



Unified Control Plane

Signum



Contents

1.	Overview	02
2.	Business Impact	04
3.	Signum Product Components	06
	Core Capabilities	
	Desktop UI · IAM · KMS	
	Log · Alert · Audit · Notification	
	Security	
	Cloud Builder	
	Hub	
4.	Observability, Security & Operations	13
5.	Works with	15

1. Overview



Signum = Unified Control Plane

Signum integrates the core control elements required for enterprise cloud operations into a single Unified Control Plane. Service access, operational events, security assets, and infrastructure build flows are all managed under one consistent standard.

01 Access & Identity Control

Desktop UI · IAM · KMS — Operate services from a web-based desktop environment, control access rights by user, group, and project in fine detail, and centrally manage internal security assets.

02 Event & Operation Control

Log · Alert · Audit · Notification — Collect operational logs across the platform, detect anomalies in real time, trace every user activity in audit logs, and deliver them through a unified notification channel.

03 Security & Governance Control

Security — Design security policies at the network, workload, and tenant level, and provide consistent isolation and control across every layer.

04 Infrastructure Lifecycle Control

Cloud Builder — Automatically build the cloud infrastructure that Aegis, Capsis, Metis, Maxis, and Paxis each require, and standardize updates and upgrades during operation.

05 Asset & Catalog Control

Hub — Explore and manage models, datasets, apps, and images in one place, with the organization deciding what can be used.

2.

Business Impact



A cloud without operational control is not infrastructure

Building a cloud does not mean you can control it. Who accessed what, when did a change occur, can anomalies be detected the moment they happen — these are the real measures of operational control.

01 Unified Operations Across All Layers

Signum integrates the full-stack elements that are structurally essential to enterprise operations. Manage your cloud like an app through an intuitive web-based desktop UI, enforce access through fine-grained IAM, and make every operational event visible through unified log, alert, and audit capabilities. Consolidate user and system notifications through Notification and centrally manage internal security assets with KMS. Instantly convert bare-metal servers into cluster resources through Cloud Builder, and govern models, datasets, apps, and images in one place with Hub.

02 Core Message

Without a consistent control framework from deployment through operations, a cloud becomes a liability rather than infrastructure. Signum integrates the essential control elements structurally required for enterprise operations from day one.

3. Signum Product Components



10 core control elements that make up Signum



Desktop UI

Run and manage all cloud services as individual apps from a web-based desktop environment



IAM

Control access rights by user, group, and project in fine detail through RBAC and PBAC



KMS

Centrally manage internal security assets such as certificates, secrets, and encryption keys



Log

Collect and analyze platform-wide operational logs from a single point



Alert

Detect infrastructure anomalies in real time and notify immediately



Audit

Track all user activity and resource change records end-to-end



Notification

Deliver operational events and system state changes through a unified notification channel



Security

Design security policies at the network, workload, and tenant level and deliver isolation across every layer



Cloud Builder

Automatically build and update the cloud infrastructure each of Aegis, Capsis, Metis, Maxis, and Paxis requires



Hub

Explore and manage models, datasets, apps, and images in one place, exposing only approved assets to teams



A unified foundation that controls service access and identity

Desktop UI, IAM, and KMS form the first control layer of cloud operations. Operate every service as an individual app through a desktop UI that runs in the browser, control access at the user, project, and tenant level with RBAC/PBAC-based IAM, and centrally manage internal security assets with KMS.

01 Desktop UI

Run and manage all cloud services as individual apps from a browser-based desktop UI. Open multiple windows simultaneously for desktop-level multitasking.

02 IAM

Securely govern permissions at the user, project, and tenant level through role-based access control (RBAC) and policy-based access control (PBAC). MFA and IP-based access policies strengthen cloud access security.

03 KMS

Centrally manage certificates, secrets, and encryption keys within the platform. Track and systematically govern the full lifecycle of each asset.



Unified visibility that detects, traces, and delivers operational events

Log, Alert, Audit, and Notification provide end-to-end visibility across cloud operations. Collect system-wide logs centrally, detect anomalies in real time, record every user activity in audit logs, and deliver them through a unified notification channel.

01 Log

Centrally aggregate every system event and log generated by Aegis, Capsis, Metis, Maxis, and Paxis. Operational transparency rises and the time it takes to trace an incident drops.

02 Alert

Monitor the state of the Aegis, Capsis, Metis, Maxis, and Paxis products in real time. Threshold-based alerts and automated recovery triggers minimize incident response time.

03 Audit

Log every operational action — API calls, permission changes, resource creation and deletion — as a real-time audit record. Deliver the audit trail required for security incident analysis and compliance evidence.

04 Notification

Manage operational events and system state changes in a unified way across channels such as email and webhook, and deliver them to users.



A control framework that meets organizational security standards and regulatory requirements

Signum provides the security and governance control framework that applies across cloud operations. Design security policies at the network, workload, and tenant level, and support consistent isolation and access control across every layer through Tenant/Namespace isolation, Security Groups, Network Policies, and FWaaS. RBAC/PBAC policies in IAM, activity tracking in Audit, and security asset management in KMS work together to strengthen regulatory response and security incident response in enterprise environments.

01 Custom Security Model

Design and apply security policies at the network, workload, and tenant level to match your organization's security standards and operational policies.

02 Full-Layer Isolation and Access Control

Deliver consistent security and isolation across VMs, containers, and networks through Tenant/Namespace isolation, Security Groups, Network Policies, and FWaaS.

03 Governance and Compliance

IAM-based access policies, Audit-based activity tracking, and KMS-based security asset management work together to support compliance evidence and security incident response.



A standardized framework that builds cloud infrastructure automatically and manages it consistently

Cloud Builder automatically builds and updates the cloud infrastructure each of Aegis, Capsis, Metis, Maxis, and Paxis requires. Standardizing the whole process — from physical server registration through OS deployment to component installation — secures operational consistency.

01 Automated Server Registration and Provisioning

Automate every step that precedes a cloud build — bare-metal server discovery, automatic BMC entry, hardware status lookup — and lower the complexity of the initial build.

02 Bulk Deployment of OS and Cloud Components

Deploy the base OS, network configuration, and storage consistently from templates, and standardize installation quality.

03 Stable Updates and Upgrades

Apply updates and upgrades to a running cloud environment without service interruption, and keep the platform in a stable state.



One place to control the AI assets your projects need

Hub is a unified asset hub for exploring, managing, and deploying models, datasets, apps, and images in one place. The organization decides what can be used, and running the assets is left to the products that consume them.

01 Asset Catalog

Search and browse in-house and open-source models, datasets, apps, and images in one place. Apply them to training and inference workflows immediately, with no environment setup.

02 Administrator Control

The organization decides what can be used. Unverified assets never reach teams.

03 Approval Process

Assets brought in from outside are released to teams only after administrator approval.

04 Consuming Apps

Approved assets are consumed directly by Metis, Maxis, and Capsis.

4.

Observability, Security & Operations



A higher standard for operational control

Without a consistent control framework from deployment through operations, a cloud becomes a liability rather than infrastructure. Signum integrates the essential control elements structurally required for enterprise operations from day one.

01 Who accessed it?

IAM / Audit — Access control by user, group, and project; activity records traced

02 What was changed?

Log / Audit — Resource creation, deletion, and change, API calls, and permission changes tracked end-to-end

03 Were anomalies detected?

Alert / Notification — Real-time infrastructure monitoring, threshold-based alerts, unified notification delivery

04 Are security assets centrally managed?

KMS / Security — Central management of certificates, secrets, and encryption keys; full-layer isolation and security policy enforcement

05 Is infrastructure built and scaled consistently?

Cloud Builder — The full process standardized, from physical server registration through OS deployment, component installation, and updates

06 What can be used?

Hub — Model, dataset, app, and image catalog; asset exposure governed by administrator approval

5.

Works with



Works with

01 Aegis + Signum

IaaS operations foundation — Provides access control, operational visibility, security isolation, and infrastructure build automation on top of the Aegis Compute and Storage infrastructure.

02 Metis + Signum

AI platform operations foundation — Supports user management, log and audit, security policy, and cluster build on top of Metis model serving and GPU/xPU resource operations.

03 Paxis + Signum

Agent platform operations foundation — Provides IAM-based access control, Audit-based agent activity tracking, and security policy on top of the Paxis Agent Builder, Enterprise RAG Engine, and MCP Tool Hub.

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

Full-stack integration — Delivers a consistent operational control framework from IaaS through AI Platform to Agent Platform on a single control plane.