



How Gemini Data Safeguards Your Data in the Cloud

Explore how Gemini Data implements essential security best practices to ensure data confidentiality, integrity, and availability within cloud environments.



Contents

Secure Infrastructure	1
Access Control	2
• Data Segregation	
• Employee Access to Customer Data	
Data Protection	3
• Encryption	
• Secure Data Processing	
• Asset Management and Disposal	
• Change Management	
Logging, Monitoring, and Response	4
Conclusion	4

As businesses increasingly rely on cloud-based services, safeguarding customer data has become a **mission-critical priority**.

This white paper outlines how Gemini Data, as a leading technology vendor, implements essential security best practices to ensure data confidentiality, integrity, and availability within cloud environments.

These practices provide transparency and assurance to business stakeholders concerned with regulatory compliance, data privacy, and operational resilience.



SECURE INFRASTRUCTURE

Every strong cloud security strategy begins with a resilient foundation. At Gemini Data, we build this foundation with secure system architecture, proactive threat monitoring, and robust design principles that **ensure continuity, scalability, and protection**.

Gemini Data establishes a robust, secure foundation across all cloud-hosted systems. This foundation is strengthened through industry-standard best practices, which include:

- Using hardened virtual machines
- Employing firewalls and intrusion prevention systems (IPS)
- Network Segmentation
- Continuous monitoring for vulnerabilities and threats.

We design our infrastructure with fault tolerance and high availability to support business continuity.

We also leverage cloud-native tools and third-party audits to validate security and fix misconfigurations before they cause harm.

ACCESS CONTROL

Controlling access is fundamental to cloud security. Our access control practices ensure that only the right individuals, at the right time, can reach sensitive systems and data. This reduces the risk of internal threats and external breaches.

Gemini Data's strict identity and access management (**IAM**) ensures only authorized users can access systems and data. Role-based access control (**RBAC**), multi-factor authentication (**MFA**), and **periodic access reviews** enforce the principle of least privilege, where users are given only the minimum level of access required to perform their tasks.

We integrate with enterprise identity providers for streamlined and secure access management. All access policies are centrally managed and enforced through automated policy engines, with alerts for anomalous access behavior (such as unusual login times, IPs, or access patterns).

Data Segregation

In multi-tenant cloud environments, clear boundaries between customer data are essential, which is why Gemini Data's cloud architecture ensures **logical or physical segregation of customer data**.

This prevents unauthorized access between tenants and supports data sovereignty and compliance needs. We use **access rules**—alongside **containerization** and **namespace isolation**—to ensure that each client's data remains securely separated from others.

Employee Access to Customer Data

Access to customer data by Gemini Data employees is tightly controlled. Our team only accesses customer data when **absolutely necessary** and **only with your consent or predefined contractual permissions**.

Access to corporate and production networks is restricted to company-issued devices only, which are equipped with full disk encryption and up-to-date antivirus software.

Authorized personnel must follow our security protocols whenever they access or manage sensitive systems or data. **All access is logged, monitored, and subject to audit.**

Additionally, employees undergo mandatory security and privacy training and operate under binding confidentiality agreements. Just-in-time access provisioning and temporary access windows further reduce risk.

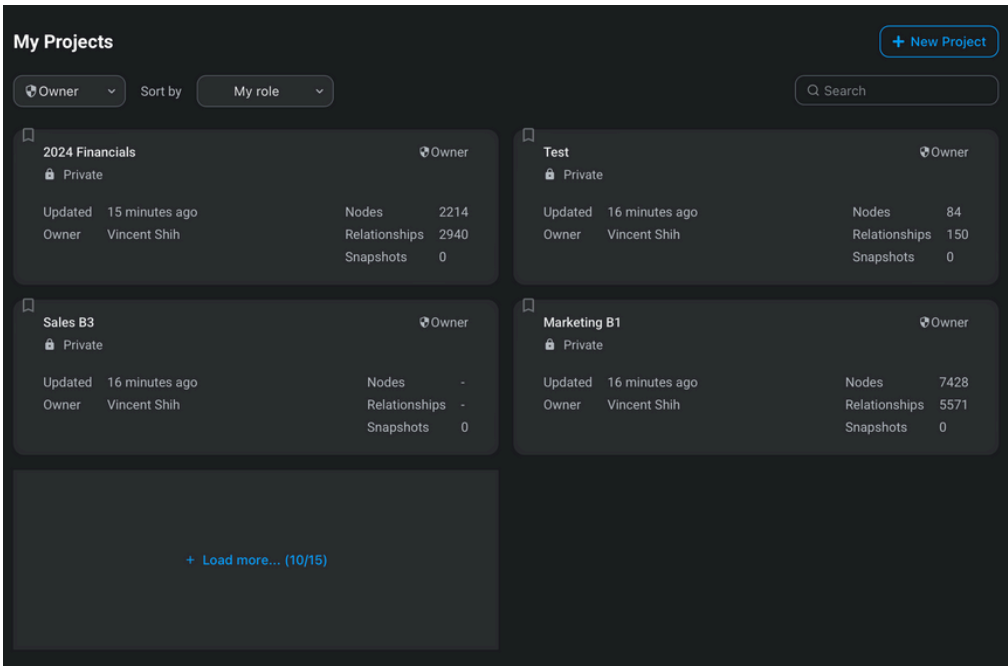


Figure 1:
Gemini Enterprise project dashboard

Individual projects are segregated and protected by Role-Based Access Controls.

DATA PROTECTION

Protecting customer data is at the heart of our security approach. We take a **multi-layered approach** to protect it—whether it's in storage, in motion, in use, or being retired. From encryption to secure disposal, your data stays safe at every stage of its lifecycle.

Encryption

Encryption is a foundational control at Gemini Data. We implement full disk encryption for storage, key management systems (**KMS**) with strict access controls, and customer-managed keys (**CMK**) when applicable.

Data in use is protected via memory encryption or confidential computing environments, which keep sensitive data encrypted even while being processed.

Our encryption protocols are regularly reviewed and aligned with industry standards such as NIST and ISO/IEC 27001.

Secure Data Processing

Gemini Data protects customer data both in transit and at rest using strong encryption standards (e.g., **TLS 1.2+** and **AES-256**). We ensure APIs and data processing services enforce authentication, authorization, and input validation.

Our secure software development lifecycle (SDLC) incorporates multiple safeguards, including code scanning, dependency checks, threat modeling, and regular penetration tests to catch vulnerabilities early.

Asset Management and Disposal

All cloud assets handling customer data are inventoried, tracked, and classified by Gemini Data. When decommissioning storage media or virtual assets, we employ secure erasure or cryptographic wiping methods to ensure data cannot be recovered.

Automated discovery tools maintain visibility into assets, and our disposal policies comply with international data protection regulations, including GDPR.

Change Management

Gemini Data follows controlled, documented processes to monitor changes to systems and applications. This includes risk assessments, testing, approvals, and rollback plans. We use automation and infrastructure-as-code to reduce human error and ensure consistent, secure deployments. In addition, CI/CD pipelines include security gates and change windows to minimize business disruption.



LOGGING, MONITORING, AND RESPONSE

Gemini Data maintains comprehensive logging of user activity, system changes, and security events to enable effective monitoring and threat detection.

Logs are retained in tamper-proof storage and reviewed regularly using security information and event management (**SIEM**) tools. Additionally, machine learning models assist in detecting anomalies and triggering alerts, allowing rapid incident triage.









Our **24/7 Security Operations Center (SOC)** handles incident detection and response. In the event of an incident, Gemini Data maintains a formal incident response plan that defines roles, communication protocols, and remediation steps.









Regular drills and coordination with customers ensure preparedness and rapid recovery from security incidents. Every incident is documented, reviewed afterward, and used to strengthen future prevention and response strategies.

CONCLUSION

Security is a shared responsibility between technology vendors and their customers. By adopting and operationalizing these best practices, we strive to build and maintain trust while enabling secure, scalable, and compliant cloud services for our clients.

To learn more about how Gemini Enterprise can help your organization meet its security goals, contact us or request a demo at geminidata.com.

	Hardened virtual machines
	Firewalls and intrusion prevention systems (IPS)
	Network segmentation
	Continuous system monitoring
	Role-based access controls (RBAC)
	Multi-factor authentication (MFA)
	Periodic access reviews
	Data segregation, containerization, and namespace isolation

	Restricted employee access to customer data
	Full disk encryption
	Key management systems with customer-managed keys
	Industry-standard encryption (including NIST and ISO/IEC 27001)
	Industry-standard data processing (including TLS 1.2+ and AES-256)
	Secure asset management and disposal (GDPR compliant)
	Controlled, documented monitoring of system and application changes
	24/7 SOC handling incident detection and response

About Gemini Data

Our mission is to redefine how data is used, analyzed, and shared. We've built the world's simplest enterprise AI assistant platform to help companies all over the world connect the dots and get answers faster, respond to unusual events, and take the next best action.

© Gemini Data, Inc.

geminidata.com

+1 800 549 7888

Amsterdam | Irvine | San Diego
San Francisco | Taipei | Tokyo