

Pinecone BYOC — Shared Responsibility Model

Zero-access BYOC: Data plane runs in customer's cloud account; control plane managed by Pinecone.

Resource / Domain	Pinecone	Customer	Notes & Conditions
Software & Updates			
Software upgrades and hotfixes	✓		Customer must opt out of auto-approve for upgrades; opt-out requires a separate agreement.
Software vulnerability remediation	✓		Same opt-out conditions apply as for software upgrades.
Infrastructure vulnerability remediation		✓	
Cost & Billing			
Cost management and attribution	✓	✓	Pinecone provides metering and billing visibility. Customer monitors cloud-provider infrastructure costs.
Compute & Storage			
Compute (autoscaling)	✓	✓	Pinecone manages service autoscaling. Customer manages index resources and max node size.
Local storage	✓		
Tiered storage (object storage)	✓		
Networking			
VPC (subnets, routing, firewall rules)		✓	
VPC peering		✓	
Private endpoint — service side		✓	
Private endpoint — consumer side		✓	
Control Plane & Access			
Control plane operations	✓		
User access controls and audit (API keys, RBAC)	✓	✓	Pinecone operates the control plane. Customer configures users and API keys through the console.
IAM (roles, service accounts, access segmentation)		✓	
Security			
Proactive threat detection	✓	✓	Pinecone issues advisories on platform threats. Customer acts on that information.

Resource / Domain	Pinecone	Customer	Notes & Conditions
Static secret rotation	✓		
Incident response	✓	✓	Pinecone provides guidance and support during incidents but does not have direct cluster access.
Reliability & Compliance			
Availability SLA		✓	
Observability and monitoring (SLOs, SLIs, tracing, alerting)	✓		
Resilience verification	✓	✓	Pinecone verifies software version and setup. Customer is responsible for VPC environment.
Managed disaster recovery		✓	

✓ = Responsible party. Shared (both columns checked) = joint responsibility with distinct scopes described in Notes.