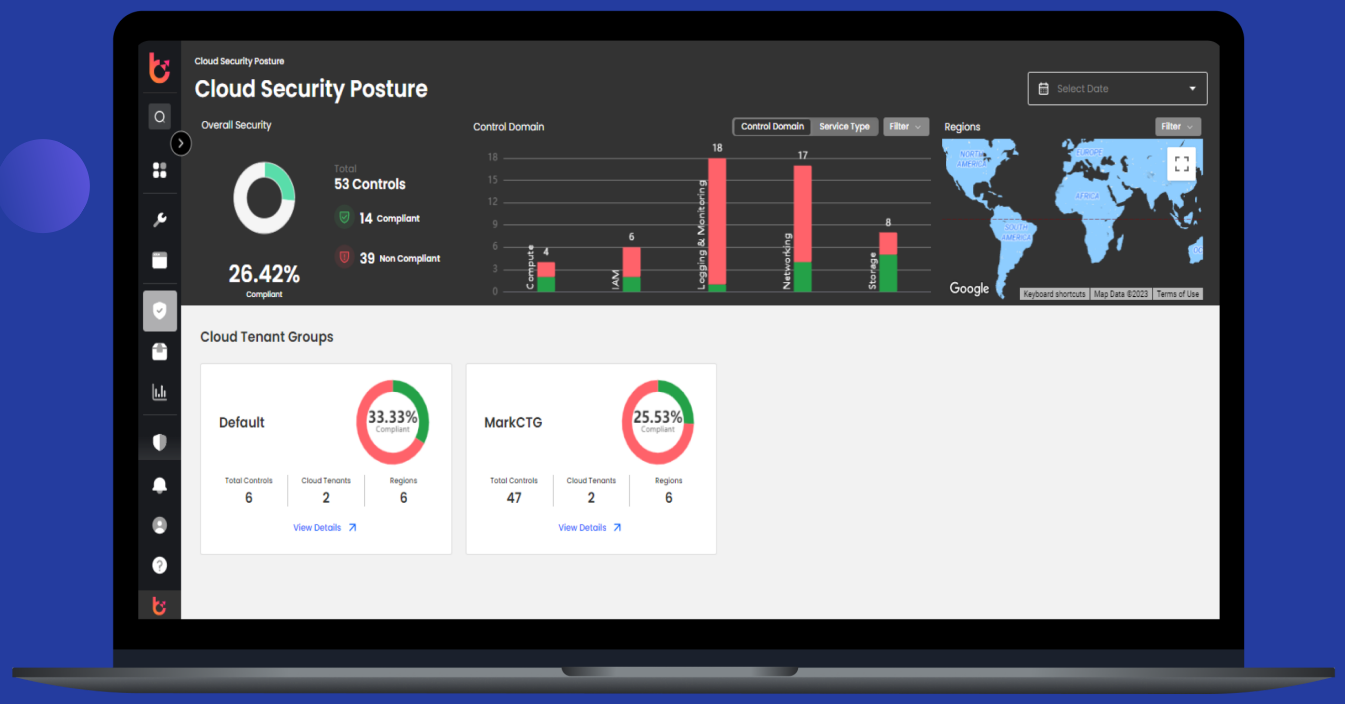
Banyan Cloud

Next Generation Cyber Security SaaS

ONE solution for **Code to Cloud Security** of all Business Applications with real-time **Security Posture Monitoring & Compliance.**



Why Banyan Cloud?

- One SaaS solution for both Security and IT teams
- Multiple Security tools on one platform
- Cloud Security Posture Management is simplified
- Enable Zero Trust Entitlement
- Data first security across Hybrid Data Technologies
- Advanced SecOps with Incident Management System
- Remediation at your fingertip

Cloud Environments We Support

aws · Azure · Google Cloud · ORACLE · Alibaba Cloud

Databases Environments We Support

MySQL · Microsoft SQL · PostgreSQL · ORACLE · mongoDB

PRODUCT OVERVIEW

Banyan Cloud is the most comprehensive Cloud Native Application Protection Platform that secures Cloud Native Applications, Cloud Infrastructure, Data Storage, and DevOps Technology Stack across Multi-Cloud and Hybrid Infrastructure Environments.

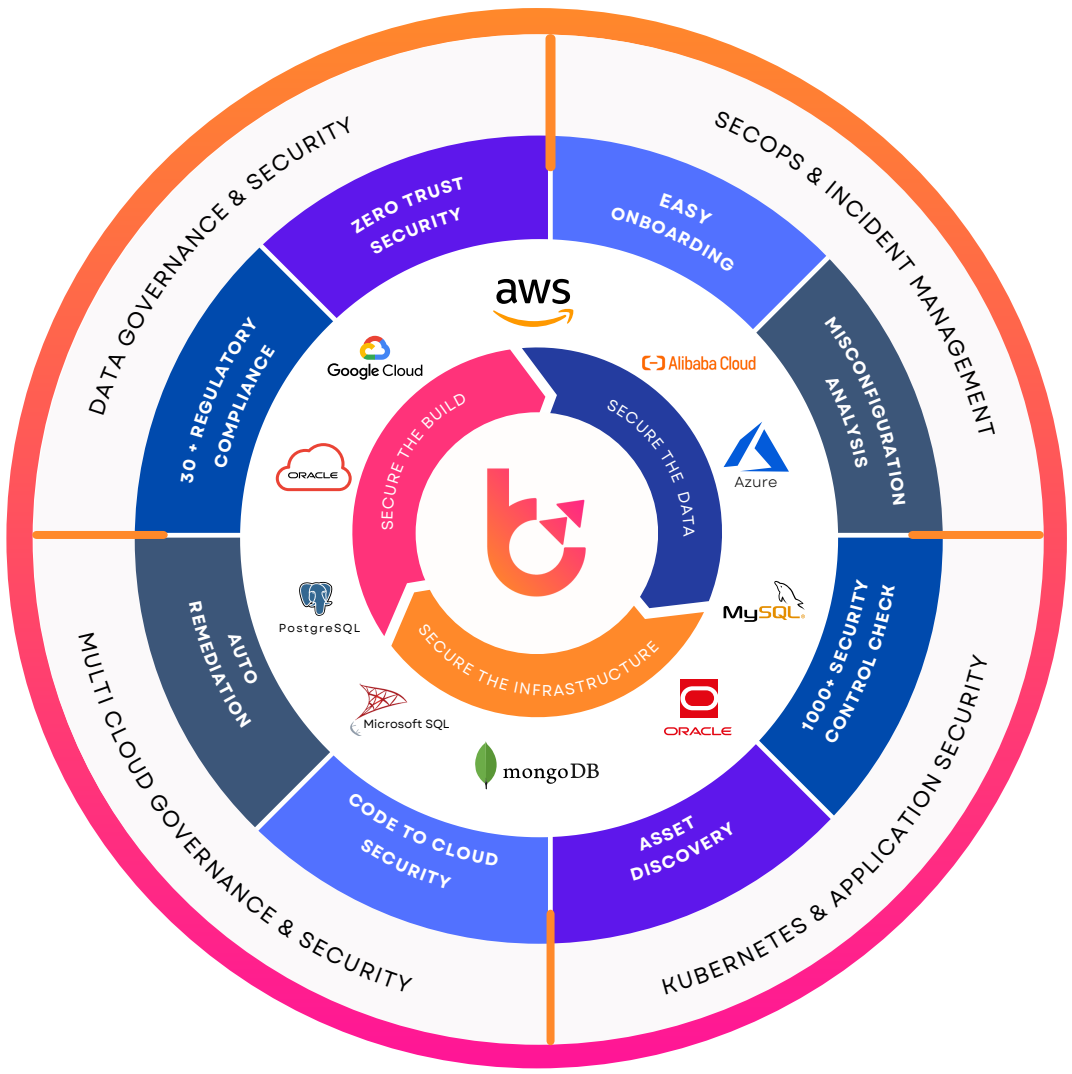
Banyan Cloud makes it necessary for businesses to collaborate and develop effective cybersecurity strategies, Serving as a market-leading product of cloud-native cybersecurity solutions and services. Our methodology offers practical strategies for strengthening cloud and data security and suggestions for enhancing compliance with many regulatory regimes.

The integrated approach of Banyan Cloud enables IT Operations, Development, and Security Operations to remain flexible, collaborate effectively, securely accelerate cloud-native application development and deployment.

BANYAN CLOUD PROVIDES EXTENSIVE SECURITY WITH THESE FEATURES

- MULTI CLOUD GOVERNANCE & SECURITY
- DATA GOVERNANCE & SECURITY
- KUBERNETES & APPLICATION SECURITY
- SECOPS & INCIDENT MANAGEMENT

One Integrated Platform For A Secure Multi-Cloud Environment



KEY BENEFITS

- **Governance, Security, and Compliance** for the entire cloud stack.
- Prevent Cyberattacks with real-time enforcement of industry-leading **Security Configuration Standards.**
- Comprehensive **Data Security & Privacy Standards** for All Data Technologies to protect from Data exposure and Ransomware threats.
- Code to Cloud security simplified - One security tool for **Shift Left, Container, Kubernetes, Data Storage, IaC and Cloud Infrastructure.**
- Focused unique CSPM approach that reduces the complexity of **Misconfiguration, Security Posture** and helps to secure multi-cloud environments while radically simplifying compliance.
- Be proactively prepared for future threats by **Continually Reviewing 30+ Compliances** to ensure your business meet industry and regulatory demands while maintaining a secure system.
- Reduce human effort and security costs by drastically improving the business performance and response capability using **Advanced SecOps with Incident Management System (IMS)** built on AI-driven technology.

WHO WE ARE?

Banyan Cloud is the most innovative Cloud-Native Application Protection Platform from Banyan Cloud Inc, USA. This security platform is built on the foundation of Zero Trust and Data First principles. The company is founded by **Nagesh Konduru, an Apple Veteran with 20+ years of expertise in securely managing Apple's** highly scalable infrastructure and data services for hyper-growth applications.

Banyan Cloud Distinct Features

FEATURES	PRODUCT HIGHLIGHTS
Cloud Governance	• One tool for Multi-Cloud and Multi-Technology stacks. • Security coverage from Code to Cloud for all business applications. • Easy onboarding of Cloud Accounts and Auto Discovery of Resources. • Deep observability of Cloud Assets with Change-Tracking Capabilities. • Highly customizable authorization and policy management for zero security implementation. • Coherence integration of security posture of Cloud with Data Storage and DevOps. • AI-based observability of multi-cloud events logs and network logs to detect potential threats.
Cloud Security Posture Management (CSPM)	• One dashboard for multi-cloud security posture management. • Unprecedented Real-time threat monitoring with detection of unsecured cloud resource configuration. • Continuous compliance checks against more than 30+ Regulatory standards across all Industries and Regions. • CIA-triad focused Security management for multi-cloud environments. • Advance search capabilities of security posture at any given time for any regulation. • High customization of security controls for fine-grain access management. • Drill-down analysis of security posture among dependent resources is easier than ever. • Enhance IT team's productivity with auto-remediation capabilities.
Data Governance	• Enablement of the Fine-grained user access controls at the data object levels across multi-data technologies. • Advanced data storage inventory capabilities that reflect data objects and their dependent objects with versioning of changes. • AI-based co-relation of Database audit logs with infrastructure logs to detect potential threats. • Unified view of popular Data storage technologies (MySQL, PGSQL, MSSQL, Oracle and Mongo DB, etc.) • Data storage on the public cloud, hybrid cloud, and on-premises is supported. • Simplified provisioning and ease of use data security operational tasks. • Single pane of glass for all the multi-data storage technologies and instances.
Data Security Posture Management	• Auto-discovery of data storage instances with agentless architecture. • Empower IT teams with Auto & Manual Remediation capabilities to fix data storage misconfigurations. • Instant compliance check against more than 30+ leading regulatory and data privacy standards (GDPR, SOC2, ISO27001, HIPPA, PCI DSS, etc.) • Real-time monitoring of data storage misconfiguration and excessive permissions granted. • Stringent data storage configuration security standards are enforced for all popular data storage technologies on the Cloud and On-premise infrastructure. • Enrich features of Security incident management of compliance failures. • The complexity of Multi data technology security posture is simplified.
Cloud Identity Entitlement Management (CIEM)	• Follow least privilege recommendations in industry frameworks like the CSA, CCM and the MITRE ATT&CK Framework • Assess compliance with relevant regulatory requirements, including PCI DSS • Monitor excessive and unused privileges. Automate remediation of overly permissive roles • Detect and identify unused and misconfigured IAM permissions that pose a heightened risk. Prioritize and remediate improper permission combinations • Use cutting-edge analysis and artificial intelligence algorithms to pinpoint critical cloud security issues and identify and mitigate risks and threats • Optimize and measure risk exposure for each platform, environment, and individual identity in cloud estate • Ensure proper access through identity-based policies, resource-based policies, service control policies, and session policies • Remediate permissions rapidly and consistently across platforms
Real-time Regulatory Compliance	• Gain valuable insights through a powerful and reliable Views and Dashboard system • Supports CIA triad-based risk categorization and level (High, Medium & Low) • Deliver actionable data to demonstrate where security posture improvements are necessary • Auto and manual remediation capabilities to fix the identified misconfiguration • Review status/progress for any given duration • Banyan Cloud's continuous monitoring system gives a complete view of compliance status at all times. Gain real-time visibility with extensive dashboards and alerts • Rich set of out-of-the-box of 30+ regulations support such as HIPAA, SOC 2, GDPR, MITRE ATT&CK v10, ISO/IEC 27001:2013, PCI DSS V3.2.1, etc. for cloud security (Supports AWS, Azure, GCP, OCI, Alibaba), and monitor corporate-specific 1000+ security controls for data sovereignty and governance • Provides historical and current data to prove security and compliance with regulations. • Monitoring essential tools and services on a regular basis to guarantee that, after you become compliant, you remain compliant

Supported Regulations

Region (Geography)	Country	Known Regulation Name Worldwide	Industry / Sector	Regulation Authority Source
GLOBAL	Global	SOC 2	Technology, SaaS, financial, healthcare, and education industries.	AICPA
		COBIT 2019	Any organization, whether public or private.	ISACA
		CSA CCM v4	All types of cloud computing industries.	CSA
		ISO/IEC 27001:2013 ISO/IEC 27001:2022 ISO/IEC 27002:2022 ISO/IEC 27701:2019	Any organization, whether public or private.	ISO
		PCI DSS v3.2.1 PCI DSS v4.0	ANY organization, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data.	PCI SSC
		NIST SP 800-171 Rev. 2	If a manufacturer is part of a Department of Defense (DoD), General Services Administration (GSA), NASA or other federal or state agencies' supply chain.	NIST
		NIST SP 800-53 Rev. 5	This is generally leveraged by large business enterprises and government agencies, but it can be a helpful framework for any organization interested in evaluating and reducing cyber risk.	
EMEA	UK	NCSC Cyber Assessment Framework v3.1	Large organisations (e.g.; Cyber security advice for businesses, charities and critical national infrastructure with more than 250 employees.), Public sector organisations employees and Cyber security professionals.	UK National Cyber Security Centre
		Cyber Essentials v2.2	For all organisations, of any size, in any sector.	UK
	Europe	GDPR	All organizations that collect personal data of EU citizen.	European Union
	UAE	UAE Information Assurance Regulation v1.1	All UAE government entities and other entities identified as critical by Telecommunications Regulatory Authority (TRA) are obligated to implement these. However, TRA highly recommends all entities in the UAE to adopt these on a voluntary basis, as applicable, in order to participate in raising the nation minimum security levels.	Telecommunications & Digital Government Regulatory Authority
APAC	Australia	Australian Privacy Principles	All organizations collect the personal data of any citizen of Australia.	Office of the Australian Information Commissioner
	Singapore	MAS Technology Risk Management Guidelines	All licensed financial institutions (FIs) in Singapore, including service providers such as Funding and investment-related companies, Insurance companies and reinsurers, Banks, wholesale banks, financial holding companies, Credit and payments-related companies, Market operators, and financial exchanges.	Monetary Authority of Singapore
US	US-Virginia	VCDPA	All organizations that collect personal data of US-Virginia.	Virginia State
	US-California	CCPA CPRA	All organizations that collect personal data of US-California.	California State
	US	CMMC v1.0 CMMC v2.0	Applies to anyone in the defense contract supply chain. Including contractors who engage directly with the US Department of Defense and subcontractors contracting with primes to fulfill and/or execute those contracts.	Federal
		HIPAA	Medical industries, Health plans, Health care clearinghouses, and Health care providers who conduct certain financial and administrative transactions electronically.	
MEXICO	Mexico	NERC CIP	All segments of the electric industry: investor-owned utilities; federal power agencies; rural electric cooperatives; state, municipal, provincial utilities; independent power producers; power marketers; and end-user customers.	
CANADA	Canada	Canada PIPEDA Principles	All organizations collect the personal data of Canadian citizens.	The Office of the Privacy Commissioner of Canada (OPC)
BRAZIL	Brazil	Brazilian Data Protection Law (LGPD)	All organizations collect the personal data of any citizen of Brazil.	The NATIONAL CONGRESS, Brazil