



Unified Control Plane

Signum



Contents

1.	개요	02
2.	비즈니스 임팩트	04
3.	Signum 제품 구성	06
	핵심 역량	
	Desktop UI · IAM · KMS	
	Log · Alert · Audit · Notification	
	Security	
	Cloud Builder	
	Hub	
4.	관측성·보안·운영	13
5.	Works with	15

1. 개요



Signum = Unified Control Plane

시그넘은 엔터프라이즈 클라우드 운영에 필요한 핵심 제어 요소를 하나의 Unified Control Plane으로 통합합니다.

사용자는 서비스 접근, 운영 이벤트, 보안 자산, 인프라 구축 흐름을 일관된 기준으로 관리할 수 있습니다.

01 Access & Identity Control

Desktop UI · IAM · KMS — 웹 기반 데스크탑 환경에서 서비스를 운영하고, 사용자·그룹·프로젝트별 접근 권한을 세밀하게 제어하며, 내부 보안 자산을 중앙에서 관리합니다.

02 Event & Operation Control

Log · Alert · Audit · Notification — 플랫폼 전반의 운영 로그를 수집하고, 이상 징후를 실시간 감지하며, 모든 사용자 활동을 감사 로그로 추적하고, 통합 통지 채널로 전달합니다.

03 Security & Governance Control

Security — 네트워크·워크로드·테넌트 단위의 보안 정책을 설계하고, 전 계층에서 일관된 격리와 통제를 제공합니다.

04 Infrastructure Lifecycle Control

Cloud Builder — Aegis·Capsis·Metis·Maxis·Paxis 각 상품에 맞는 클라우드 인프라를 자동으로 구축하고, 운영 중 업데이트·업그레이드를 표준화합니다.

05 Asset & Catalog Control

Hub — 모델·데이터셋·앱·이미지를 한 곳에서 탐색·관리하고 무엇을 쓸 수 있게 할지 회사가 정합니다.

2.

비즈니스 임팩트



운영 통제권 없는 클라우드는 인프라가 아닙니다

클라우드를 구축했다고 해서 통제할 수 있는 것은 아닙니다. 누가 무엇에 접근했는지, 언제 어떤 변경이 발생했는지, 이상 징후가 있을 때 즉시 감지할 수 있는지 — 이 모든 것이 실제 운영 통제권의 기준입니다.

01 전 계층 통합 운영

시그넘은 엔터프라이즈 운영에 구조적으로 필요한 전 계층 요소를 통합합니다. 직관적인 웹 기반 데스크탑 UI로 클라우드를 앱처럼 운영하고 세밀한 IAM으로 접근을 통제하며 통합 로그·알림·감사로 모든 운영 이벤트를 가시화합니다. Notification으로 사용자·시스템 통지를 일원화하고 KMS로 내부 보안 자산을 중앙에서 관리합니다. Cloud Builder로 베어메탈 서버를 클러스터 자원으로 즉시 전환하고 Hub로 모델·데이터셋·앱·이미지를 한 곳에서 통제합니다.

02 핵심 메시지

배포부터 운영까지 일관된 통제 체계가 없다면 클라우드는 인프라가 아닌 부채가 됩니다. 시그넘은 엔터프라이즈 운영에 구조적으로 필요한 핵심 제어 요소를 처음부터 통합합니다.

3.

Signum 제품 구성



시그넘을 구성하는 10개 핵심 제어 요소



Desktop UI

웹 기반 데스크탑 환경에서 모든 클라우드 서비스를 앱 단위로 실행하고 관리



IAM

사용자·그룹·프로젝트별 접근 권한을 RBAC/PBAC로 세밀하게 제어



KMS

인증서·시크릿·암호화 키 등 내부 보안 자산을 중앙 관리



Log

플랫폼 전반의 운영 로그를 단일 지점에서 수집·분석



Alert

인프라 이상 징후를 실시간 감지하고 즉시 통보



Audit

모든 사용자 활동과 리소스 변경 기록을 전 구간 추적



Notification

운영 이벤트와 시스템 상태 변경을 통합 통지 채널로 전달



Security

네트워크·워크로드·테넌트 단위의 보안 정책을 설계하고 전 계층 격리 제공



Cloud Builder

Aegis·Capsis·Metis·Maxis·Paxis 각 상품에 맞는 클라우드 인프라를 자동 구축·업데이트



Hub

모델·데이터셋·앱·이미지를 한 곳에서 탐색·관리하고 승인된 자산만 현장에 공개



서비스 접근과 신원을 통제하는 통합 기반

Desktop UI·IAM·KMS는 클라우드 운영의 첫 번째 통제 계층을 구성합니다. 브라우저에서 실행되는 데스크탑 UI로 모든 서비스를 앱 단위로 운영하고, RBAC/PBAC 기반 IAM으로 사용자·프로젝트·테넌트 단위의 접근을 통제하며, KMS로 내부 보안 자산을 중앙에서 관리합니다.

01 Desktop UI

브라우저에서 실행되는 데스크탑 UI로 모든 클라우드 서비스를 앱 단위로 실행하고 관리합니다. 여러 창을 동시에 열어 데스크탑 수준의 멀티태스킹이 가능합니다.

02 IAM

역할 기반 접근 제어(RBAC)와 정책 기반 접근 제어(PBAC)를 통해 사용자·프로젝트·테넌트 단위의 권한을 안전하게 통제합니다. MFA와 IP 접근 제어를 지원하여 클라우드 접근 보안을 강화합니다.

03 KMS

인증서·시크릿·암호화 키 등 내부 보안 자산을 중앙에서 통합 관리하고, 자산의 생명주기를 추적하여 체계적으로 통제합니다.



운영 이벤트를 감지하고, 추적하고, 전달하는 통합 가시성

Log·Alert·Audit·Notification은 클라우드 운영의 전 구간 가시성을 제공합니다. 시스템 전반의 로그를 중앙에서 수집하고, 이상 징후를 실시간으로 감지하며, 모든 사용자 활동을 감사 로그로 기록하고, 통합 통지 채널로 전달합니다.

01 Log

Aegis, Capsis, Metis, Maxis, Paxis에서 발생하는 모든 시스템 이벤트와 로그를 중앙에서 통합 수집합니다. 운영 투명성을 높이고 장애 추적 시간을 단축합니다.

02 Alert

Aegis, Capsis, Metis, Maxis, Paxis의 Product 전반의 상태를 실시간으로 감시합니다. 임계값 기반 알림과 자동 복구 트리거를 통해 장애 대응 시간을 최소화합니다.

03 Audit

API 호출, 권한 변경, 리소스 생성·삭제까지 모든 운영 활동을 실시간 감사 로그로 기록합니다. 보안 사고 분석과 컴플라이언스 증빙에 필요한 감사 추적 체계를 제공합니다.

04 Notification

이메일, 웹훅 등 다양한 채널로 운영 이벤트와 시스템 상태 변경을 통합 관리하고 사용자에게 전달합니다.



조직의 보안 기준과 규제 요구를 충족하는 통제 체계

Signum은 클라우드 운영 전반에 적용되는 보안·거버넌스 제어 체계를 제공합니다. 네트워크·워크로드·테넌트 단위의 보안 정책을 설계하고, Tenant/Namespace 격리, Security Group, Network Policy, FWaaS를 통해 전 계층에서 일관된 격리와 접근 통제를 지원합니다. IAM의 RBAC/PBAC 정책, Audit의 활동 추적, KMS의 보안 자산 관리가 연계되어 엔터프라이즈 환경에서 요구되는 규제 대응과 보안 사고 대응 체계를 강화합니다.

01 맞춤형 보안 모델

기업의 보안 기준과 운영 정책에 맞춰 네트워크·워크로드·테넌트 단위의 보안 정책을 설계하고 적용합니다.

02 전 계층 격리 및 접근 제어

Tenant/Namespace 격리, Security Group, Network Policy, FWaaS를 통해 VM·컨테이너·네트워크 전 계층에서 일관된 보안과 격리를 제공합니다.

03 거버넌스 및 컴플라이언스

IAM 기반 접근 정책, Audit 기반 활동 추적, KMS 기반 보안 자산 관리가 연계되어 규제 준수 증빙과 보안 사고 대응 체계를 지원합니다.



클라우드 인프라를 자동으로 구축하고 일관되게 관리하는 표준화 체계

Cloud Builder는 Aegis·Capsis·Metis·Maxis·Paxis 각 제품에 맞는 클라우드 인프라를 자동으로 구축하고 업데이트합니다.
물리 서버 등록부터 OS 배포, 구성요소 설치까지 전 과정을 표준화하여 운영 일관성을 확보합니다.

01 자동화된 물리 서버 등록 및 프로비저닝

베어메탈 서버 감지, BMC 정보 자동 입력, HW 상태 조회 등 클라우드 구축 전 단계를 자동화하여 초기 구축 복잡도를 낮춥니다.

02 OS·클라우드 구성요소 일괄 배포

Base OS, 네트워크 구성, 스토리지 등을 템플릿 기반으로 일관되게 배포하여 설치 품질을 표준화합니다.

03 안정적인 업데이트·업그레이드

운영 중인 클라우드 환경에 대해 서비스 중단 없이 업데이트·업그레이드를 적용해 안정적인 플랫폼 상태를 유지합니다.



프로젝트에 필요한 AI 자산을 한 곳에서 통제하는 기반

Hub는 모델·데이터셋·앱·이미지를 한 곳에서 탐색·관리·배포하는 통합 자산 허브입니다. 무엇을 쓸 수 있게 할지는 회사가 정하고 자산을 실제로 돌리는 일은 그 자산을 쓰는 제품이 맡습니다.

01 자산 카탈로그

사내·오픈소스 모델, 데이터셋, 앱, 이미지를 한 곳에서 검색·조회합니다. 환경 구성 없이 자산을 즉시 training-inference 워크플로우에 적용합니다.

02 관리자 통제

무엇을 쓸 수 있게 할지 회사가 정합니다. 검증되지 않은 자산이 현장에 들어가지 않습니다.

03 승인 절차

외부에서 가져온 자산은 관리자 승인을 거쳐야 현장에 열립니다.

04 소비 앱 연계

골라 둔 자산은 Metis · Maxis · Capsis에서 바로 씁니다.

4.

관측성·보안·운영



운영 통제권의 기준이 다릅니다

배포부터 운영까지 일관된 통제 체계가 없다면 클라우드는 인프라가 아닌 부채가 됩니다. 시그넘은 엔터프라이즈 운영에 구조적으로 필요한 핵심 제어 요소를 처음부터 통합합니다.

01 누가 접근했는가

IAM / Audit — 사용자·그룹·프로젝트 단위 접근 제어 및 활동 기록 추적

02 무엇이 변경됐는가

Log / Audit — 리소스 생성·삭제·변경, API 호출, 권한 변경 기록 전 구간 추적

03 이상 징후를 감지했는가

Alert / Notification — 인프라 상태 실시간 감시, 임계값 기반 알림, 통합 통지 채널 전달

04 보안 자산이 중앙 관리되는가

KMS / Security — 인증서·시크릿·암호화 키 중앙 관리, 전 계층 격리 및 보안 정책 적용

05 인프라를 일관되게 구축·확장하는가

Cloud Builder — 물리 서버 등록부터 OS 배포·구성요소 설치·업데이트까지 전 과정 표준화

06 무엇을 쓸 수 있게 하는가

Hub — 모델·데이터셋·앱·이미지 카탈로그, 관리자 승인 기반 자산 공개 통제

5.

Works with



Works with

01 Aegis + Signum

IaaS 운영 기반 — Aegis의 Compute·Storage 인프라 위에서 접근 통제, 운영 가시성, 보안 격리, 인프라 구축 자동화를 제공합니다.

02 Metis + Signum

AI 플랫폼 운영 기반 — Metis의 모델 serving·GPU/xPU 자원 운영 위에서 사용자 관리, 로그·감사, 보안 정책, 클러스터 구축을 지원합니다.

03 Paxis + Signum

Agent 플랫폼 운영 기반 — Paxis의 Agent Builder·Enterprise RAG Engine·MCP Tool Hub 위에서 IAM 기반 접근 통제, Audit 기반 Agent 활동 추적, 보안 정책을 제공합니다.

04 Aegis + Capsis + Metis + Maxis + Paxis + Signum

전 계층 통합 — IaaS부터 AI Platform, Agent Platform까지 단일 제어 플레인으로 일관된 운영 통제 체계를 제공합니다.