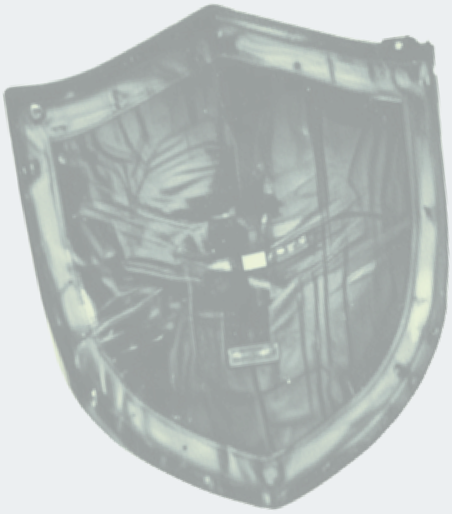
AlgoVerde Platform Security



■ An Overview

AlgoVerde transforms product development and market intelligence with cutting-edge AI solutions. **Trusted by Fortune 500 companies**, our platform enables businesses to ideate, test, and validate product concepts faster and with greater confidence.
Algoverde was designed with robust security as a top priority. **Security is paramount** both at the application and user levels.

Cloud-Based Deployment

AV is hosted on Amazon Web Services (AWS) and complies with the latest standards and best practices adopted by leading enterprise applications, including Salesforce and Microsoft 365. No components of the AV infrastructure are hosted at AlgoVerde corporate offices, nor does AlgoVerde store customer data on its premises.

User Authentication

To safeguard data security and integrity, AV requires the creation of user profiles with secure and unique login credentials. Only authorized individuals who have been explicitly invited to the platform are granted access to AV. This ensures tight control over platform usage and prevents unauthorized access.

Role-Based Access

AV enables customers to define user roles and permissions with precision within each innovation space. This role-based access control provides granular management over which users can access specific workspaces, ensuring sensitive information remains secure and confidential.

Firewall

AV applies a multi-layered firewall architecture, including AWS firewalls and AV-specific firewalls, to protect user data. Additionally, AV can be configured to ensure that all user data resides exclusively within the boundaries of a company's internal firewall, providing an added layer of control and security for customers.

Certifications

AlgoVerde has obtained **SOC2 Type 1 certification** and is in the process of obtaining **SOC2 Type 2 certification**, in addition to **ISO27001 certification**.

Data **Security**

AV is deeply committed to safeguarding the integrity and confidentiality of customer data. Our approach to data security is based on:

- **Dedicated Instances:** Each customer is provided with a dedicated software instance, functioning as an isolated workspace. This ensures that no customer data is ever shared with other customers.
  All internal work, including prompts and responses, is fully contained within a secure customer instance.

- **Data Obfuscation:** Using an embedding integration process, only the obfuscated (tokenized) representation of the data is maintained on the AV platform,ensuring both data confidentiality and security.

- **Data Encryption:** The data encryption includes disk encryption and database encryption. Encryption keys are managed by and stored securely in AWS. AV personnel do not have access to the encryption keys. All key usage is logged and monitored for anomalous activity.This process provides protection against unauthorized access, theft, and data breaches.

- **Data Retention Policy:** AV retains customer data only for the duration of the agreement. Following termination, data is retained in accordance with AV's Data Retention Policy, unless it receives a written data deletion request. AWS is responsible for ensuring the proper sanitization of disks and physical media. AV sanitizes employee laptops prior to reuse or disposal.

- **AV GenAI Twins:** GenAI Twins are proprietary to a company and will never be shared with anybody beyond the permissions dictated by that company.

- **AV Workflows:** As with all other data, the tailored workflows developed by AlgoVerde for custom deployments are protected by the same level of security.

Integration with **External AI Models**

The AV platform is designed to deploy a **combination of open-source LLMs** (private instances) **and external AI models**, such as ChatGPT, Claude, and others. When external models are utilized, AV notifies users of any potential security concerns and implements the highest security measures available. Additionally, **it can integrate a company's private instance** of ChatGPT, Gemini, Claude, or any other proprietary models developed in-house.
In case these models are used, AV notifies users of any possible security concerns and utilizes the **maximum security measures** allowed by these third-party models. It can also **integrate a company's private instance** of ChatGPT, Gemini, Claude, or other.

Confidentiality Agreement with **Employees**

Security of the AV environment is the shared responsibility of all AV employees and contractors who have access to AV's information systems. No AV employee is able to access a company's Innovation Space or proprietary data unless specifically invited by the company itself. **Employees and contractors must also sign a confidentiality agreement**, the employee handbook, **and AV's security policies**.

Customer's **Responsibilities**

While AV is responsible for the vast majority of the security controls implemented to secure customer data and the application, our **customers are responsible for securing their user accounts**. This includes creating strong passwords, provisioning user accounts and permissions, and disabling accounts as needed. Additionally, **customers are responsible for determining the appropriateness of the data entered into the application**.