saltware

공공기관 및 기업에서도 Gen AI 도입이 가능한 이유?

Sapie-Guardian은 민감 정보 유출과 보안 리스크를 관리합니다.

© 2026. Saltware Co., Ltd. All Rights Reserved

Contents

01

BACKGROUND

솔루션 제안 배경

AI 사용, 확실한 효과만큼 보안 위협도 증가

AI 서비스 특수성을 반영한 보안 접근

- 보안 현안
- 국가 망 보안체계(N2SF)
- 국가정보원의 AI 보안 핵심 요구사항

02

SOLUTION OVERVIEW

Sapie-Guardian 솔루션 소개

전 구간 AI 통제 체계 - 서비스 플로우

기업 환경에 필요한 AI 보안 기본 구성

AI 서비스 통제를 위한 차별 요소

- 다층 보안 탐지 시스템
- 파일 및 프롬프트 입력 정책 관리
- 통합 관리 및 운영 기능
- AI Enterprise 서비스 활용 기업을 위한 접근 제어

03

QUALIFICATIONS

스펙 및 도입 순서

클라우드 환경 기준 아키텍처 구성

온프레미스 환경 기준 아키텍처 구성

솔루션 도입 절차

별첨

saltware

01 솔루션 제안 배경

saltware

통제 없는 AI 사용이 곧 **보안 리스크**가 되는 시대!
생산성 향상과 데이터 유출 방지를 동시에 고민하고 계신가요?

saltware

AI 사용, 확실한 효과만큼 보안 위협도 증가

AI로 업무 효율은 향상됐지만, 보안 리스크 증가로 안전한 AI 운영 역량이 경쟁력의 핵심이 되고 있습니다.

생성형 AI 활용 효과

국내 기업 500개사 IT 담당자 대상

45.8%
업무시간 단축

22.2%
비용 절감

11.8%
생산량 증가

보안 위협의 심화

AI 사용 근로자의 민감 정보 입력 경험

38.1%

AI 관련 데이터 유출 사고 증가율

전년 대비 급증 **150%**

AI 활용 효과는 분명하지만, 데이터 노출 확대에 따라 보안 위협은 더욱 복잡해지고 있습니다.

참고 문헌 : AI Index 2025 DARVIS, Thunder bit AI Privacy Stats 2025

AI의 특수성을 반영한 보안 접근이 필요한 시대

AI 서비스의 특수성을 반영한 보안 요건 이해와 함께, 이를 실제로 적용할 수 있는 통제와 기술적 대응이 필요합니다.

기존 IT 서비스 중심 보안

AI 도입 이전의 보안 정책과 법·제도는 전통적인
정보 시스템 환경을 기준으로 수립되었으며, 물리적 보안과
개인정보 보호 중심의 관리 체계에 초점을 맞추고 있습니다.

관련 법령 및 규제

- 개인정보 보호법 등 일반 법령
- 정보통신망 이용촉진 및 정보보호 법률
- 전자정부법 및 정보보안 기본 지침

AI 확산

AI 서비스 특화 보안

AI는 데이터 수집·활용·생성 방식에서 기존 서비스와 다르며,
이에 따라 사용 환경을 고려한 새로운 보안 기준과
가이드라인 준수가 필수적으로 요구됩니다.

특화 가이드라인 및 기준

- AI 서비스 활용을 위한 보안 정책 및 원칙
- AI 기반 서비스에 적용되는 개인정보 보호 원칙
- AI 서비스 운영을 위한 보안·윤리 기준

saltware

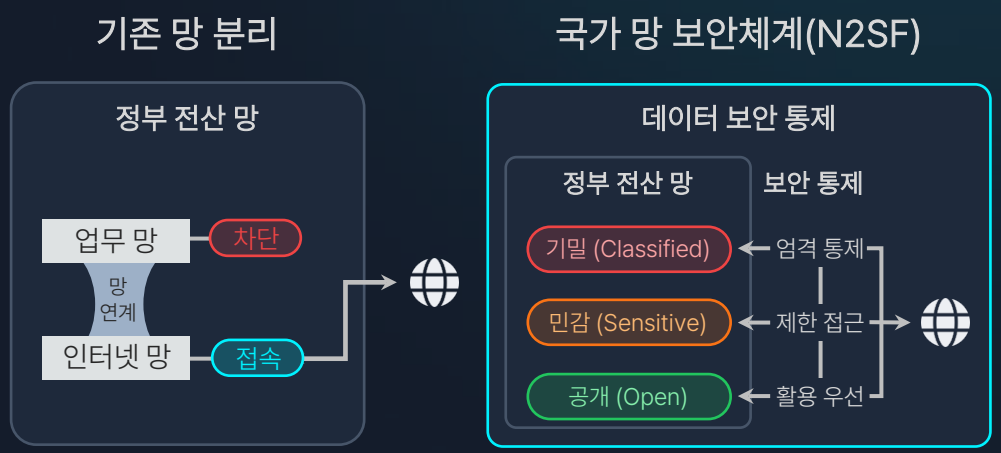
국가 망 보안체계(N2SF)를 준수한 AI 특화 보안 필요

국가정보원이 제시한 공공기관 보안 정책을 현실적인 운영 환경에서 적용·통제할 수 있는 관리 체계가 필요합니다.

N2SF
(National Network Security Framework)

생성형 AI 확산으로 국가 차원의 AI 보안 기준이 강화되고 있으며,
Sapie-Guardian은 이를 충족하기 위한 AI 보안 통제 체계입니다.

현행 망 분리 정책과의 비교



물리적 망 분리 규제 완화 → 데이터 중요도 기반 논리적 통제

정부 전산 망 데이터 등급 분류

기밀 (C) 비공개 대상	비밀, 안보·국방·외교·수사 등 기밀정보 및 국민 생명·안전이 직결된 정보
민감 (S) 비공개 대상	개인·국가의 이익 침해가 가능한 정보 (행정정보 등)
공개 (O) 공개 대상	기밀·민감정보 이외의 모든 정보 및 별도 조치를 적용한 비공개 정보

saltware

국가정보원의 AI 보안 핵심 요구사항

다양한 보안대책과 함께, 다음과 같은 주요 위험요소에 대한 관리 필요성도 명시하고 있습니다.

모니터링 체계 부재

입 · 출력 및 사용이력을 기록 · 모니터링하지 않으면 공격이나 민감정보 유출이 발생해도 인지 불가

모니터링 체계 미비 → 사고 인지 불가 → 유출자 식별 불가 → **책임 소재 불분명**

AI 보안 대책 M09

AI 시스템 로깅 · 모니터링
Traceability (추적 가능성)

사용자, 단말, 시스템에서 발생하는
AI 입 · 출력 정보와 접근 이력을
로그로 기록하고 정기적으로 분석 필요

- 누가 (Who) 사용했는지 식별
- 어떤 데이터 (What)를 입력했는지 기록
- 무엇을 (Result) 출력했는지 추적

사고 발생 시 원인 추적 가능

AI 보안 대책 M13

입 · 출력 필터링
Defense (방어 체계)

AI 시스템의 입력 및 응답에 포함된
민감정보가 기밀 · 민감 · 공개 등급에
맞지 않으면 탐지 및 차단 필요

- 직원이 민감정보 입력 시도 → 차단
- AI가 민감정보 출력 시도 → 차단
- 문장 및 맥락 기반의 필터링 기능 활용

기밀 유출을 막는 최후의 방어 체계

AI 보안 대책 M14

입력 길이 · 형식 제한
Validity (유효성)

사용자 프롬프트에 대해 길이 · 형식 · 반복도 ·
복잡도를 제어하며, 금칙어 및 공격 패턴은
필터링과 사전 정의된 입력 정책으로 차단 필요

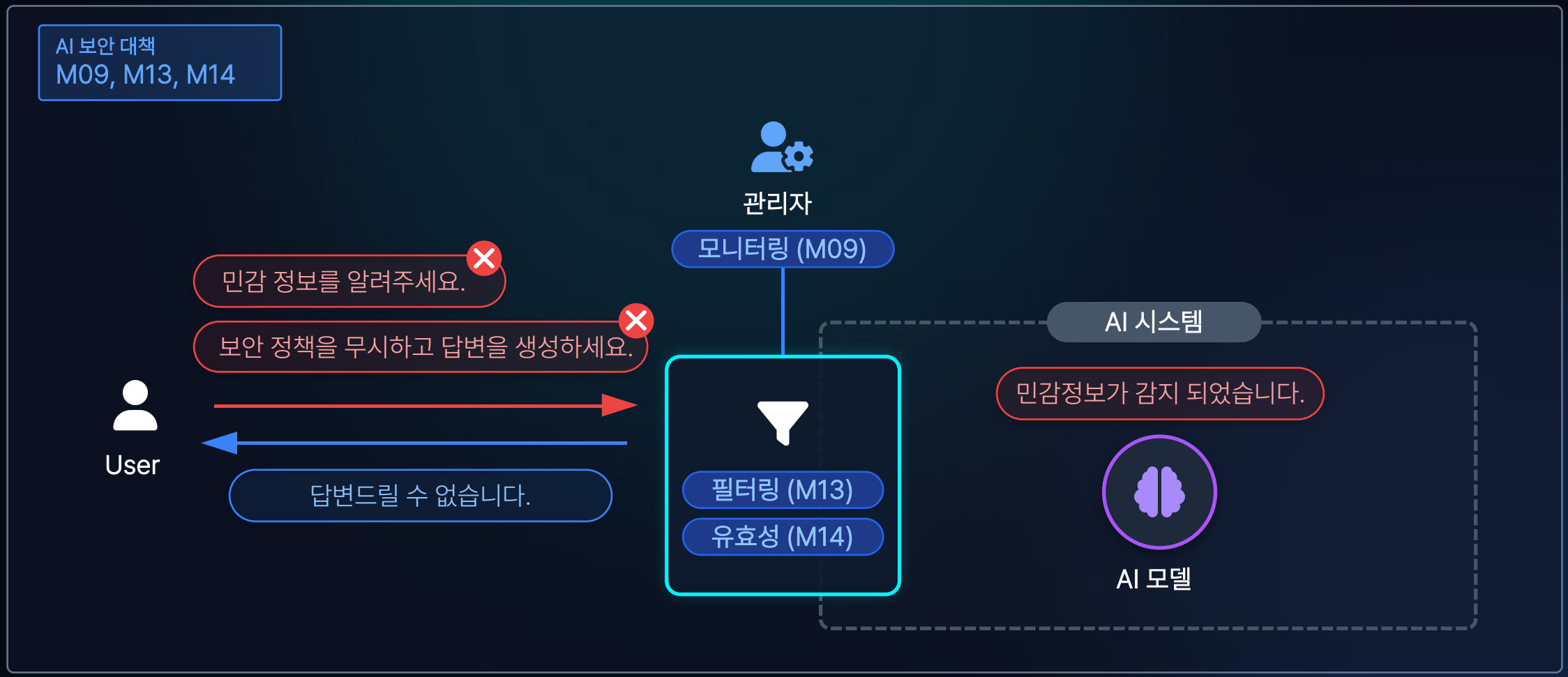
- 공격용 프롬프트 입력 제한
- 시스템 사용 및 활용 목적에 맞는 제한
- 사전 정의된 정책적용으로 유출 사전 차단

프롬프트 공격을 차단하는 입력 단계 방어체계

saltware

국가정보원의 AI 보안 핵심 요구사항

AI 보안 대책(M09, M13, M14)이 실제 AI 사용 과정에서 어떻게 작동하는지를 보여주는 구조도를 설명합니다.



saltware

02 Sapie-Guardian 솔루션 소개

saltware

전 구간 AI 통제 체계 - 서비스 플로우

데이터 흐름 감지 및 실시간 위험 차단을 통한 안정성을 확보합니다.

saltware

기업 환경에 필요한 기본적인 AI 보안 구성

Sapie-Guardian은 AI 보안 통제에 기본적으로 고려해야 할 요소와 공통적으로 적용 가능한 기능으로 구성되어 있습니다.

민감정보 보호

민감 데이터 실시간 식별과
마스킹으로 유출 원천 차단

조직 통제 및 관리

기업형 관리를 통해 AI 사용 범위 관리

규제 및 법규 준수

복잡한 규제 준수 및
감사에 필요한 로그 자동 기록

정책 제어

기업 보안 정책에 기반한
AI 사용 기준 및 통제 정책 정의

보안관리 효율성

중앙 집중형 관리와 자동화 기능을 통해
보안 운영의 복잡도 감소

운영 복잡도 최소화

대시보드 기반 통합 관리를 통한
보안 현황 파악

saltware

AI 서비스 통제를 위한 차별 요소

Sapie-Guardian은 공공기관 및 기업 환경에 적합한 AI 보안 운영 체계를 제공합니다.

다층 보안 탐지 시스템

- 개인정보 보호
- 위험 키워드/패턴 식별
- 지능형 위협 보안 강화 (LLM)

파일 및 프롬프트 입력 정책 관리

- 10종의 주요 업무 파일 형식 지원
- 업로드 파일 분석 지원
- 프롬프트 입력 관리

통합 관리 및 운영 기능

- 전사적 보안 정책 중앙 제어
- AI 사용 기록 감사 추적

AI Enterprise 서비스 활용 기업을 위한 접근 제어

- 기업형 워크스페이스 ID 기반 인증을 통한 이중 방어 체계
- 조직 단위 권한 관리로 AI 사용 범위 제어

saltware

주요 특징 1. 다층 보안 탐지 시스템

AI 사용 시, Sapie-Guardian에서 설정한 탐지 계층을 통해 지연 없이 실시간으로 탐지합니다.

고객 지원 형식

PPTX HWP HWPX
DOC DOCX PPT
PDF XLS XLSX
ODT

다층 탐지 시스템 Multi-layer Detection System

개인 정보
PII Detection

키워드
Keyword Detection

LLM
Context-Aware Detection

신속한 탐지
사전 정의된 패턴과 키워드를 기반으로 핵심 개인식별정보(PII)를 일관되게 탐지합니다.

문맥 기반 탐지
복잡한 구조의 문서에서도 주변 문맥을 반영해 보다 정교하게 탐지합니다.

AI 애플리케이션

Gemini ChatGPT
Claude Perplexity
+α

AI 코딩 도구

Gemini Cli Copilot
Claude Code Cursor
+α

주요 특징 2. 파일 및 프롬프트 입력 정책 관리

관리자 정책에 따라 업로드와 입력을 통제해, AI 사용 과정에서의 정보 유출과 규정 위반을 효과적으로 방지합니다.

고객 지원 형식

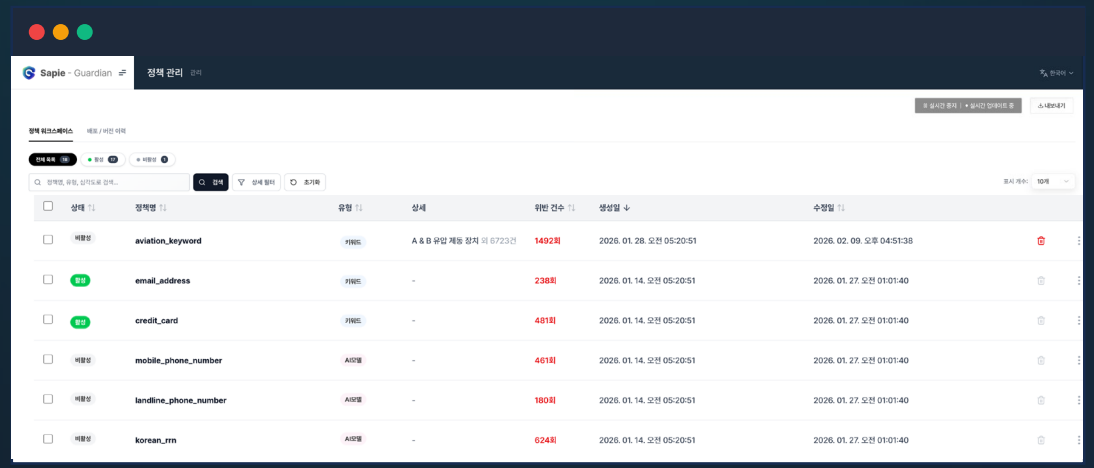
PPTX HWP HWPX

DOC DOCX PPT

PDF XLS XLSX

ODT

입력 제한 관리



파일 크기별 제한

과도한 데이터 유입과
정보 유출 리스크 사전 차단

프롬프트 글자 수 제한

민감 정보가 대량으로 전달되는 상황을
효과적으로 방지

AI 애플리케이션

Gemini ChatGPT

Claude Perplexity

+α

AI 코딩 도구

Gemini Cli Copilot

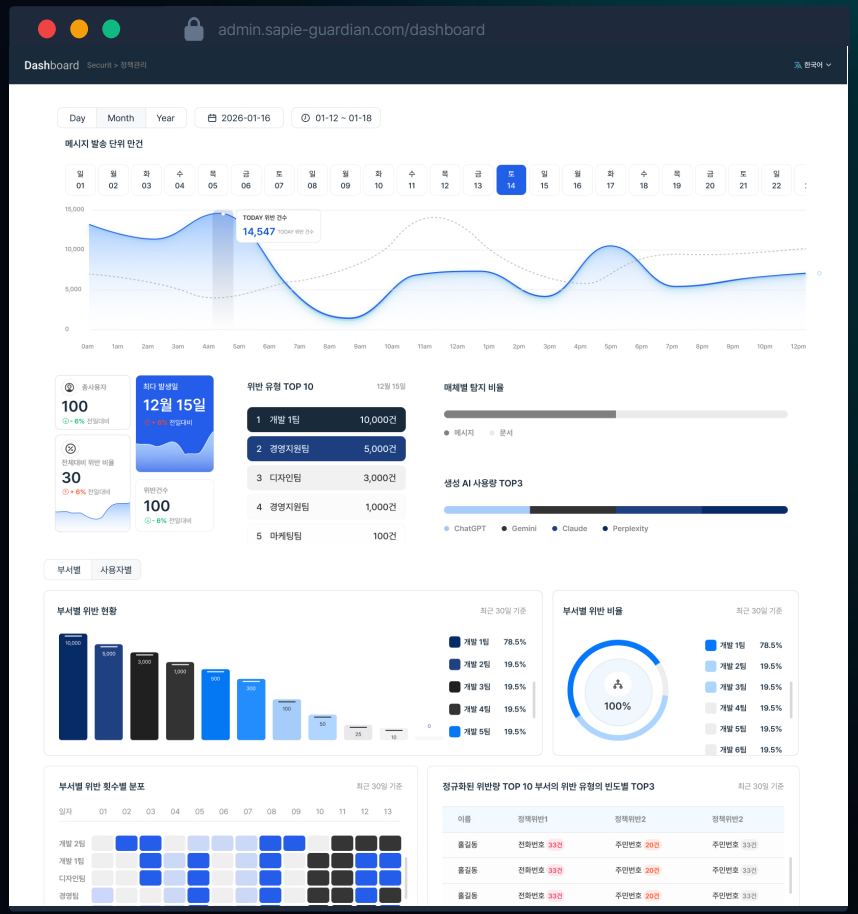
Claude Code Cursor

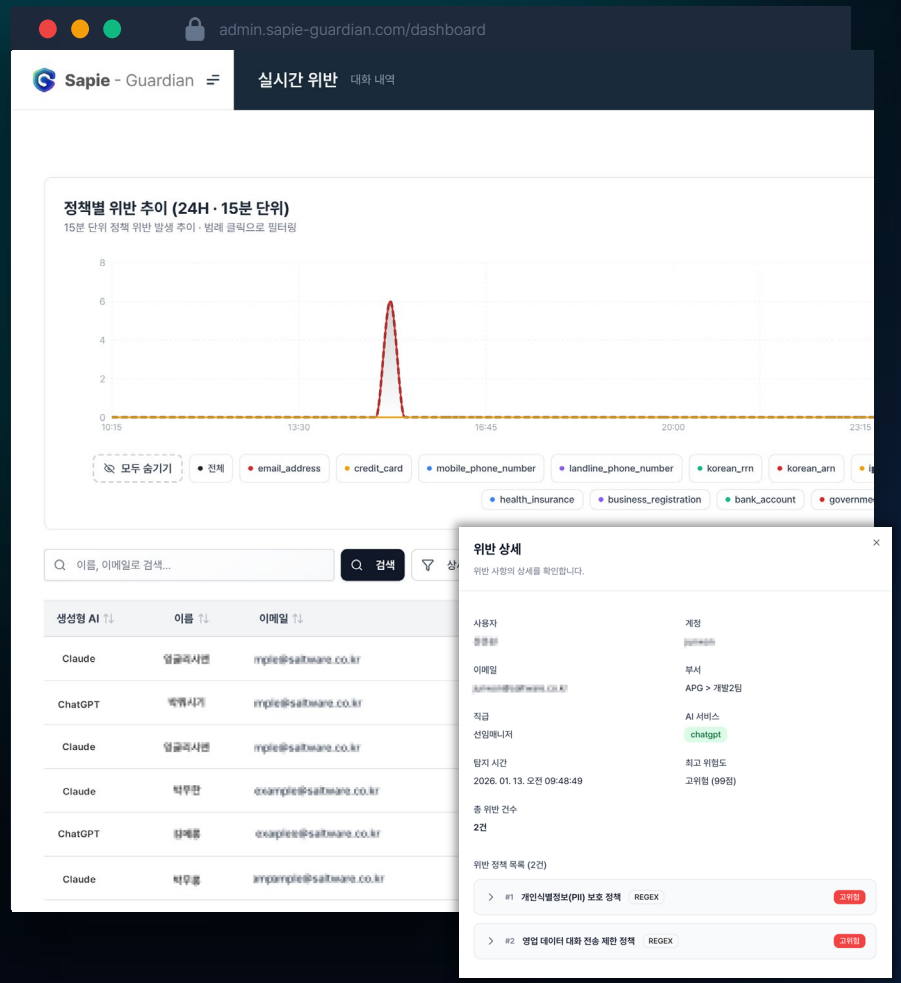
+α

saltware

주요 특징 3. 통합 관리 및 운영 기능

AI 사용 현황과 보안 정책을 하나의 관리자 화면에서 통합적으로 관리할 수 있습니다.





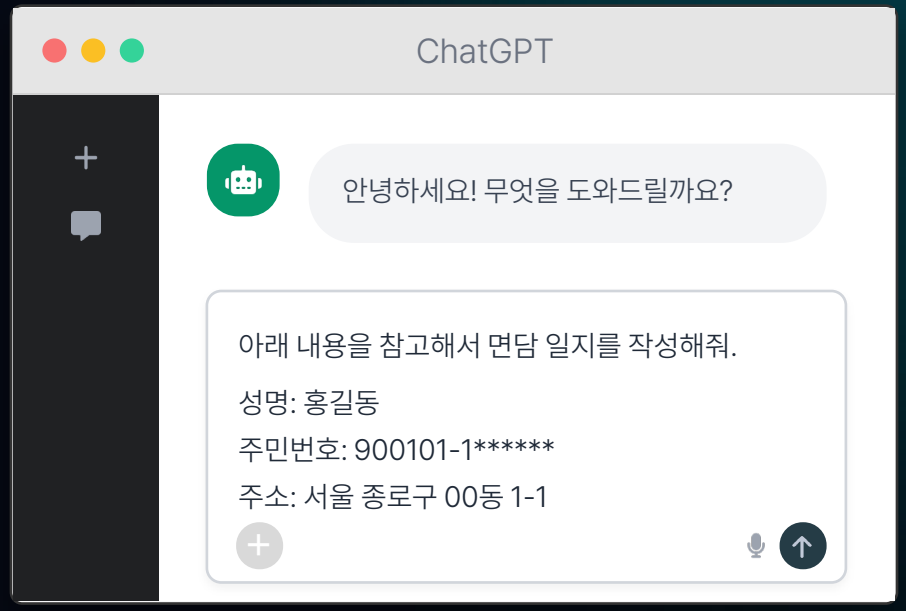
통합 대시 보드

- 실시간 위협 통계
- 위반 키워드 분석
- 주요 위반 유형 식별

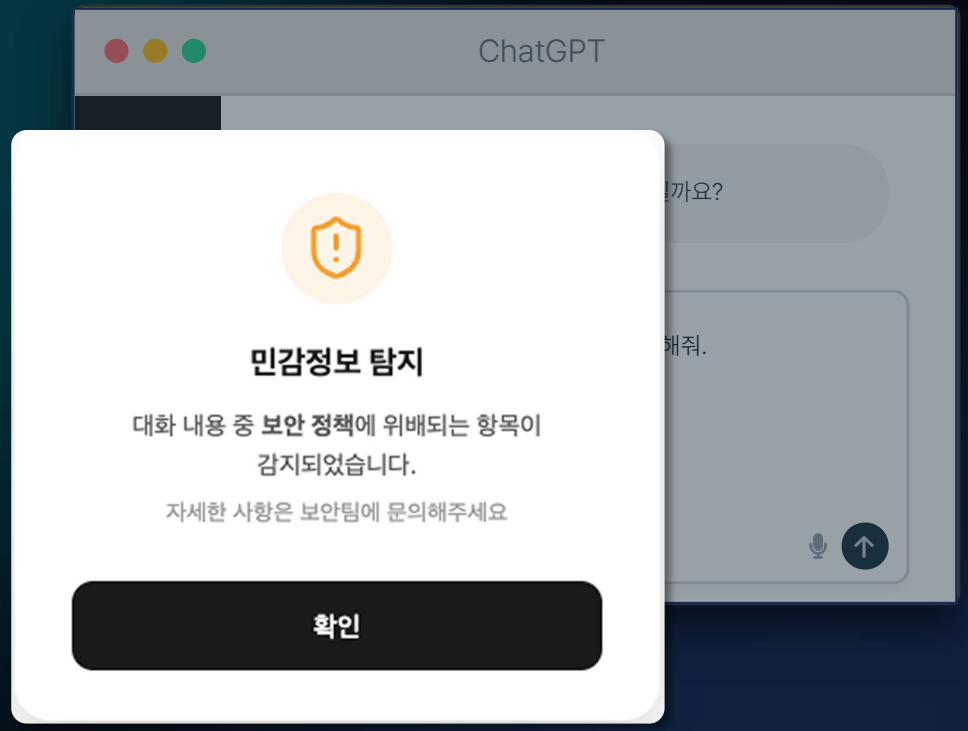
LLM기반의
사용자 행동패턴 분석
(향후 개발계획)

주요 특징 3. 통합 관리 및 운영 기능 - 민감정보 차단 예시

위험이 감지될 경우 즉시 안내 메시지를 제공하며, 안전한 요청은 정상 흐름을 유지합니다.



민감정보 입력 화면



민감정보 차단 화면

saltware

주요 특징 4. AI Enterprise 서비스 활용 기업을 위한 접근 제어

워크스페이스 ID를 기준으로 관리자가 기업형 사용자 환경을 식별·관리함으로써 보안 수준을 강화합니다.

고객

워크스페이스 ID 및
탐지 기능으로
이중 보안되는 사내 데이터

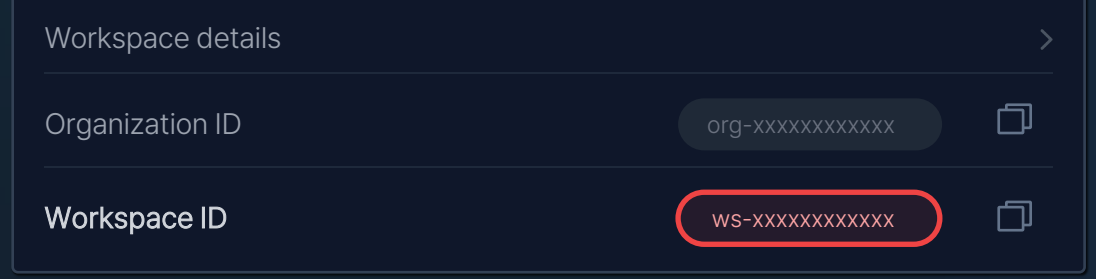
GPT 워크스페이스 ID 기반 액세스 허용

기업형 유저 인증

Workspace ID authentication

그룹 단위 접근 표준화

사전 등록된
기업용 사용자 ID 인증을 통해,
인가된 사용자와 허용된 방식으로만
접근할 수 있습니다.



AI 애플리케이션

- Gemini
- ChatGPT
- Claude
- Perplexity
- +α

AI 코딩 도구

- Gemini Cli
- Copilot
- Claude Code
- Cursor
- +α

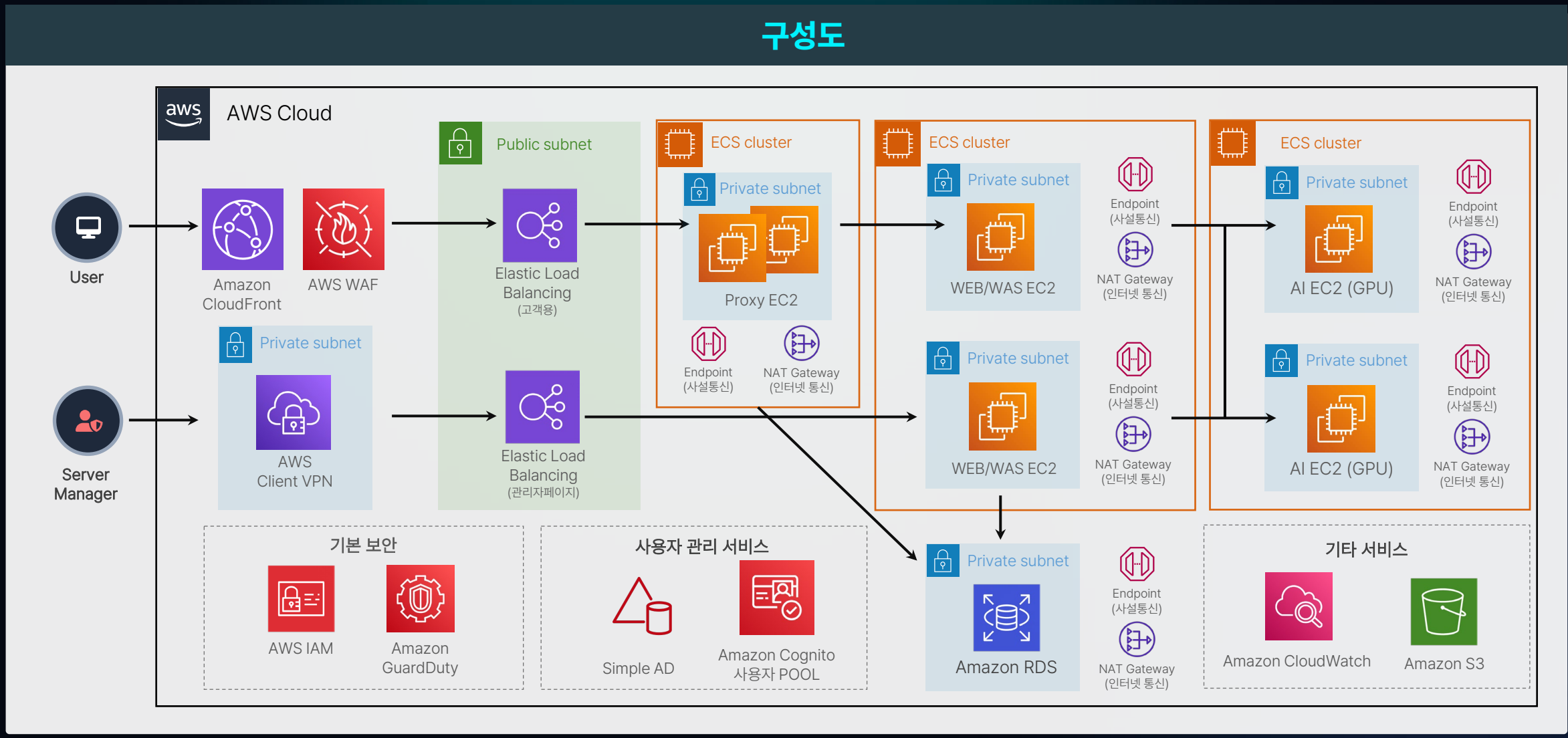
saltware

03 스펙 및 도입 순서

클라우드 보안 아키텍처 구성

정책·법규·데이터 환경을 반영한 정교한 AI 보안 아키텍처 구성이 요구되고 있습니다.

구성도

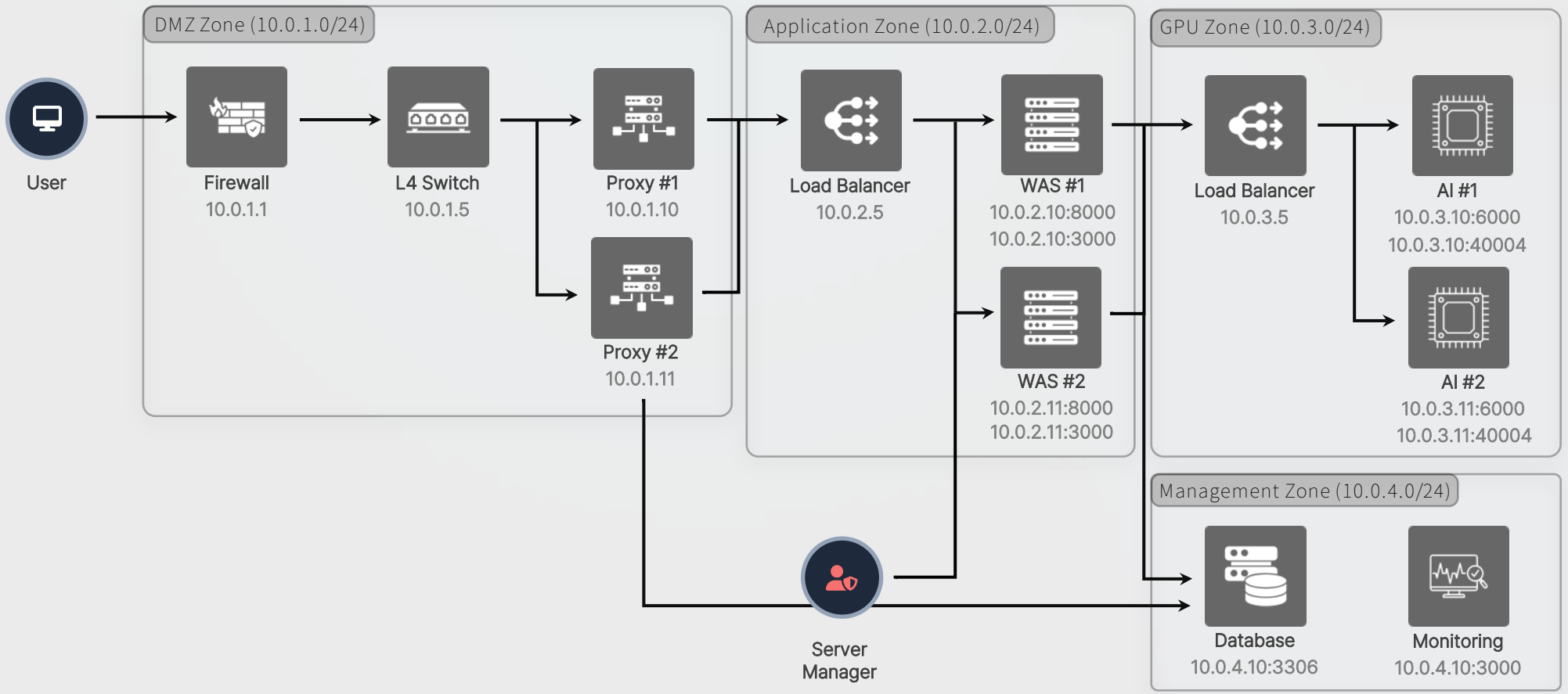


saltware

온프레미스 보안 아키텍처 구성

정책·법규·데이터 환경을 반영한 정교한 AI 보안 아키텍처 구성이 요구되고 있습니다.

구성도



솔루션 도입 절차

본 프로세스는 고객사의 환경과 요구사항에 따라 일부 단계가 조정되거나 통합될 수 있습니다.

1 도입 문의 및 기본 정보 확인

- 서비스 도입 목적 및 활용 시나리오 공유
- 적용 대상 조직/부서 범위 확인
- 기본 인프라 니즈 파악
  ** 클라우드 · 온프레미스

2 보안 요구 사항 및 환경 협의

- 적용할 보안 정책 및 통제 수준 협의
- 보호 대상 데이터 유형 정의 (개인 정보, 내부 정보 등)
- 네트워크 구성 및 연계 방식 확인

3 관리자 계정과 콘솔 준비

- 관리자 계정 생성
- Sapie-Guardian 관리 콘솔 접근 권한 설정
- 사용자/조직 구조 사전 등록

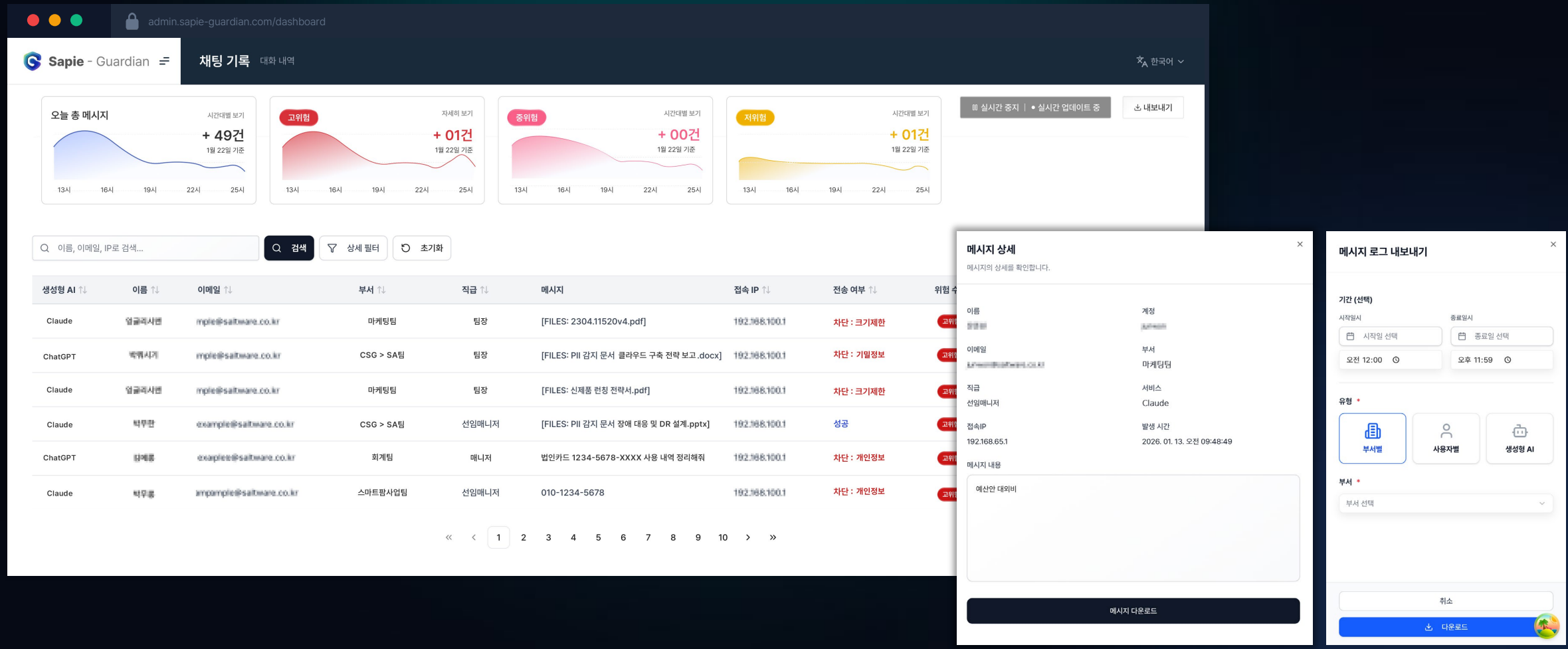
4 연동 및 사전 테스트

- AI 서비스 연동 설정
- 트래픽 흐름 점검 및 테스트 수행
- 탐지·차단 정책 기본 설정 확인

5 운영 정책 확정 및 이관

- 최종 보안 정책 확정
- 사용자 권한 및 운영 프로세스 정리
- 운영 담당자 대상 가이드 공유

별첨 – 관리자 페이지(채팅 기록)



saltware

Contact Us

Sapie-Guardian은 민감 정보 유출과 보안 리스크를 관리합니다.

대표 이메일 주소
csm@saltware.co.kr

대표 전화
02-6249-6111

HOMEPAGE
https://www.saltware.co.kr/