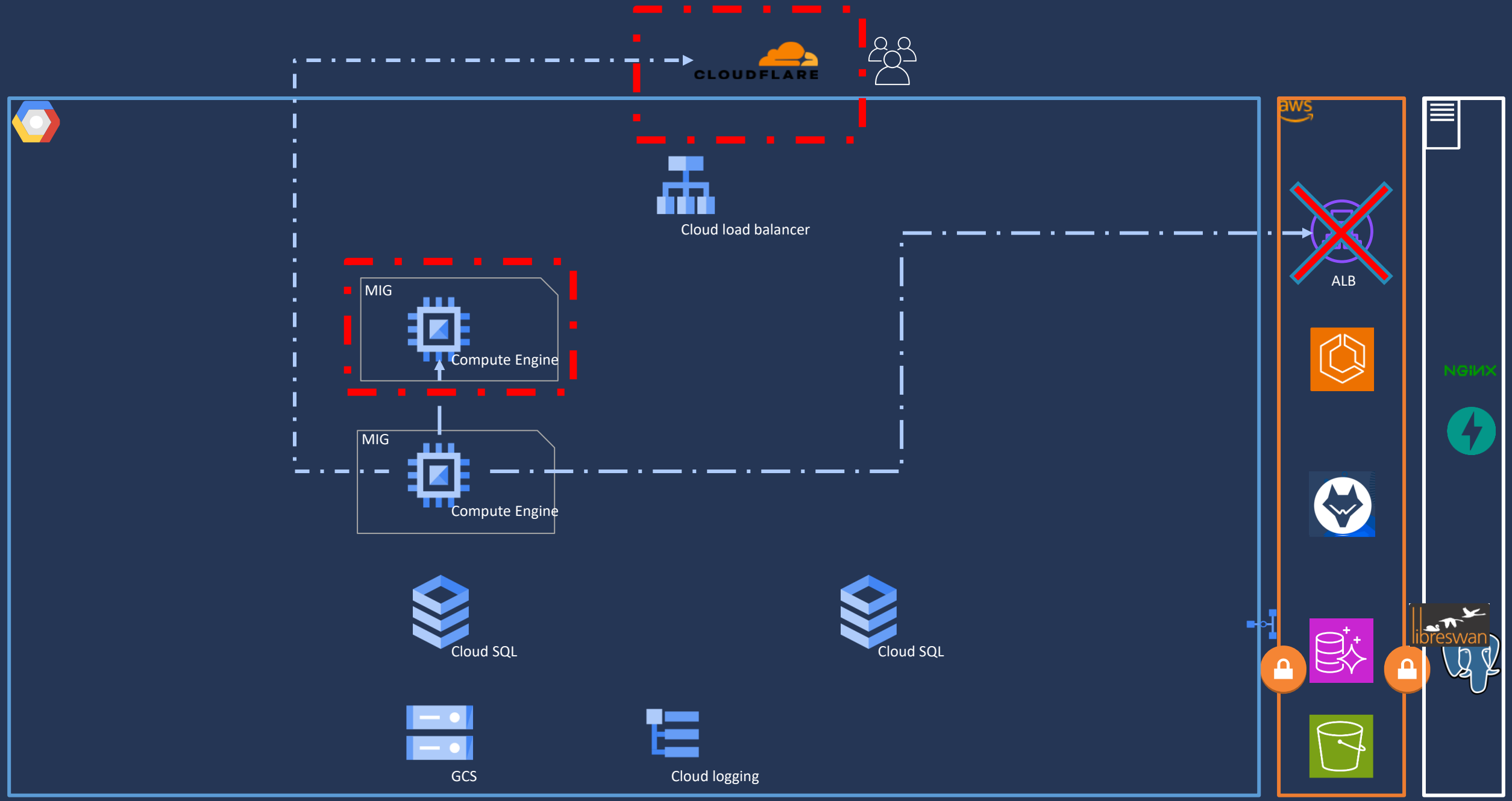
비용 최적화 운영 편의 AI활용 비용분석

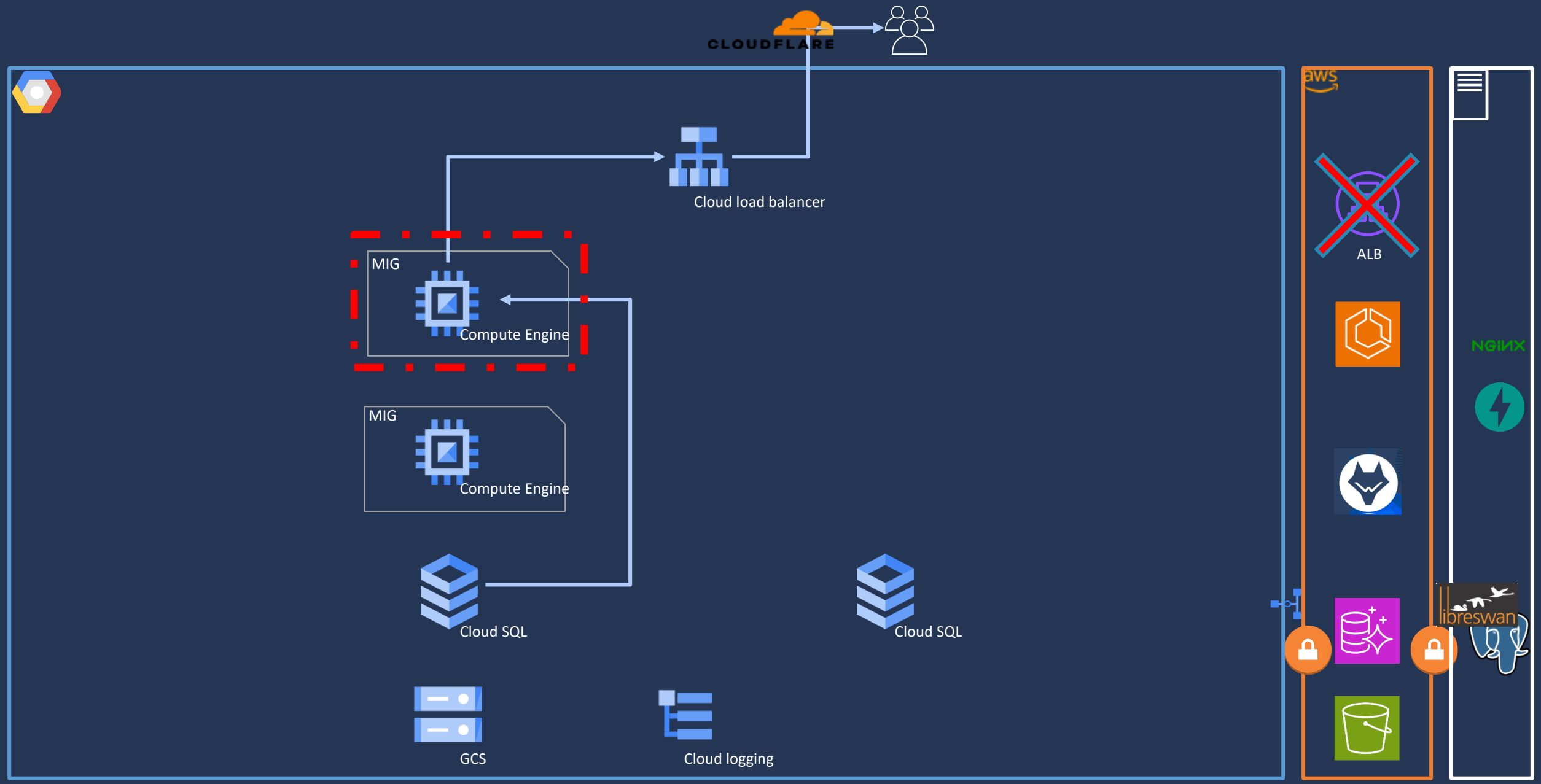


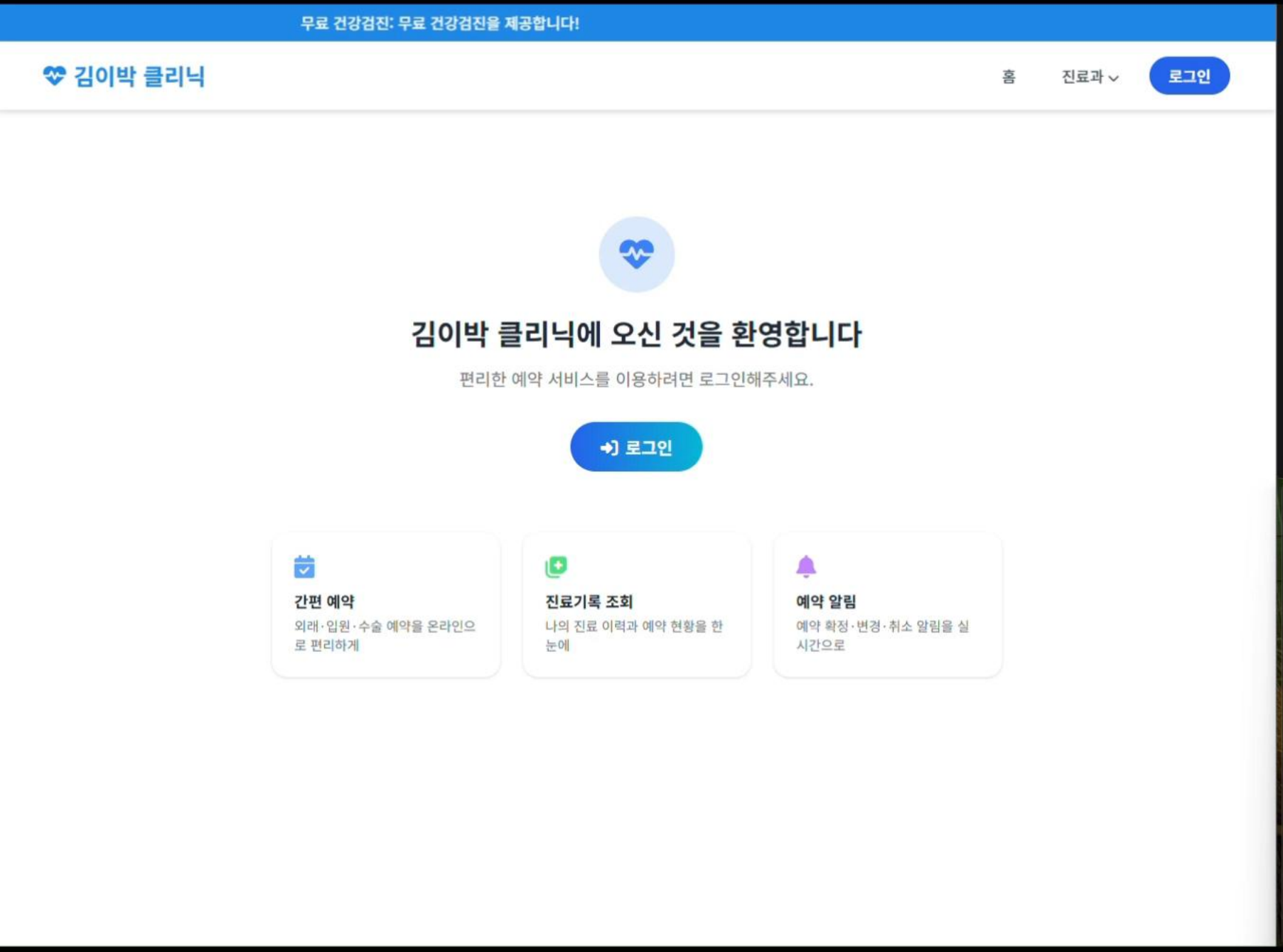

CLOUDFLARE
Cloud load balancer
MIG
Compute Engine
MIG
Compute Engine
aws
ALB
NGINX
libreswan
Cloud SQL
Cloud SQL
GCS
Cloud logging

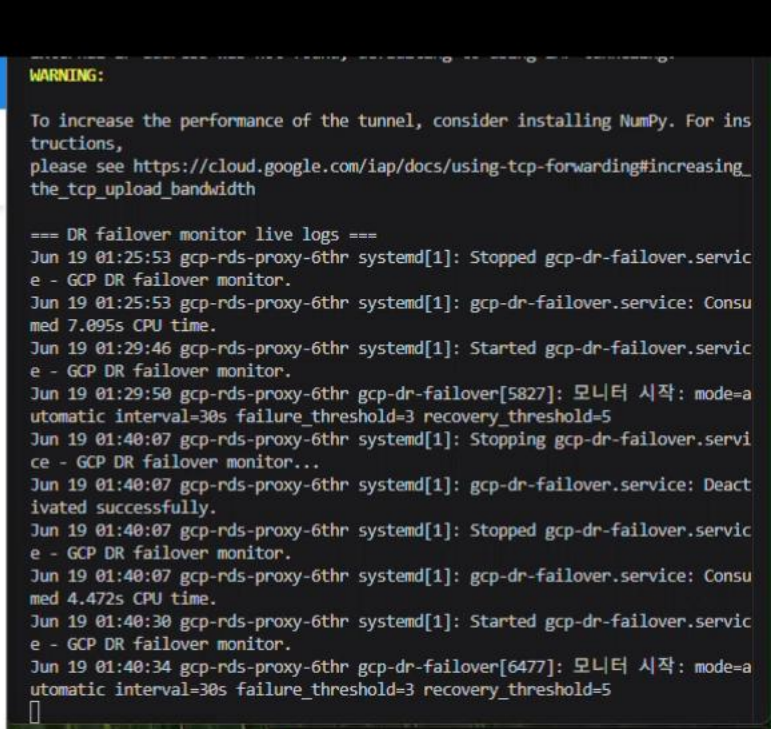

CLOUDFLARE
Cloud load balancer
MIG
Compute Engine
MIG
Compute Engine
Cloud SQL
Cloud SQL
GCS
Cloud logging
aws
ALB
NGINX
libreswan

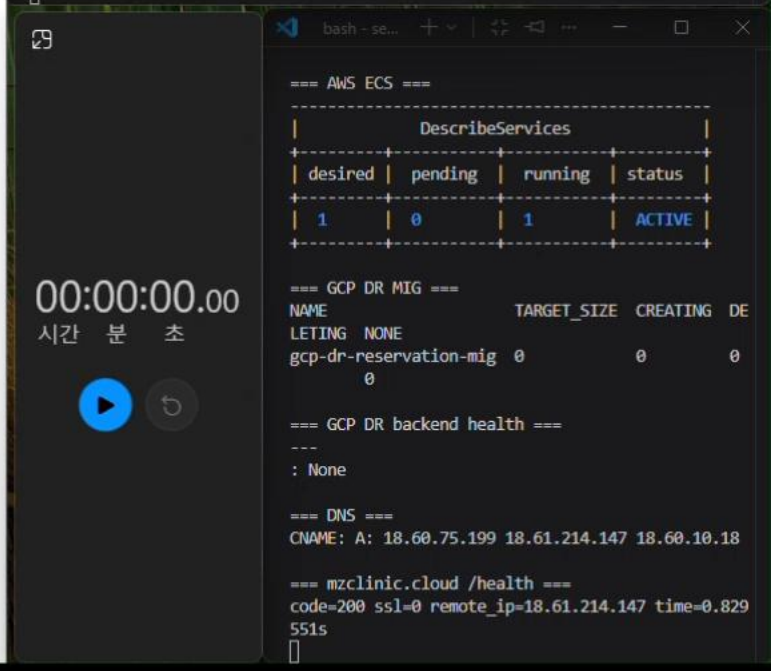

CLOUDFLARE
Cloud load balancer
MIG
Compute Engine
MIG
Compute Engine
Cloud SQL
Cloud SQL
GCS
Cloud logging
aws
ALB
NGINX
libreswan


CLOUDFLARE
Cloud load balancer
MIG
Compute Engine
MIG
Compute Engine
Cloud SQL
Cloud SQL
GCS
Cloud logging
aws
ALB
NGINX
libreswan


CLOUDFLARE
Cloud load balancer
MIG
Compute Engine
MIG
Compute Engine
Cloud SQL
Cloud SQL
GCS
Cloud logging
aws
ALB
NGINX
libreswan


무료 건강검진: 무료 건강검진을 제공합니다!
김이박 클리닉
홈
진료과
로그인
김이박 클리닉에 오신 것을 환영합니다
편리한 예약 서비스를 이용하려면 로그인해주세요.
로그인
간편 예약
외래·입원·수술 예약을 온라인으로 편리하게
진료기록 조회
나의 진료 이력과 예약 현황을 한눈에
예약 알림
예약 확정·변경·취소 알림을 실시간으로


WARNING:
To increase the performance of the tunnel, consider installing NumPy. For instructions,
please see https://cloud.google.com/iap/docs/using-tcp-forwarding#increasing_the_tcp_upload_bandwidth
=== DR failover monitor live logs ===
Jun 19 01:25:53 gcp-rds-proxy-6thr systemd[1]: Stopped gcp-dr-failover.service - GCP DR failover monitor.
Jun 19 01:25:53 gcp-rds-proxy-6thr systemd[1]: gcp-dr-failover.service: Consumed 7.095s CPU time.
Jun 19 01:29:46 gcp-rds-proxy-6thr systemd[1]: Started gcp-dr-failover.service - GCP DR failover monitor.
Jun 19 01:29:50 gcp-rds-proxy-6thr gcp-dr-failover[5827]: 모니터 시작: mode=automatic interval=30s failure_threshold=3 recovery_threshold=5
Jun 19 01:40:07 gcp-rds-proxy-6thr systemd[1]: Stopping gcp-dr-failover.service - GCP DR failover monitor...
Jun 19 01:40:07 gcp-rds-proxy-6thr systemd[1]: gcp-dr-failover.service: Deactivated successfully.
Jun 19 01:40:07 gcp-rds-proxy-6thr systemd[1]: Stopped gcp-dr-failover.service - GCP DR failover monitor.
Jun 19 01:40:07 gcp-rds-proxy-6thr systemd[1]: gcp-dr-failover.service: Consumed 4.472s CPU time.
Jun 19 01:40:30 gcp-rds-proxy-6thr systemd[1]: Started gcp-dr-failover.service - GCP DR failover monitor.
Jun 19 01:40:34 gcp-rds-proxy-6thr gcp-dr-failover[6477]: 모니터 시작: mode=automatic interval=30s failure_threshold=3 recovery_threshold=5


00:00:00.00
시간 분 초
bash - se...
=== AWS ECS ===
DescribeServices
desired | pending | running | status
1 | 0 | 1 | ACTIVE
=== GCP DR MIG ===
NAME TARGET_SIZE CREATING DELETING NONE
gcp-dr-reservation-mig 0 0 0 0
=== GCP DR backend health ===
: None
=== DNS ===
CNAME: A: 18.60.75.199 18.61.214.147 18.60.10.18
=== mzclinic.cloud /health ===
code=200 ssl=0 remote_ip=18.61.214.147 time=0.829551s

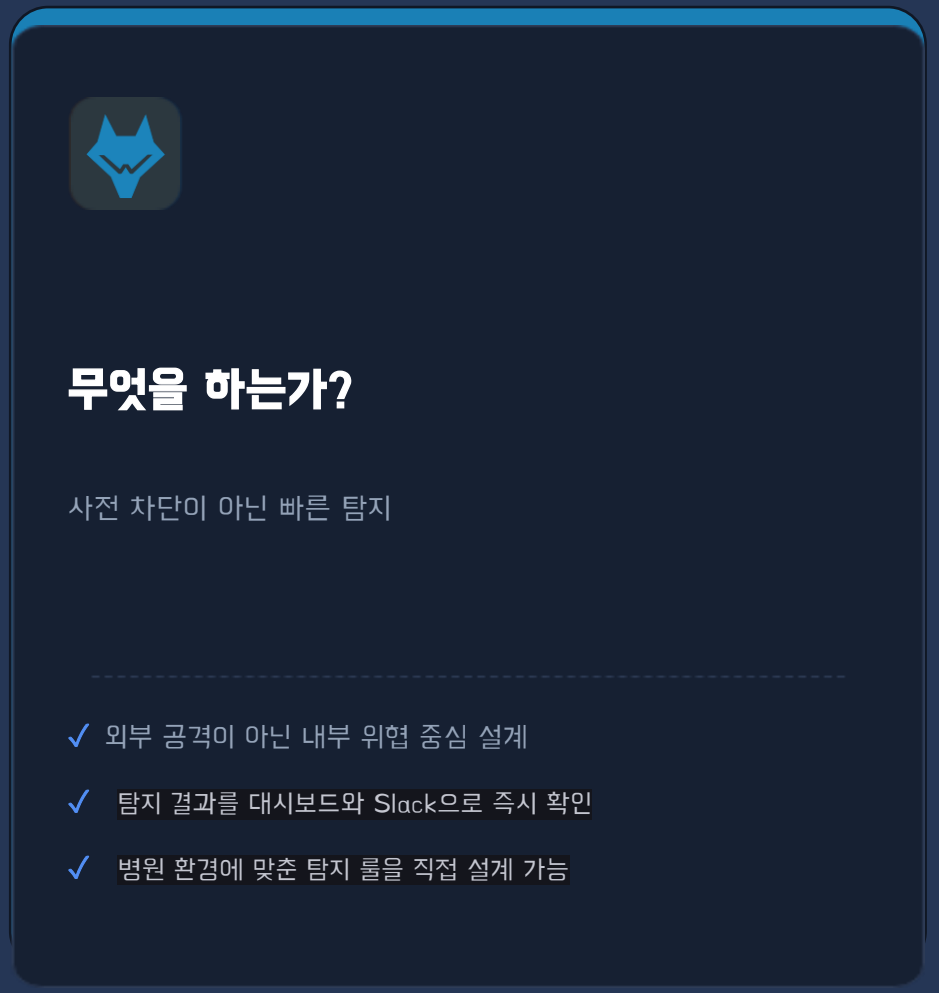
보안 운영 관제

담당자 ○○○

와주란?

What is Wazuh?

서버의 로그와 행위를 실시간으로 감시해,
보안 위협을 탐지하는 오픈소스 플랫폼



Wazuh 구성 요소

Agent

로그를 수집하고

매니저로 전송

Manager

룰로 분석하고

위협 판단

Indexer

결과를 저장하고

인덱싱

Dashboard

데이터를 시각화하고

조회 확인

Wazuh 구성 요소

Agent

로그를 수집하고

매니저로 전송

Manager

룰로 분석하고

위협 판단

Indexer

결과를 저장하고

인덱싱

Dashboard

데이터를 시각화하고

조회 확인

Wazuh 구성 요소

Agent

로그를 수집하고

매니저로 전송

Manager

룰로 분석하고

위협 판단

Indexer

결과를 저장하고

인덱싱

Dashboard

데이터를 시각화하고

조회 확인

Wazuh 구성 요소

Agent

로그를 수집하고

매니저로 전송

Manager

룰로 분석하고

위협 판단

Indexer

결과를 저장하고

인덱싱

Dashboard

데이터를 시각화하고

조회 확인

와주 도입 이유

공격 패턴 탐지 , 취약점 탐지 , SIEM

AWS 보안 서비스의 한계

보안의 사각지대가 곧 가장 민감한 데이터의 위치

- ✓ 온프레미스는 탐지 범위 밖
- ✓ OS 내부 실시간 파일 변조 탐지 기능 x
- ✓ 파일 변조나 내부자 이상 행위를 실시간으로 탐지하는 기능 제공 x

환경 통합 Agent 배포

AWS GCP 온프레미스 어디든 동일하게 설치

- ✓ 하이브리드 환경에 적합
- ✓ 인프라가 달라도 동일한 보안 기준 유지
- ✓ 하이브리드 환경에서도 끊김 없는 일관된 탐지

사전 차단이 아닌 빠른 탐지

사전 차단이 아닌 빠른 탐지

- ✓ 외부 공격이 아닌 내부 위협 중심 설계
- ✓ 랜섬웨어 데이터 유출 패턴 즉시 탐지
- ✓ 사고 인지까지 걸리는 시간 최소화

왜 다른 SIEM이 아닌 Wazuh인가?

공격 패턴 탐지 , 취약점 탐지 , SIEM

	Wazuh	Elastic Security	Splunk	OSSEC
비용	무료	일부 유료	데이터량 기반 과금	무료
파일 무결성 검사	내장	별도 모듈 필요	별도로 필요	내장
SIEM 대시보드	내장	강력함	매우 강력함	없음
멀티 환경 통합	가능	가능 , 설정 복잡	가능 , 비용 증가	없음

요구사항에 따른 구현

예약 인증 가용성

SFR-007

로그 수집 및 통합 관리

온프레미스 및 AWS 로그 통합 수집 분석

- ✓ 온프레미스 로그 직접 수집 전송
- ✓ AWS 로그 수집 Wazuh 연계
- ✓ GCP 감사로그 보존

SFR-005

SIEM 위협 탐지

Wazuh 기반 내부자 위협 및 랜섬웨어 탐지 구현

- ✓ 비정상 조회 및 접근 탐지
- ✓ 병원 내부자 위협 시나리오 선정 탐지 룰 구현
- ✓ USB 대량 복사 등 이동식 저장매체 반출 시도 탐지

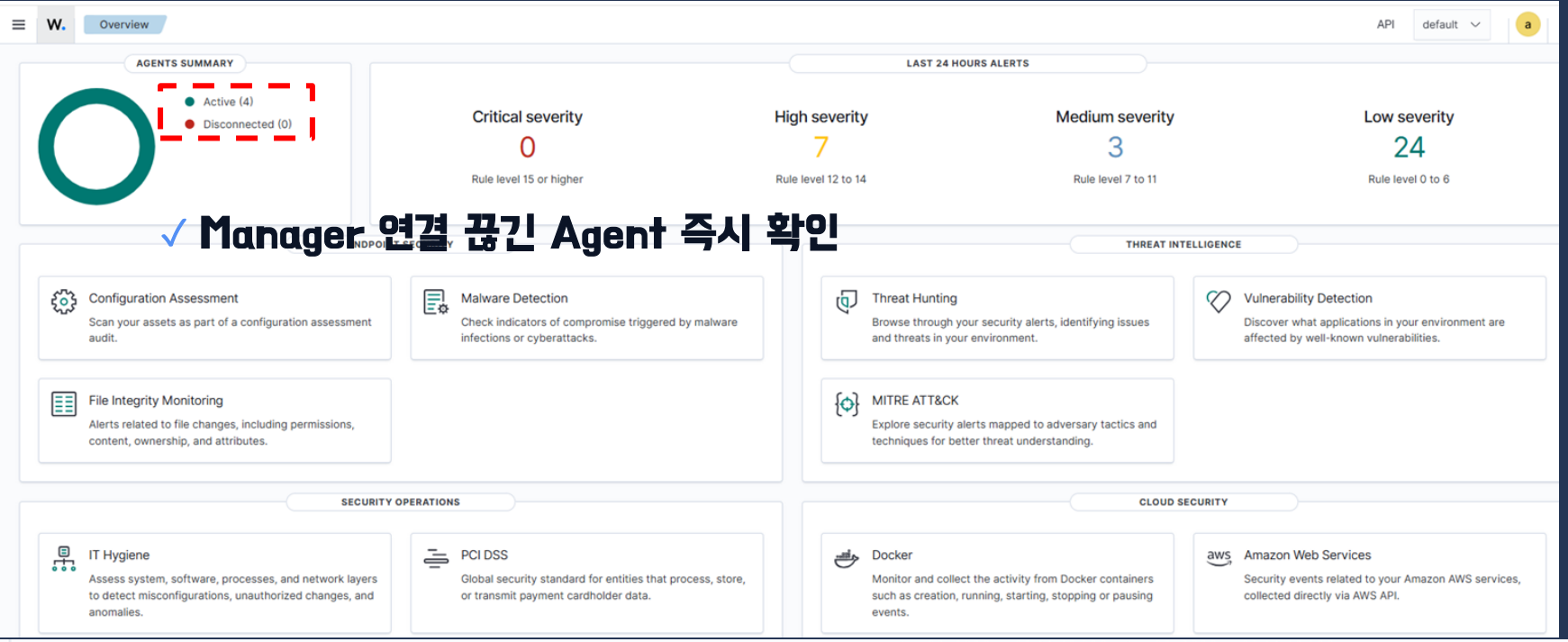
○○○,
개인 프로젝트

SFR-019

보안 관제 및 일일 보고 자동화

일일 보안 보고서를 생성하여 Slack으로 발송하는 보안 관제 자동화 시스템

- ✓ 각각의 인프라 보안 이벤트를 수집하고 저장
- ✓ 전일 보안 이벤트를 자동 집계
- ✓ 취약점 스냅샷 분석 포함



Jun 22, 2026 @ 09:14:48.896 - Jun 23, 2026 @ 09:14:48.896

Export Formatted | Reset view | 884 available fields | Columns | Density | 1 fields sorted | Full screen

✓ 어떤 룰에 걸려서 어떤 레벨로 탐지됐는지 확인 가능

timestamp	agent.name	rule.description	rule.level	rule.id
Jun 23, 2026 @ 09:13:06.325	ip-10-0-11-66	Lambda 실행 실패 탐지 — [ERROR]	12	100830
Jun 23, 2026 @ 09:13:06.323	ip-10-0-11-66	Lambda 실행 실패 탐지 — [ERROR]	12	100830
Jun 23, 2026 @ 09:13:06.322	ip-10-0-11-66	Lambda 실행 실패 탐지 — [ERROR]	12	100830
Jun 23, 2026 @ 09:13:06.319	ip-10-0-11-66	Lambda 실행 실패 탐지 — [ERROR]	12	100830
Jun 23, 2026 @ 09:12:30.888	ip-10-0-11-66	파일 무결성 변조 감지 — 경로: /var/ossec/etc/rules/alb_rules.xml 변경 항목: size,inode,mtime,md5,sha1,sha256	12	550
Jun 23, 2026 @ 09:12:21.388	ip-10-0-11-66	sudo root 권한 전환 — 사용자: ssm-user 실행 명령: /usr/bin/vi /var/ossec/etc/rules/alb_rules.xml	8	100001
Jun 23, 2026 @ 09:10:03.380	ip-10-0-11-66	sudo root 권한 전환 — 사용자: ssm-user 실행 명령: /usr/bin/cat /var/ossec/etc/rules/local_rules.xml	8	100001
Jun 23, 2026 @ 09:06:16.906	ip-10-0-11-66	파일 무결성 변조 감지 — 경로: /var/ossec/etc/rules/lambda_rules.xml 변경 항목: inode,mtime	12	550
Jun 23, 2026 @ 09:06:15.366	ip-10-0-11-66	sudo root 권한 전환 — 사용자: ssm-user 실행 명령: /usr/bin/vi /var/ossec/etc/rules/lambda_rules.xml	8	100001
Jun 23, 2026 @ 09:05:39.364	ip-10-0-11-66	sudo root 권한 전환 — 사용자: ssm-user 실행 명령: /usr/bin/vi /var/ossec/etc/rules/alb_rules.xml	8	100001
Jun 23, 2026 @ 08:01:36.296	ecs-ec2-10-0-13-15	Wazuh agent stopped.	3	506
Jun 23, 2026 @ 07:51:06.719	gcp-rds-proxy-01	Cloud SQL 관리자 작업 탐지 — action: ADMIN_AUTOMATICSTORA	8	100202
Jun 23, 2026 @ 07:48:00.455	ip-10-0-11-66	RDS 클라이언트 접속 기록	3	100113
Jun 23, 2026 @ 07:46:08.071	ecs-ec2-10-0-13-15	systemd 서비스 파일 변경 탐지 (/etc) - persistence 의심	13	100020
Jun 23, 2026 @ 07:46:08.065	ecs-ec2-10-0-13-15	systemd 서비스 파일 변경 탐지 (/etc) - persistence 의심	13	100020

탐지 룰 설계

1

베이스 룰 찾기

로그 중류만 식별

2

조건 걸기

if_sid로 참조 + 조건 추가

3

위험도 부여

level 설정 alert

예) Rule 100650 (베이스) Rule 100654 (조건: 60초 내 50회) 데이터 유출 탐지 (level 12)

탐지 룰 설계

1

베이스 룰 찾기

로그 중류만 식별

2

조건 걸기

if_sid로 참조 + 조건 추가

3

위험도 부여

level 설정 alert

예) Rule 100650 (베이스) Rule 100654 (조건: 60초 내 50회) 데이터 유출 탐지 (level 12)

탐지 룰 설계

1

베이스 룰 찾기

로그 중류만 식별

2

조건 걸기

if_sid로 참조 + 조건 추가

3

위험도 부여

level 설정 alert

예) Rule 100650 (베이스) Rule 100654 (조건: 60초 내 50회) 데이터 유출 탐지 (level 12)

11:22:21

```
mspadmin@mspserver:~$ curl -o /home/mspadmin/deidentification-api/ransomware_payloa
sh http://127.0.0.1:8888/ransomware_demo.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  6757  100  6757    0     0  7087k      0 --:--:-- --:--:-- --:--:-- 6598k
mspadmin@mspserver:~$
```

100651 *(Level 12)*

어제 오후 9:54 봇이 추가한 wazuh-slack

VAZUH Alert

온프레미스 DB 위험 이벤트 — LOCK_USER 사용자: cfae00e0-62f2-41ad-b5d9-65521397f2fe IP: 127.0.0.1 테이블: users

{"audit_log_id":"decd1538-76f4-43ee-a34a-2fad7bb617ce","user_id":"cfae00-41ad-b5d9-65521397f2fe","patient_id":null,"action_type":"LOCK_USER","target_table":"ut_id":"6b416483-3d6a-4b43-9ce2-83ad6ed5ba6f","source_ip":"127.0.0.1","result_code":"200","event_at":"2026-18T12:53:25.04075"}

Agent

(003) - onprem-mspserver

Location

/var/log/deident/db_audit.log

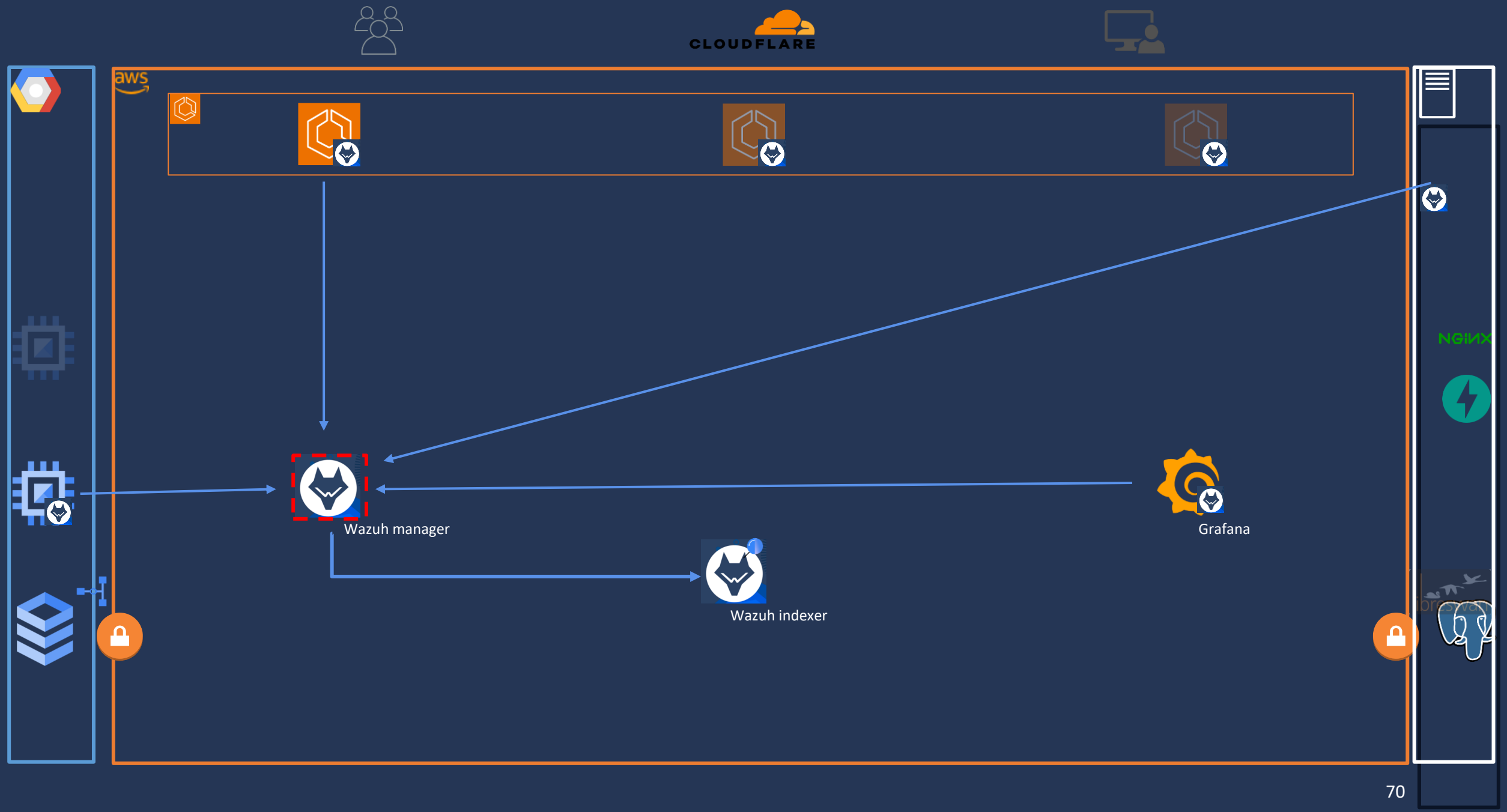
Rule ID

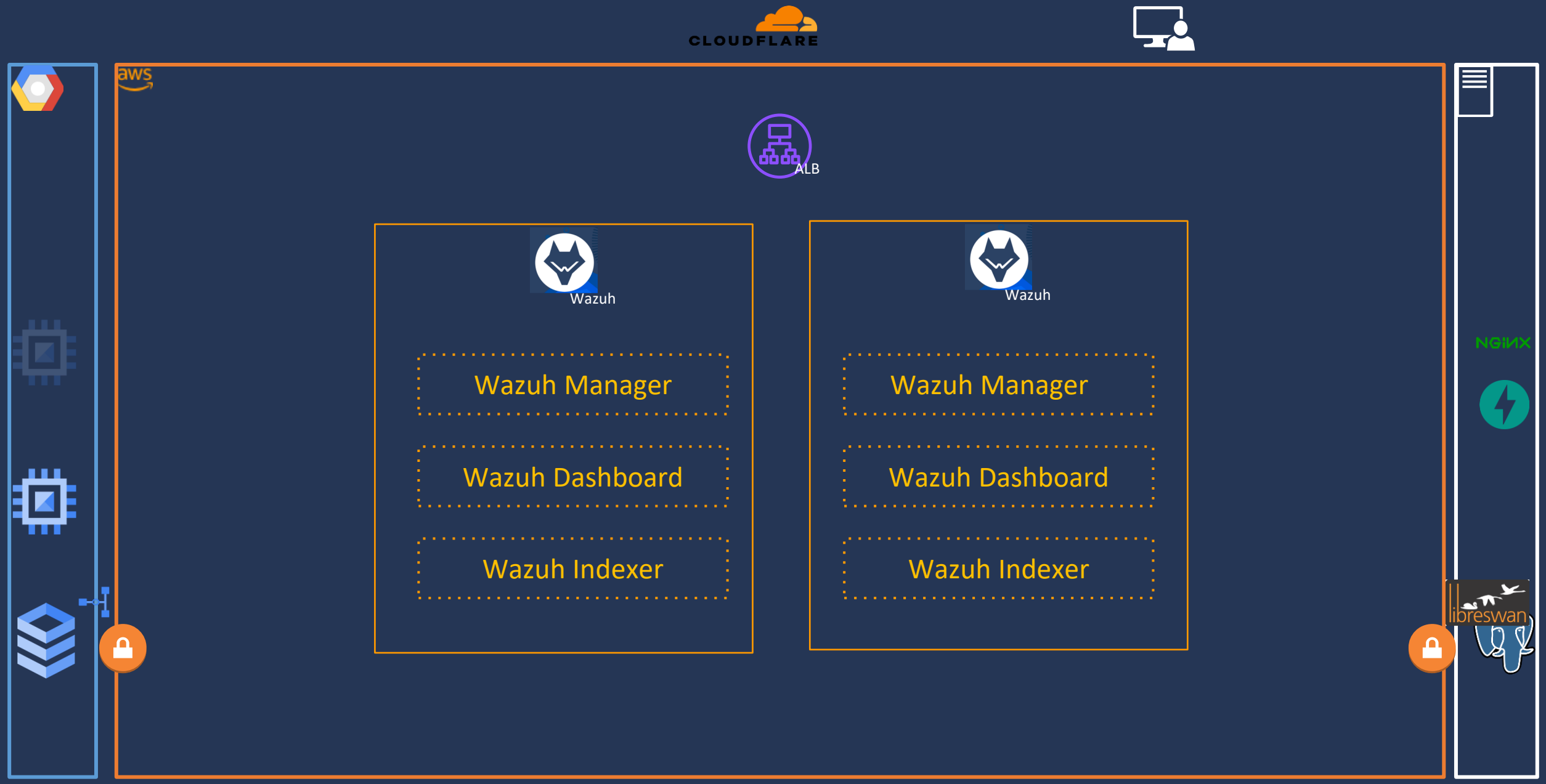
100651 *(Level 12)*

어제 오후 9:54 봇이 추가한 wazuh-slack

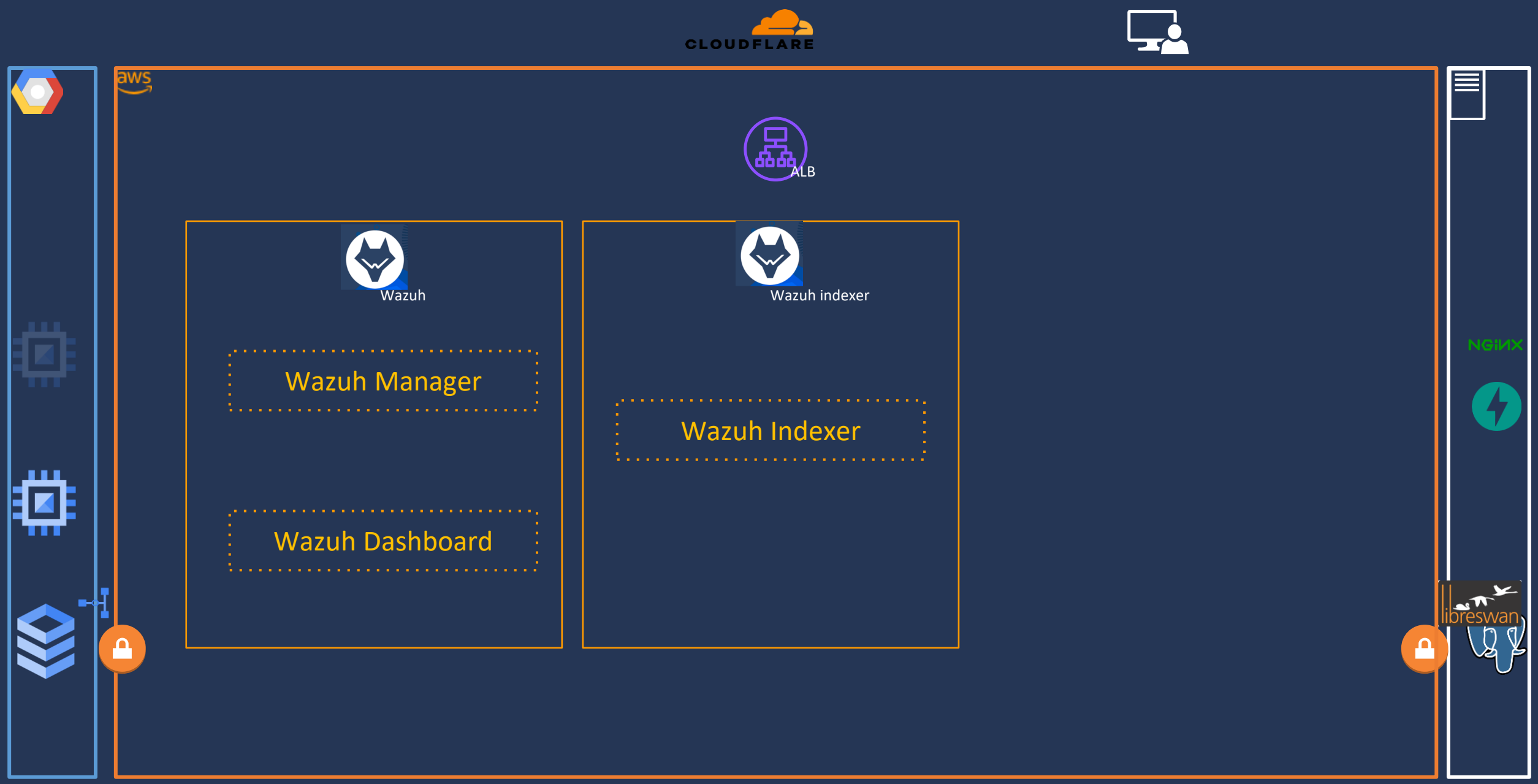
STEP 0 — 공격 준비

랜섬웨어 페이로드를 다운로드하고 실행 권한(chmod +x)을 부여합니다


CLOUDFLARE
aws
NGINX
Wazuh manager
Grafana
Wazuh indexer


CLOUDFLARE
aws
ALB
Wazuh
Wazuh Manager
Wazuh Dashboard
Wazuh Indexer
Wazuh
Wazuh Manager
Wazuh Dashboard
Wazuh Indexer
NGINX
libreswan


CLOUDFLARE
aws
ALB
Wazuh
Wazuh indexer
Wazuh
Wazuh Manager
Wazuh Indexer
Wazuh Manager
Wazuh Dashboard
Wazuh Dashboard
NGINX
libreswan


CLOUDFLARE
aws
ALB
Wazuh
Wazuh indexer
Wazuh Manager
Wazuh Indexer
Wazuh Dashboard
NGINX
libreswan

요구사항에 따른 구현

비용 최적화 운영 편의 AI활용 비용분석

SFR-014

SIEM 인프라 자동 복구 시스템

SIEM 인프라 인스턴스가 중지 또는 종료될 경우 자동으로 재구축하는 자동 복구 시스템

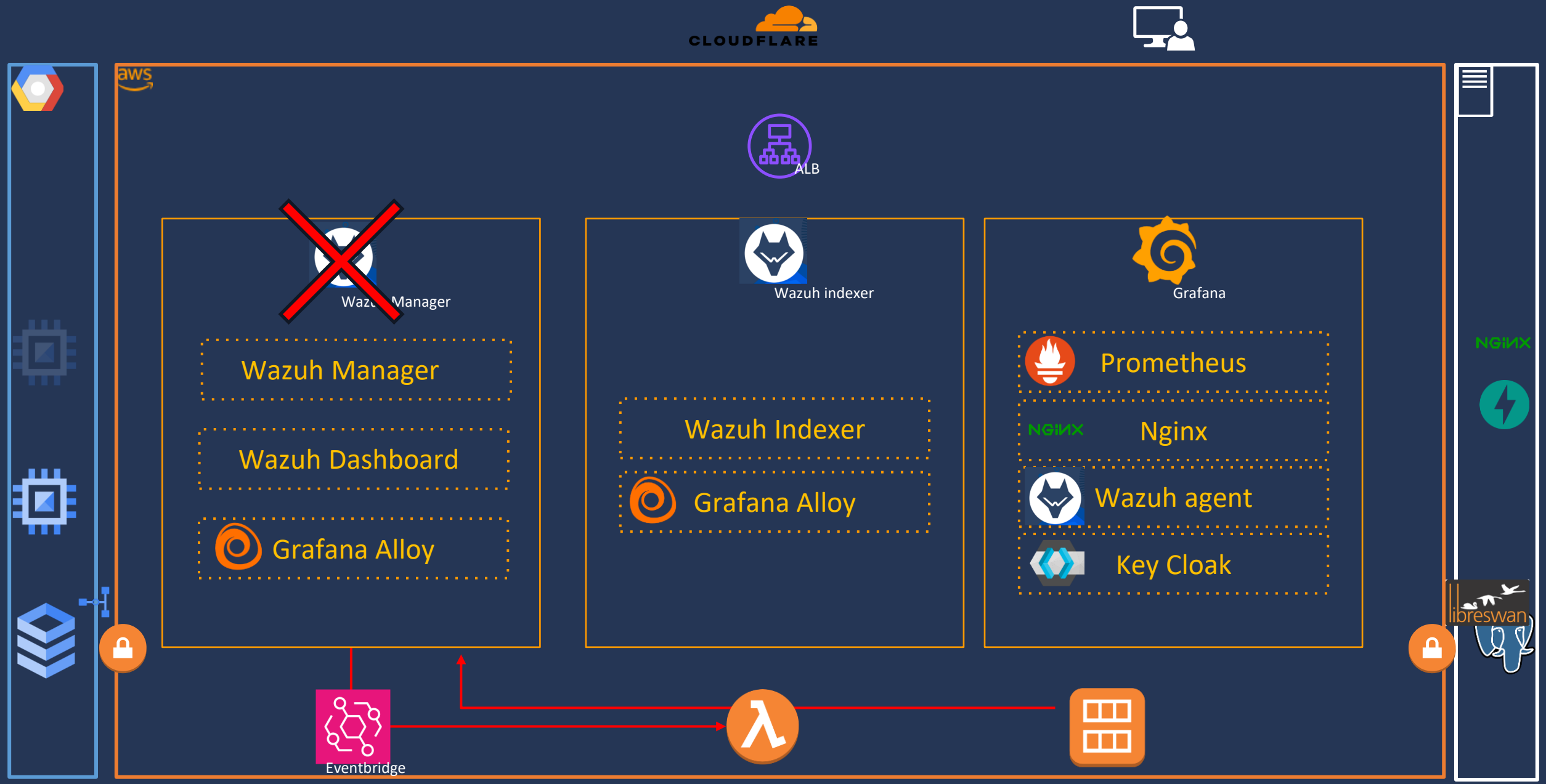
- ✓ Wazuh 매니저, 인덱서, 모니터링 서버의 최신 Golden AMI 구축
- ✓ 복구 시 데이터 보존 및 연속성 확보
- ✓ 중지/종료 이벤트 발생 시 즉시 알림을 발송

SFR-012

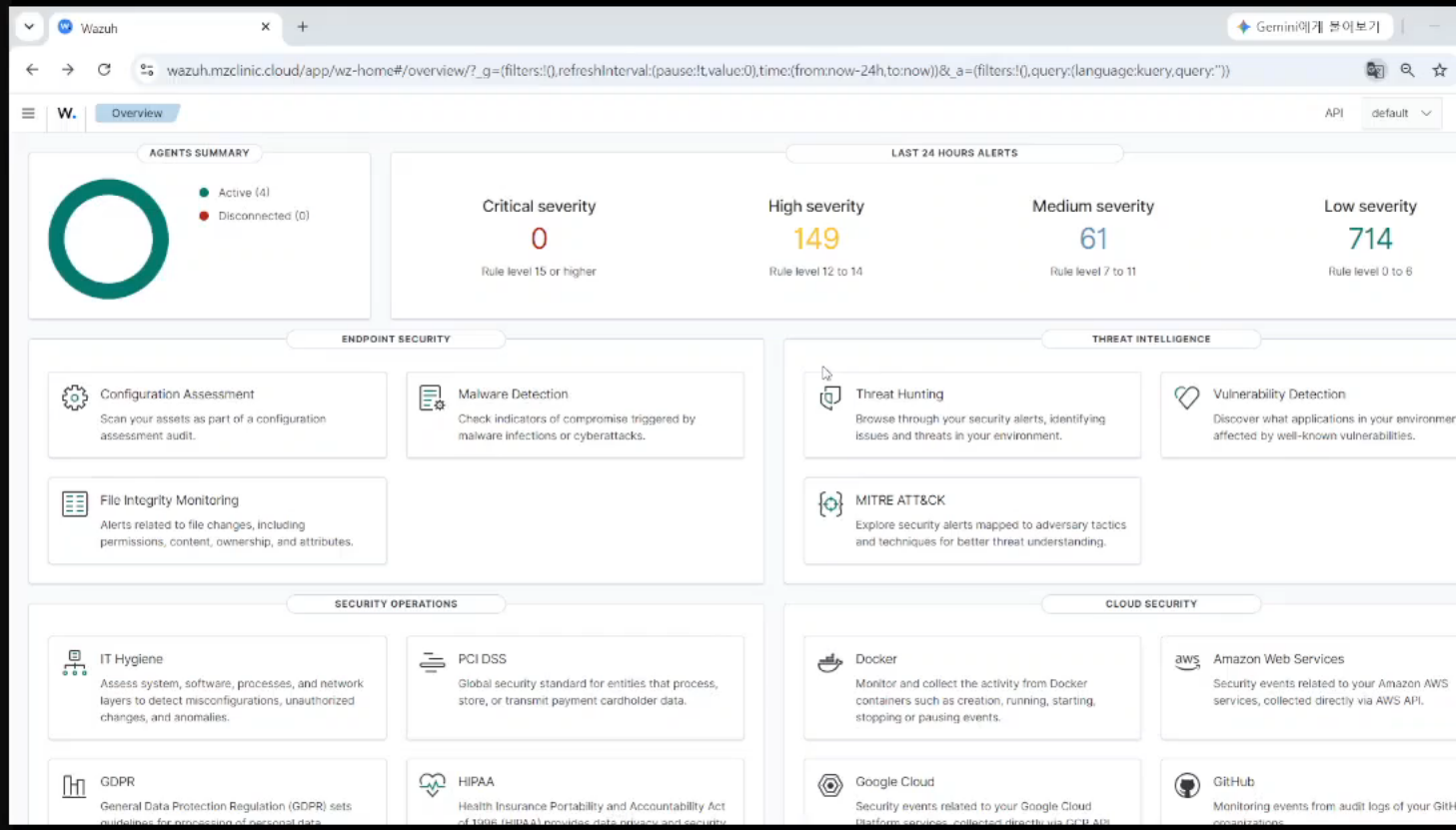
통합관리 대시보드

MSP 운영 관점의 시스템 상태, 보안 백업, DR 현황 등 통합 조회 기능 구현

- ✓ 운영 대시보드 제작 운용
- ✓ 서비스 상태, 보안 이벤트, 장애 통합 조회
- ✓ 통합 로그인으로 한번에 접근


CLOUDFLARE
aws
ALB
Wazuh Manager
Wazuh indexer
Grafana
Wazuh Manager
Wazuh Dashboard
Grafana Alloy
Wazuh Indexer
Grafana Alloy
Prometheus
Nginx
Wazuh agent
Key Cloak
Eventbridge
NGINX
libreswan

```
wins_user@wins:~$ bash demo_log_indexer.sh i-0b4aad8e5f637b07b
=== 장애 상황 발생: 인덱서 인스턴스 종료 ===
```



0.00

매트릭 수집

Alloy + Prometheus + Grafana

왜 Alloy를 선택했나?

Grafana가 만든 오픈소스 메트릭 수집 에이전트

Alloy

✓ Push 방식 에이전트가 직접 전송

✓ WAL 버퍼로 장애 중에도 최대 8시간 메트릭 보존

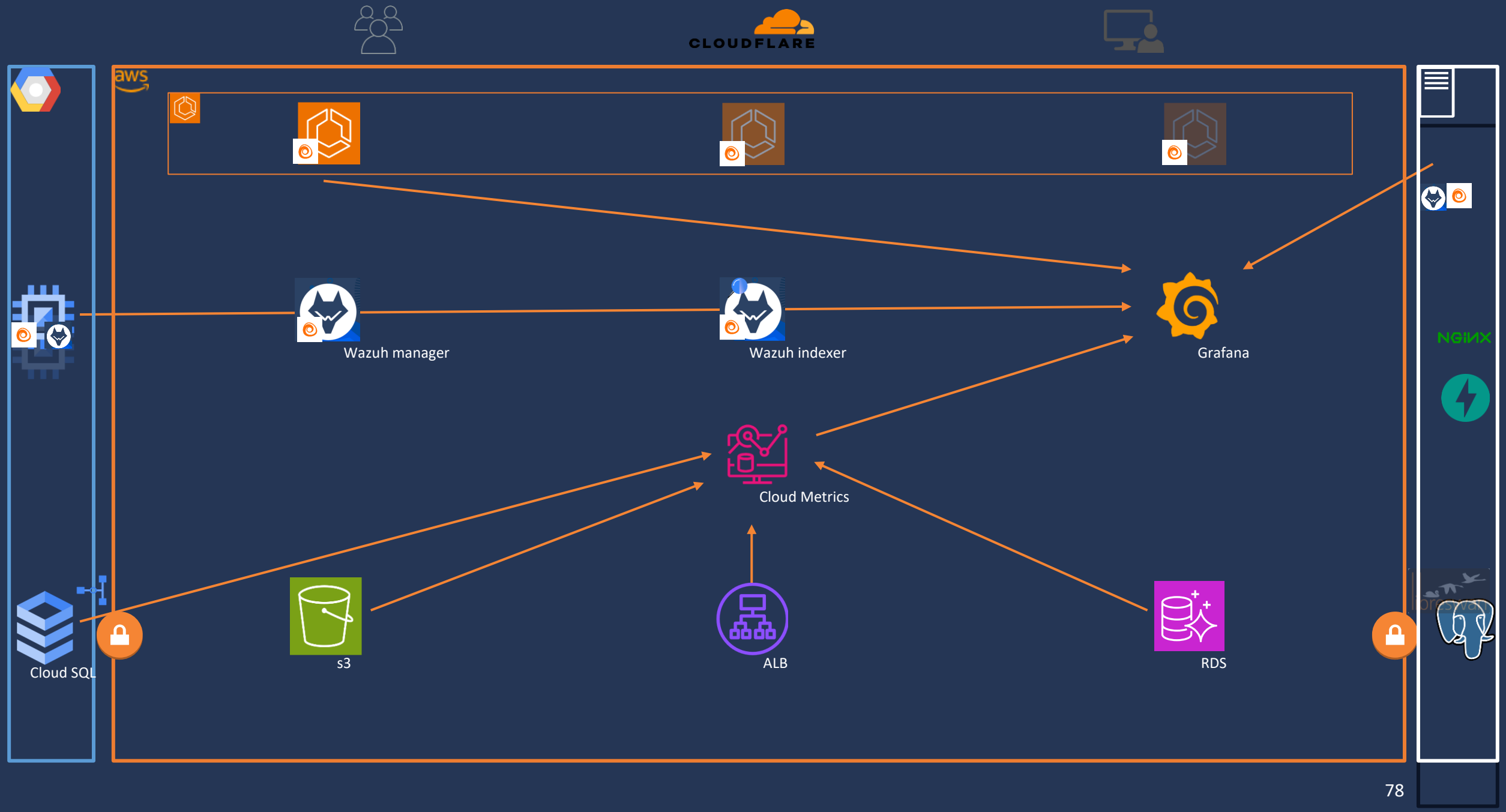
✓ 장애 복구 후 자동 재전송

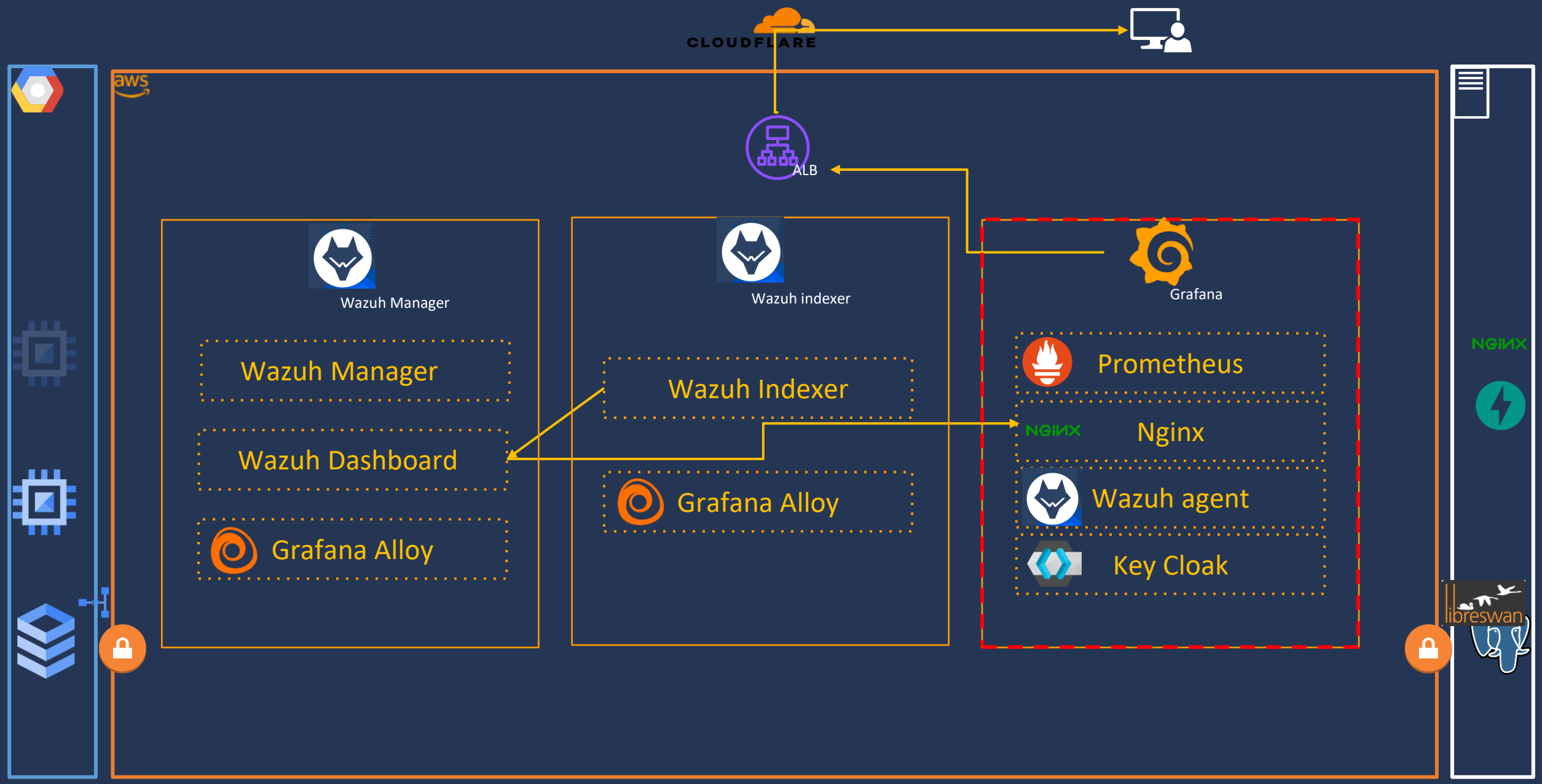
Node Exporter

✓ Pull 방식 Prometheus가 주기적으로 수집

✗ 자체 버퍼 없음

✗ 서버 재생성 중 데이터 유실


CLOUDFLARE
aws
Wazuh manager
Wazuh indexer
Grafana
NGINX
Cloud Metrics
Cloud SQL
s3
ALB
RDS


CLOUDFLARE
aws
ALB
Wazuh Manager
Wazuh Manager
Wazuh Dashboard
Grafana Alloy
Wazuh indexer
Wazuh Indexer
Grafana Alloy
Grafana
Prometheus
Nginx
Wazuh agent
Key Cloak
NGINX
libreswan

mzclinic.cloud
통합 모니터링 대시보드

Keycloak SSO · Grafana / Wazuh / Cost AI

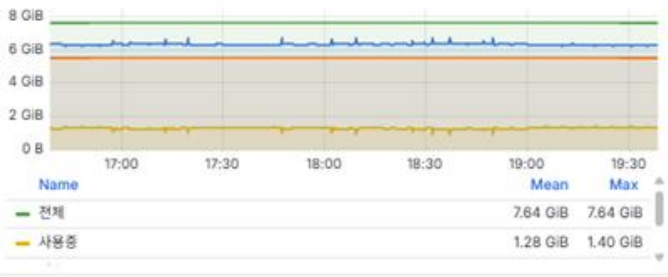
Grafana 새 창

CPU

CPU 사용률 상세

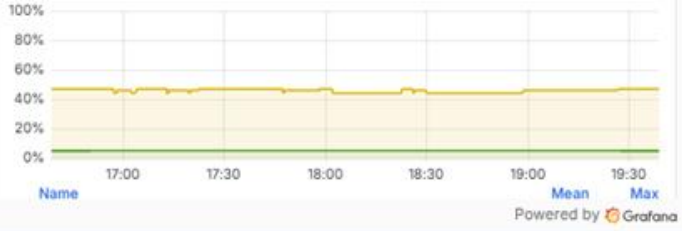
메모리

메모리 사용량



디스크

디스크 사용률



Powered by Grafana

Wazuh 새 창

Overview

AGENTS SUMMARY

Active (4)

Disconnected (0)

LAST 24 HOURS ALERTS

Critical severity

0

Rule level 15 or higher

High severity

0

Rule level 12 to 14

Medium severity

1

Rule level 7 to 11

Low severity

12

Rule level 0 to 6

ENDPOINT SECURITY

Cost AI 새 창

재무 분석 예산 현황 비용 추이 보고서 생성

김이박 클리닉 IT 인프라 비용 분석

AWS · GCP · On-premises

대화 저장 ↓ 연결됨

GCP 비용이 왜 이렇게 올랐어?

오후 07:38

AI

GCP 비용 상승 분석

GCP 비용이 크게 올라진 것처럼 보이지만, **실제로는 안정적인 수준에서 완만한 증가**를 보이고 있습니다. 상황을 정확히 설명하겠습니다.

GCP 비용 추이

월	비용	전월 대비
1월	75,616원	-
2월	78,935원	+4.4%
3월	81,788원	+3.6%
4월	84,813원	+3.7%
5월	87,068원	+2.7%
6월(예상)	165,972원	+90.6%

⚠ 6월 비용이 비정상적으로 높은 이유

6월은 아직 16일만 진행된 상태(2026-06-18 기준)이기 때문입니다.

- **6월 누적(16일)**: 88,518원
- **일평균 소진율**: 5,532원/일
- **월말 예상치(30일 기준)**: 165,972원

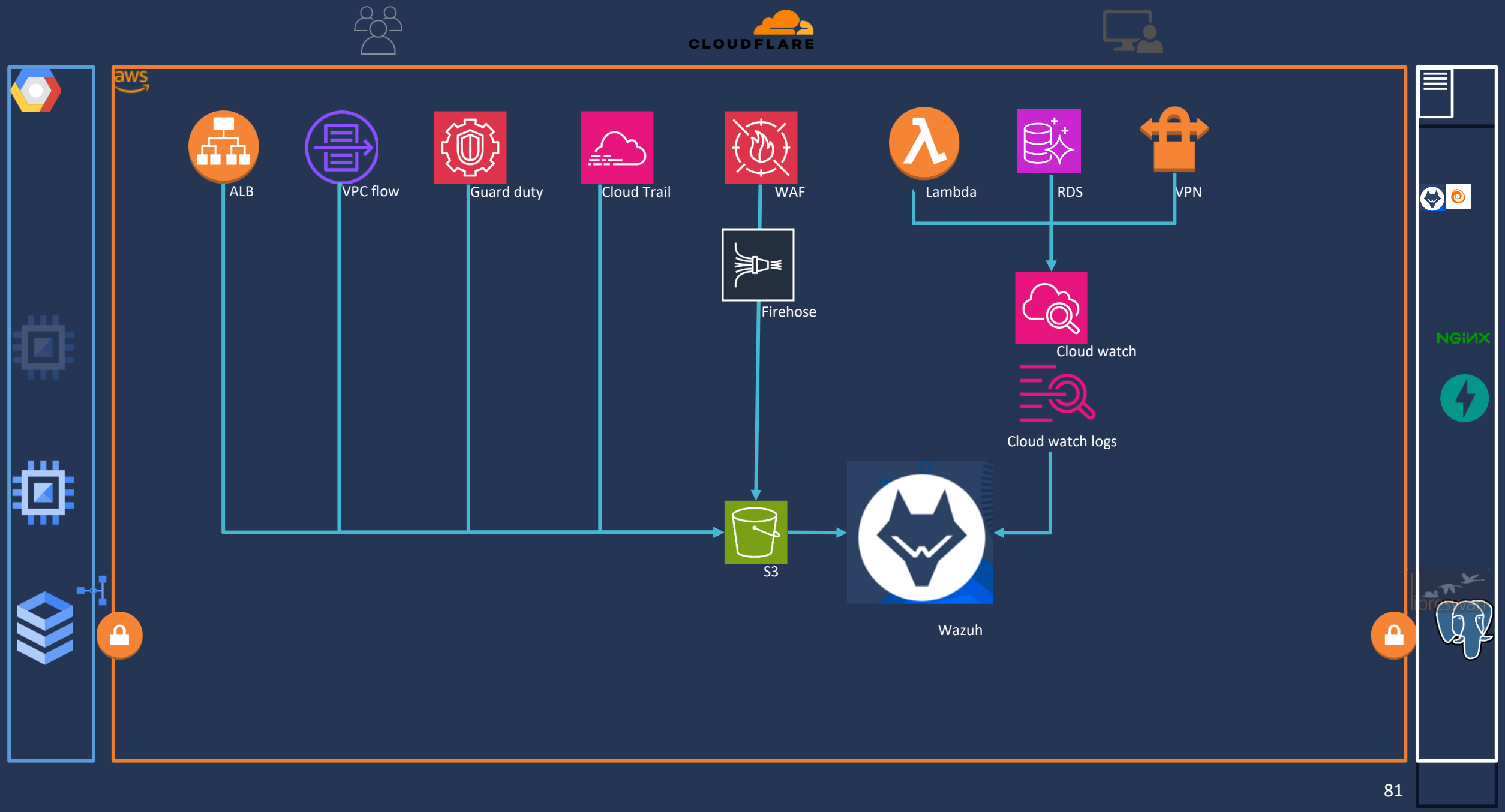
문제점:

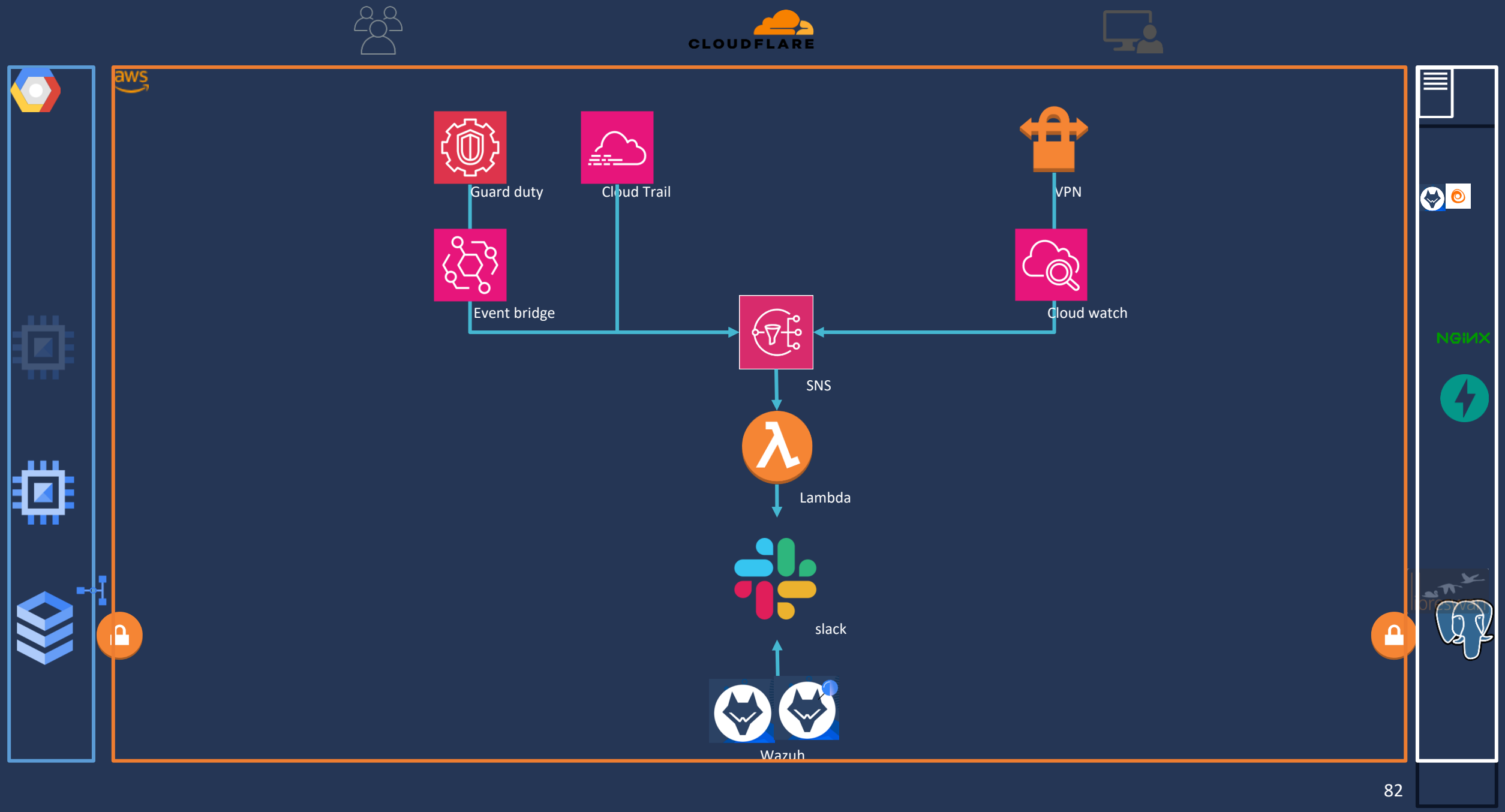
6월 예상치가 실제 5월 비용(87,068원)의 **90.6%까지 올라갈 것**으로 예상되는 것은 **데이터 외삽(extrapolation) 오류**입니다. 실제 5월과 유사한 추세라면 6월 실제 청구액은 **약 89,000~92,000원 수준**일 가능성이 높습니다.

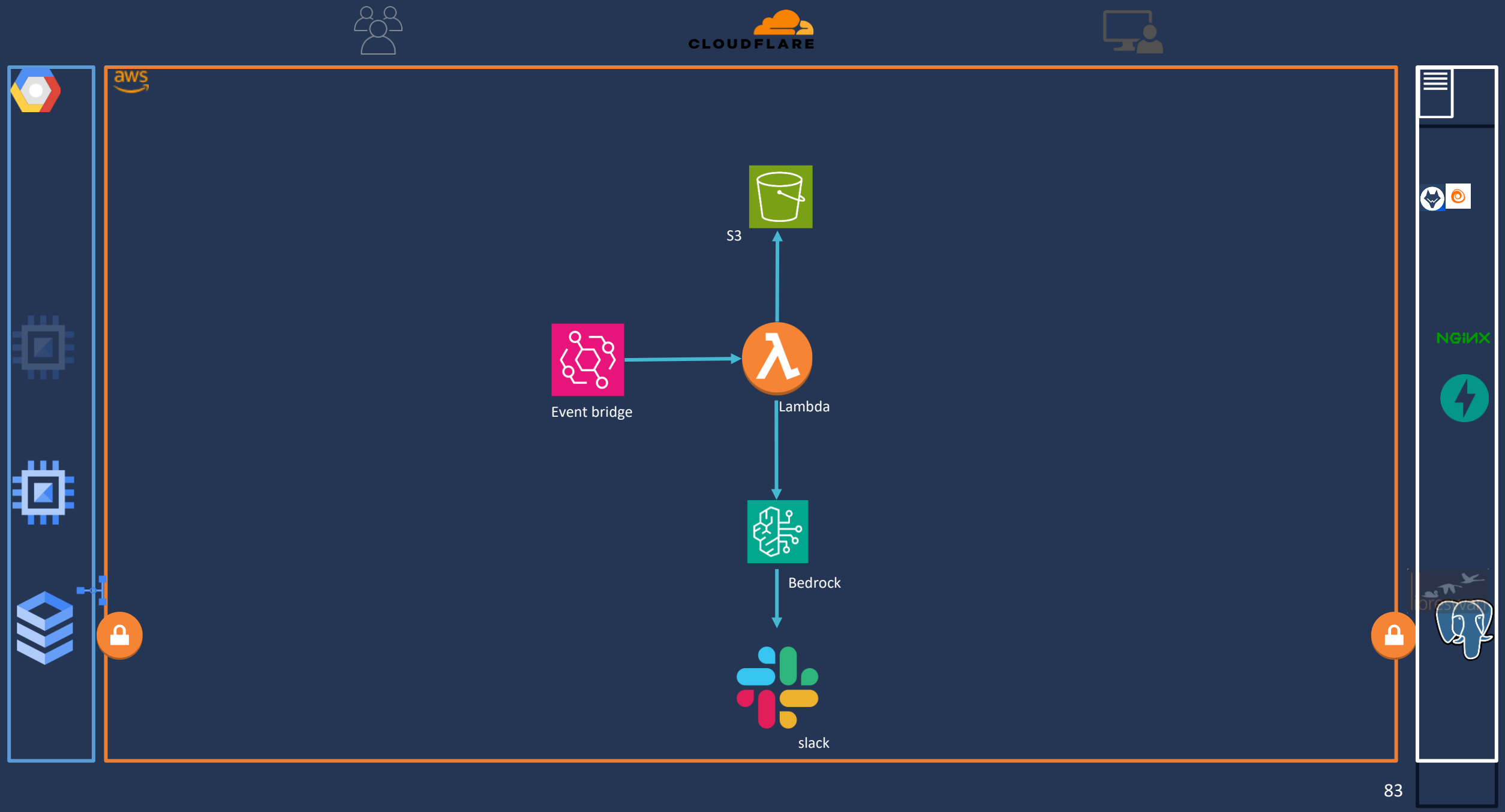
이번 달 전체 비용 GCP 비용 급등 원인 CAPEX / OPEX 예산 집행률 절감 추천

비용 관련 질문을 입력하세요...

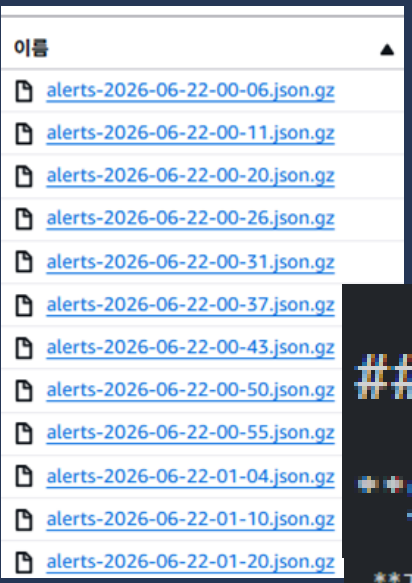
Enter 전송 · Shift+Enter 줄바꿈

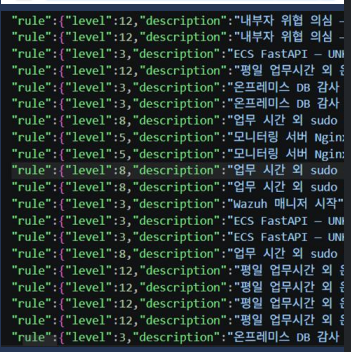

CLOUDFLARE
aws
ALB
VPC flow
Guard duty
Cloud Trail
WAF
Lambda
RDS
VPN
Firehose
Cloud watch
Cloud watch logs
S3
Wazuh
NGINX

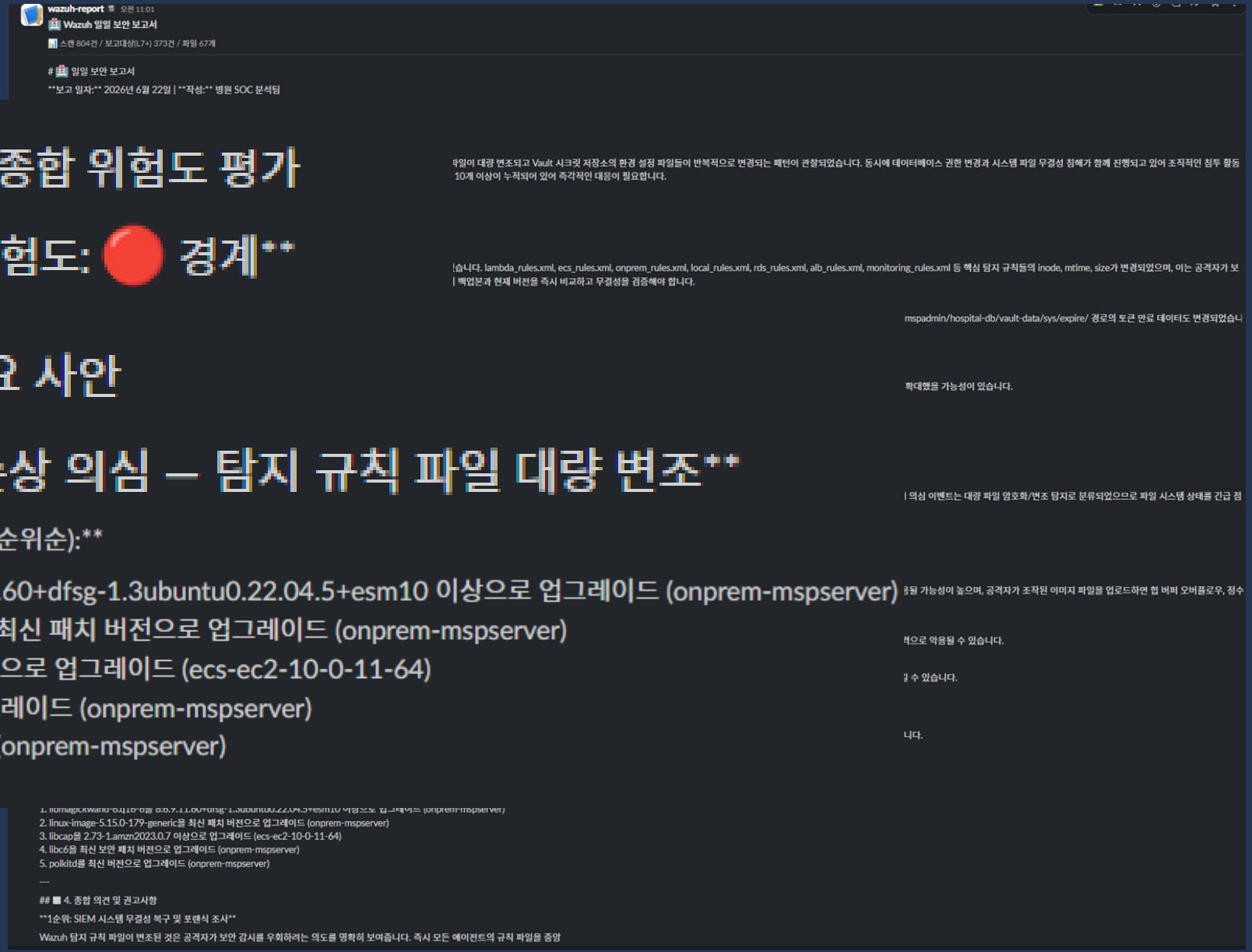

CLOUDFLARE
aws
Guard duty
Cloud Trail
VPN
Event bridge
Cloud watch
SNS
Lambda
slack
Wazuh
NGINX


CLOUDFLARE
aws
S3
Event bridge
Lambda
Bedrock
slack
NGINX

Wazuh 룰 적용 로그


이름
alerts-2026-06-22-00-06.json.gz
alerts-2026-06-22-00-11.json.gz
alerts-2026-06-22-00-20.json.gz
alerts-2026-06-22-00-26.json.gz
alerts-2026-06-22-00-31.json.gz
alerts-2026-06-22-00-37.json.gz
alerts-2026-06-22-00-43.json.gz
alerts-2026-06-22-00-50.json.gz
alerts-2026-06-22-00-55.json.gz
alerts-2026-06-22-01-04.json.gz
alerts-2026-06-22-01-10.json.gz
alerts-2026-06-22-01-20.json.gz


"rule":{"level":12,"description":"내부자 위협 의심 –
"rule":{"level":12,"description":"내부자 위협 의심 –
"rule":{"level":3,"description":"ECS FastAPI – UNI
"rule":{"level":12,"description":"평일 업무시간 외
"rule":{"level":3,"description":"온프레미스 DB 감사
"rule":{"level":3,"description":"온프레미스 DB 감사
"rule":{"level":8,"description":"업무 시간 외 sudo
"rule":{"level":5,"description":"모니터링 서버 Ngin
"rule":{"level":5,"description":"모니터링 서버 Ngin
"rule":{"level":8,"description":"업무 시간 외 sudo
"rule":{"level":8,"description":"업무 시간 외 sudo
"rule":{"level":3,"description":"Wazuh 매니저 시작"
"rule":{"level":3,"description":"ECS FastAPI – UNI
"rule":{"level":3,"description":"ECS FastAPI – UNI
"rule":{"level":8,"description":"업무 시간 외 sudo
"rule":{"level":12,"description":"평일 업무시간 외
"rule":{"level":12,"description":"평일 업무시간 외
"rule":{"level":12,"description":"평일 업무시간 외
"rule":{"level":12,"description":"평일 업무시간 외
"rule":{"level":3,"description":"온프레미스 DB 감사


wazuh-report 오전 11:01
Wazuh 일일 보안 보고서
스캔 804건 / 보고대상(L7+) 373건 / 파일 67개
일일 보안 보고서
보고 일자: 2026년 6월 22일 | **작성:** 병원 SOC 분석팀
1. 종합 위험도 평가
현재 위험도: 경계
즉시 조치 필요 사안
SIEM 시스템 자체 손상 의심 – 탐지 규칙 파일 대량 변조
지금 바로 적용해야 할 업데이트 (우선순위순):
1. libmagickwand-6.q16-6을 8:6.9.11.60+dfsg-1.3ubuntu0.22.04.5+esm10 이상으로 업그레이드 (onprem-mspserver)
2. linux-image-5.15.0-179-generic을 최신 패치 버전으로 업그레이드 (onprem-mspserver)
3. libcap을 2.73-1.amzn2023.0.7 이상으로 업그레이드 (ecs-ec2-10-0-11-64)
4. libc6을 최신 보안 패치 버전으로 업그레이드 (onprem-mspserver)
5. polkitd를 최신 버전으로 업그레이드 (onprem-mspserver)
---
4. 종합 의견 및 권고사항
1순위: SIEM 시스템 무결성 복구 및 포렌식 조사
Wazuh 탐지 규칙 파일이 변조된 것은 공격자가 보안 감시를 우회하려는 의도를 명확히 보여줍니다. 즉시 모든 에이전트의 규칙 파일을 중앙
mspadmin/hospital-db/vault-data/sys/expire/ 경로의 토큰 만료 데이터도 변경되었습니
확대했을 가능성이 있습니다.
| 의심 이벤트는 대량 파일 암호화/변조 탐지로 분류되었으므로 파일 시스템 상태를 긴급 점
용될 가능성이 높으며, 공격자가 조작된 이미지 파일을 업로드하면 힙 버퍼 오버플로우, 정수
적으로 악용될 수 있습니다.
할 수 있습니다.
니다.

마무리

인프라 총 비용

AWS + GCP + 온프레미스 = 약 월 2,000,000 (연 24,000,000)

AWS 클라우드

월 약 1,600,000

GCP 클라우드

월 약 200,000

온프레미스 비용

월 200,000

(서버 감가상각, 전기료, 네트워크 회선)

비용 절감

환경	항목	AS-IS	TO-BE	절감율
GCP	GCP DR VM	AWS 장애 발생 할 때까지 상시 대기	평상시 0 대 유지	5.29%
GCP	AWS-GCP VPN 연결	GCP HA VPN (고정 시간당 요금)	Classic VPN + HAProxy를 올린 CE 1대	43.8%
AWS	ALB 통합	patient-alb(환자), staff-alb(의료진) 분리	hospital-alb 단일 ALB로 통합	1.6%
AWS	ECS EC2 다운사이징	t3.large	t3.medium	2.6%
AWS	ECS Warmpool	EC2 상시 대기 (중단된 상태로 EBS 비용 발생)	프로그램 설치된 Custum AMI 사용	0.15%
AWS	S3 스토리지 계층 전환	S3 기본 계층 사용	시스템 로그, RDS 덤프, Terraform 소스 코드 등을 액세스 빈도에 따라 Glacier Archive 또는 Glacier 계층으로 전환	0.2%

비용 절감

환경	항목	AS-IS	TO-BE	절감율
GCP	GCP DR VM	AWS 장애 발생 할 때까지 상시 대기	평상시 0 대 유지	5.29%
GCP	AWS-GCP VPN 연결	GCP HA VPN (고정 시간당 요금)	Classic VPN + HAProxy를 올린 CE 1대	43.8%
AWS	ALB 통합	patient-alb(환자), staff-alb(의료진) 분리	hospital-alb 단일 ALB로 통합	1.6%
AWS	ECS EC2 다운사이징	t3.large	t3.medium	2.6%
AWS	ECS Warmpool	EC2 상시 대기 (중단된 상태로 EBS 비용 발생)	프로그램 설치된 Custum AMI 사용	0.15%
AWS	S3 스토리지 계층 전환	S3 기본 계층 사용	시스템 로그, RDS 덤프, Terraform 소스 코드 등을 액세스 빈도에 따라 Glacier Archive 또는 Glacier 계층으로 전환	0.2%

QnA