ARTIFICIAL INTELLIGENCE · ADVANCED · 2 DAYS

Cursor for Enterprise: Security, Governance and Cost Control

The administration layer for organisations deploying Cursor at scale. Covers identity and access, data handling and privacy enforcement, audit and AI code visibility, usage-based cost control, extension governance, and the policy work that has to exist before AI-authored code reaches production.

Why Cursor for Enterprise?

Policy before rollout

Identity, privacy and acceptable-use settled before the first licence is assigned.

Visibility into AI-authored code

Know how much of your codebase came from an agent and who reviewed it.

Predictable spend

Usage-based pricing is easy to lose control of. Learn the levers that actually work.

Supply chain awareness

Extensions and MCP servers are a real attack surface. Govern them deliberately.

What you'll be able to do

- ✓ Compare plan tiers and select the right one against actual requirements
- ✓ Configure single sign-on, provisioning and role-based access
- ✓ Enforce privacy settings and understand what leaves the developer machine
- ✓ Use audit logs and code tracking to see how AI-authored code enters the codebase
- ✓ Model, budget and control usage-based consumption across teams
- ✓ Govern extensions, plugins and MCP servers as a supply chain concern
- ✓ Write an acceptable-use policy for AI-assisted and AI-authored code
- ✓ Design a rollout with pilot gates and meaningful success metrics

Who this is for

- Engineering leadership and platform owners
- Security architects and application security teams
- IT administrators managing developer tooling
- Procurement and FinOps stakeholders on developer spend

Curriculum

01 Plans, Deployment and Identity

- Plan tiers compared on governance capability rather than feature lists
- Single sign-on with SAML and OIDC
- Automated provisioning and deprovisioning
- Role-based access and administrative delegation
- **Hands-on:** map your organisation's requirements to a tier and configuration

02 Data Handling and Privacy Enforcement

- What leaves the developer machine, and under which settings
- Enforcing privacy mode organisation-wide rather than per developer
- Codebase indexing and what it means for sensitive repositories
- Considerations for regulated, air-gapped and client-restricted work
- Answering the questions your security review will actually ask

03 Audit, Visibility and AI Code Tracking

- Audit logs and what activity is captured
- Tracking the proportion of code authored with AI assistance
- Attribution, labelling and traceability of agent-generated changes
- Producing evidence for internal audit or client assurance
- Establishing a review cadence on the data you collect

04 Cost Control and Usage Management

- How usage-based consumption accumulates across surfaces
- Separate usage pools and what falls into each
- Model selection as the primary cost lever
- Budgeting, monitoring and handling overage by team
- **Hands-on:** build a consumption forecast for a team of thirty

05 Extension and MCP Governance

- Team marketplaces and centralised plugin control
- Approving extensions and MCP servers rather than allowing anything
- Supply chain risk in developer tooling
- Reviewing what a connector can reach before it is approved
- Maintaining an approved list without blocking legitimate work

06 Policy, Rollout and Measurement

- Writing an acceptable-use policy for AI-assisted and AI-authored code
- Licence allocation and phased rollout with genuine decision gates
- Metrics that survive scrutiny: cycle time, review load, escaped defects
- Avoiding vanity metrics that prove nothing to a finance director
- **Hands-on:** draft a rollout and governance plan for your organisation