Unified AI-Driven Cybersecurity and Governance Platform

A cloud-native application protection platform (CNAPP) for multicloud, hybrid and on-premises environments.

Platform at a Glance

The platform secures cloud infrastructure, identities, databases, and workloads from code to runtime, with AI-driven threat detection for unusual activity, just-in-time (JIT) controls for least-privilege access, and cloud change governance. Its FinOps capabilities forecast cloud spend with AI and identify opportunities to optimize costs.

Deployment Environments

- Public and private cloud
- Hybrid and multi-cloud
- On-premises infrastructure
- Air-gapped environments

Industries Served

- Financial services and healthcare
- Technology and manufacturing
- Retail, education and government



Platform Coverage

Cloud Security & Governance

Posture, access governance and threat detection

Database Security & Governance

Posture, access and activity monitoring

Managed Security Services

Monitoring, assessment and audit support

Workload Protection

Pre-deployment checks and runtime protection

CloudOps & FinOps

Governed operations, cost forecasting and optimization

50+ compliance frameworks

1,000+ deployments

Frameworks include GDPR, HIPAA, PCI DSS, ISO 27001, SOC 2, NIST, PIPEDA, PDPA and the Australian Privacy Act.

Cloud Security & Workload Protection

Cloud Security & Governance

Monitor cloud posture, govern access and investigate threats across environments. Apply security policies and route operational changes for approval.

Cloud Security Posture Management (CSPM)

Monitor posture, customize policies and use snapshots for audits.

Cloud Governance & IaC Security

Track asset changes, enforce policies and prioritize vulnerabilities by risk.

Access Governance (CIEM + JIT)

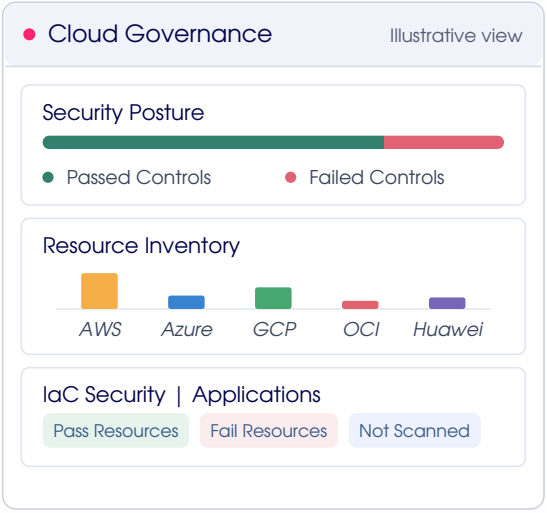
Apply least privilege and just-in-time access through IAM workflows.

AI-Driven Cloud Detection & Response (CDR)

Detect threats using signatures and behavior. Investigate and respond.

Secure Cloud Operations

Apply security controls and route operational changes for approval.



Runtime Workload Protection

Monitor Kubernetes, containers and hosts. Detect threats, enforce runtime policies and respond across cloud, hybrid and on-premises environments.

Runtime Monitoring

Monitor processes, network activity and file changes in Kubernetes and containers.

Real-Time Response

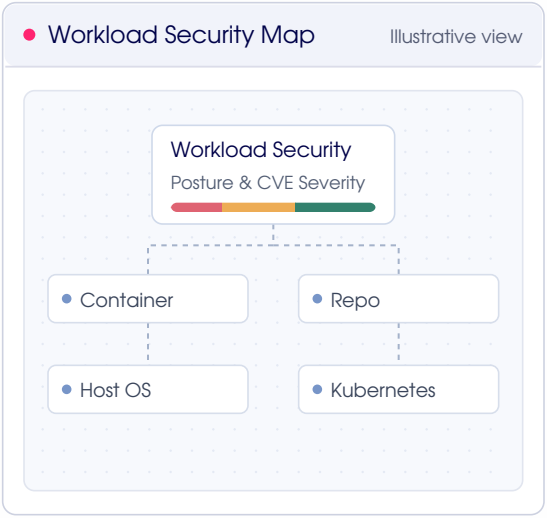
Block connections, stop processes, isolate workloads, quarantine containers or open tickets.

AI Security Analytics

Detect unusual behavior, map it to MITRE ATT&CK and enforce runtime policies.

Pre-Deployment Security

Check Kubernetes, containers and hosts for vulnerabilities and exposed secrets.



Supported Workload Platforms & Integrations
Kubernetes on AWS, Azure, Google Cloud and OCI · GitHub · GitLab · Windows · Linux

FinOps & Database Security

AI-Driven FinOps & Cost Optimization

See where cloud spend goes, forecast costs with AI and review security and operational risks before acting on savings opportunities.

AI-Driven Forecasting & Budgeting

Forecast spend from usage trends. Track budgets and review alerts.

Cost Visibility & Allocation

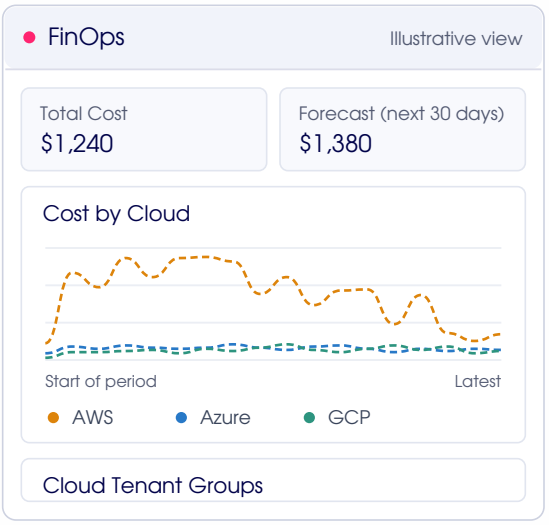
Track spend by account and environment. Allocate costs for showback and chargeback.

Cost Governance & Guardrails

Set cost policies and apply rules for tags and resource usage.

Cost Optimization & Savings

Find idle and oversized resources. Review right-sizing options and expected savings.



Database Security & Governance

Discover sensitive data, monitor database activity and govern access. Find configuration issues and track compliance across your database estate.

Database Security Posture Management (DbSPM)

Find misconfigurations and vulnerabilities. Monitor compliance.

Database Infrastructure Entitlement Management (DIEM)

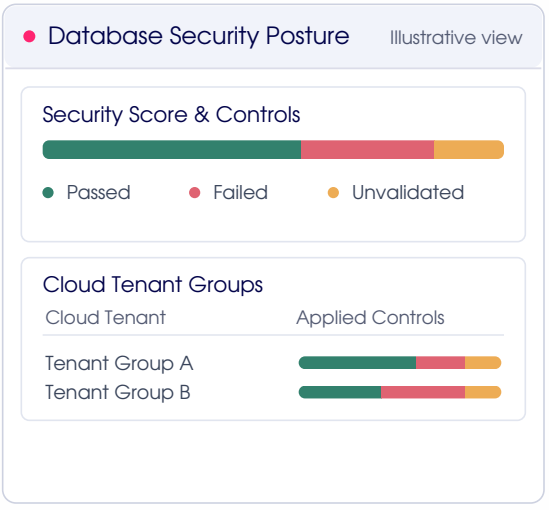
Review entitlements and grant least-privilege access just in time.

Data Discovery & Classification

Find and classify sensitive data. Maintain a data inventory.

Database Activity Monitoring (DAM)

Monitor user activity and queries. Detect suspicious behavior.



Supported Databases
Oracle, SQL Server, MySQL, MongoDB and PostgreSQL

Managed Security & Professional Services

Cybersecurity as a Service

Banyan Cloud delivers managed cybersecurity through its own CNAPP, with services for cloud risk, threat response, assurance and security leadership.

Managed Cloud Risk

Find and prioritize risks across cloud posture, workloads, identities, vulnerabilities and exposed data.

Detect & Respond

Monitor cloud and on-premises environments 24×7. Investigate, contain and respond to threats.

Assurance & Compliance

Assess vulnerabilities, test defenses and audit infrastructure. Review compliance evidence and verify fixes.

Security Leadership

Get guidance on security strategy, governance and risk, with reporting for boards and regulators.

Explore Cybersecurity as a Service

How the Services Work Together

- **Prioritize Cloud Risk**
  Find the risks that need action first.
- **Investigate & Respond**
  Contain threats around the clock.
- **Validate Controls**
  Test defenses and verify fixes.
- **Guide Security Decisions**
  Set priorities and report progress.

Why Banyan Cloud

Security & Governance

- Agentless visibility and attack path analysis
- AI-driven risk prioritization and response
- Continuous compliance monitoring and audit reporting
- Security and operations in one platform

Deployment Options

- SaaS and private SaaS
- On-premises and air-gapped environments
- Self-service onboarding and executive reporting

See Banyan Cloud in action

Request a demo to see how Banyan Cloud brings security, compliance, operations and cost management together.

Request a demo