Whitepaper

Security at Jasper

The technology and processes behind our enterprise-ready AI content platform, and exactly how Jasper keeps your data private.

jasper

Introduction

Jasper is the future of marketing content creation. We are committed to providing a highly available and secure environment for you to create content. This whitepaper highlights our security practices to help you understand how we ensure security by design.

Protecting your data is our top priority

Jasper's Security team, led by our Directory of Security, is responsible for implementing and managing our security program. The focus of Jasper's security program is to prevent unauthorized access, use, and disclosure of customer data. Our security program is aligned with AICPA Trust Services Principles and is constantly evolving in accordance with industry best practices.

Independent attestation

Customers may self-serve copies of Jasper's SOC2 report, penetration test report, as well as all other available documentation from our Compliance Portal: security.jasper.ai.

Security compliance

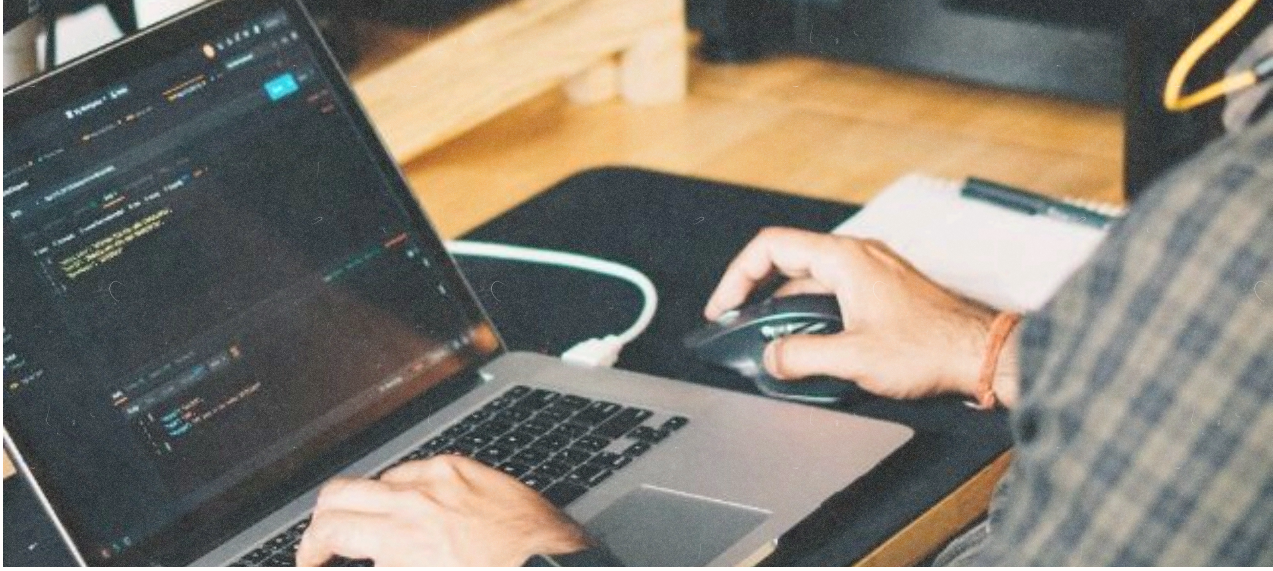
Jasper is continuously monitoring and improving upon the design and effectiveness of our security controls. We partner with a reputable third party for their independent assessment of our efforts. All internal and external audit findings are shared with executive management.

Penetration testing

Jasper engages an independent third party to conduct annual network and application penetration tests. Identified findings are tracked to resolution, and results reports are shared with executive management.

Jasper's responsibility

Policies & practices for protecting your data



Access control

When provisioning access, IT adheres to the principles of least privilege and role-based access control, meaning that employees are only authorized the access and permissions required to fulfill their job responsibilities. User access reviews, including production access, are performed semi-annually. Access to the production infrastructure and supporting systems requires MFA.

Employee access is revoked within two business days of an employee's termination. In the event of involuntary termination, access is revoked immediately.

Cloud hosting

Jasper uses GCP as its cloud hosting provider. The Jasper application is hosted across multiple availability zones in the US-East1 and US-East4 regions for increased redundancy. Jasper utilizes serverless instances across GCP to ensure high availability of all services. Kubernetes node components are hardened and have a base configuration image applied.

Jasper is a remote company and does not have any corporate offices.

Data retention

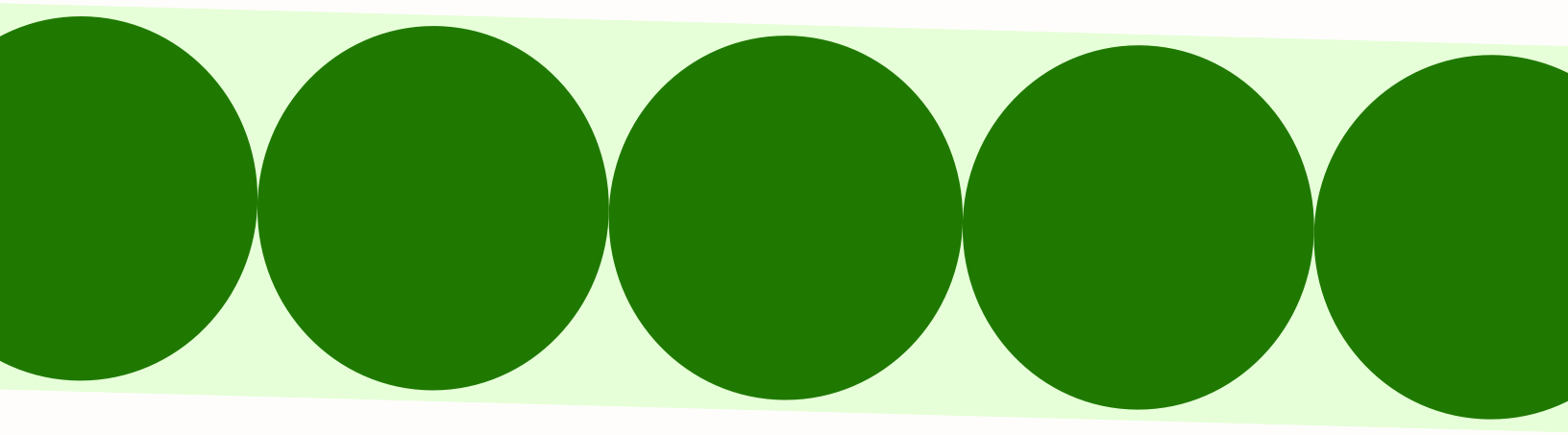
Jasper retains customer data for the duration of the agreement in order to provide the services. Following termination, data is retained in accordance with Jasper's Data Retention Policy, unless Jasper receives a written data deletion request.

Jasper's hosting provider, GCP, is responsible for ensuring the proper sanitization of disks and physical media. Jasper sanitizes employee laptops prior to reuse or disposal.

Encryption

Jasper encrypts all customer data at rest and in transit using strong encryption methods. All information is transmitted via HTTPS using TLS1.2+ with AES256 encryption and SHA2 signatures, defaulting to TLS1.3 based on client ability. Data at rest is encrypted at the storage level using AES256. Database connections are verified using TLS certificates, and encrypted in transit using SSL.

Encryption keys are managed by and stored securely in GCP. Jasper personnel do not have access to the encryption keys. All key usage is logged and monitored for anomalous activity.



Endpoints

Employees are provisioned company-managed workstations. Employees are not permitted to use their personal devices for work (e.g., BYOD). All workstations are configured with disk encryption, anti-malware, password protection, idle lockout, and automatic OS updates. IT monitors employee workstation for deviations to ensure they are compliant with corporate policy.

Logging

Centralized logging is enabled for all production systems. These logs are reviewed for indications of compromise and alerted upon. The Security team is responsible for monitoring and alerting thresholds are reached, tracking security events to resolution in accordance with the incident response plan.

Network

Jasper's firewalls are configured to deny all incoming traffic by default. Firewall rules are reviewed at least annually. Alerts generated by the Intrusion Detection System (IDS) are sent to on-call personnel for investigation and triage. Jasper also utilizes a WAF and CDN in order to both protect against common web application vulnerabilities, like DDoS attacks, and to provide faster access to the application.

Personnel

Security of the Jasper environment is the shared responsibility of all Jasper employees and contractors who have access to Jasper's information systems. Prior to their start date, all employees and contractors must have a completed background check on file, as legally permissible. Employees and contractors must also sign a confidentiality agreement and Jasper's security policies.

All employees are required to complete security awareness training upon hire and annually thereafter. Training curriculum includes phishing awareness, remote work best practices, device security, and incident reporting. Developers are required to complete additional training scoped to secure coding practices.

Violations of any corporate policies may result in disciplinary measures up to and including termination.

Secure development

Jasper has built a secure software development lifecycle (SDLC), including requirements like independent peer code review and automated testing. Non-standard changes go through a change management process that covers emergency changes and hotfixes. The agile nature of the process allows for engineers to follow their own release cycles, deploying continuous improvements to the Jasper application.

All code is managed in a version control repository, with branch protections in place. SAST and DAST are also in place. Access to source code requires MFA.

Third parties

Jasper partners with third parties to provide key services. Third parties that handle customer personal data, also known as sub-processors, are continuously monitored in order to ensure that their security programs continue to meet Jasper's standards. Jasper reassesses its subprocessors annually, which includes a review of their independent audit reports and penetration test reports. For the full list of Jasper's subprocessors, please see legal.jasper.ai/#sub-processors.

Vulnerability management

Internal and external vulnerability scans are performed weekly. Identified vulnerabilities are remediated in accordance with severity.

Your responsibility

Though Jasper is responsible for the vast majority of the security controls implemented to securing customer data and the application, our customers are responsible for securing their user accounts. This includes creating strong passwords, provisioning user accounts, managing permissions, and disabling accounts as needed.

Additionally, customers are responsible for determining the appropriateness of the data entered into the application. By default, Jasper handles limited sensitive information (end-user name and email). The sensitivity of the data that customers input to generate content is ultimately their responsibility. Customers should refrain from providing cardholder information (CHD), protected health information (PHI), and other types of highly sensitive data.

Conclusion

Ensuring the security and privacy of customer information is vital to our company mission. The success of our customers is at the core of what we do.

We hope this insight into our security program helps to build and maintain your trust in Jasper.

Want to get in touch?

Phone	(650) 600-3985
Email	hey@jasper.ai