grammarly

Security at Grammarly

Whitepaper

Contents

Introduction

Grammarly's AI-powered products help people communicate more effectively. Millions of users rely on Grammarly every day to make their messages, documents, and social media posts clear and impactful. Grammarly is one of the world's fastest-growing consumer software companies with over 20 million daily active users and $110M raised from top-tier Silicon Valley venture capital firms, including General Catalyst, Institutional Venture Partners, and Spark Capital. Grammarly has offices in San Francisco, New York, and Kyiv.

Grammarly's client applications are powered by secure infrastructure in the cloud to ensure fast and reliable processing. We're continually evolving our product and architecture to speed up text processing, improve our algorithms, and safeguard user data. Maintaining customer trust is critical for our mission, and we consider security and our users' privacy a top priority. In this document, we aim to help you understand our high-level system architecture and our approach to security.

Architecture overview

In this section, we'll explain how user content is transferred, stored, and processed securely by Grammarly infrastructure in the cloud.

Client applications

Grammarly provides a range of client apps for various communication platforms:

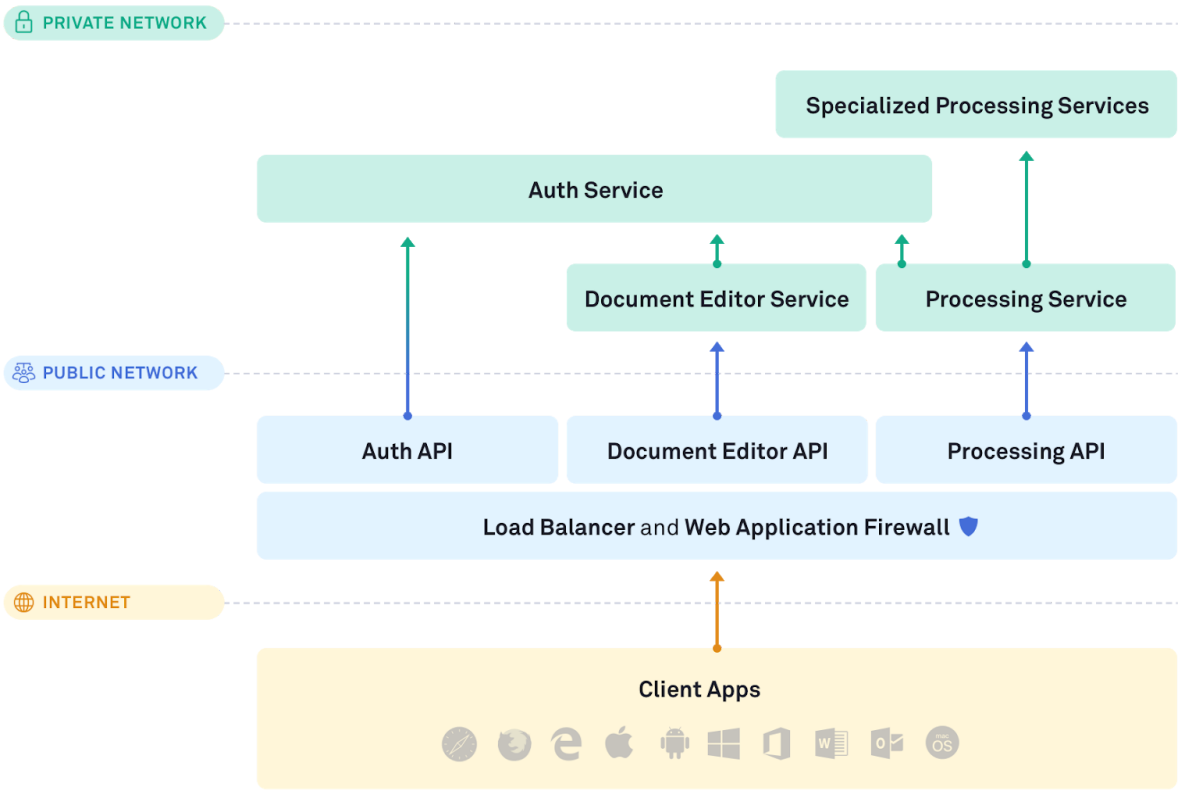
- Browser extensions for Google Chrome (including Google Docs), Apple Safari, Mozilla Firefox, and Microsoft Edge
- Grammarly Microsoft Office Add-in (Windows)
- The Grammarly Editor for all major browsers
- Desktop apps for Windows and Mac
- The Grammarly Keyboard for iOS and Android

All Grammarly server-side infrastructure is hosted in an industry-leading secure cloud platform hosted by Amazon Web Services (AWS) in the United States. Only a small number of Grammarly's servers and network ports are accessible from the Internet, and are behind load balancers and a web application firewall. All components that process user data operate in Grammarly's private network inside our secure cloud platform.

Text processing infrastructure

Grammarly's text processing infrastructure comprises the following main components:

- **Authentication Service** that authenticates Grammarly users by login/password or social sign-on with Google or Facebook
- **Document Editor Service** in which users can create, edit, and save documents via the Grammarly Editor or desktop apps
- **Processing Service** that manages connections from all client apps (such as the browser extension and mobile keyboard), providing writing corrections and suggestions by Grammarly



Data encryption and isolation

Data is encrypted in transit and at rest:

- Connections between the client apps and the backend infrastructure are protected by up-to-date encryption protocols (including SSL/TLS 1.2) while maintaining compatibility with the cipher suites the client supports.
- All databases, data storage, and backups are encrypted at rest using the industry-standard AES-256 algorithm.

Each Grammarly user's data is segregated logically from other users' data. A user must be logged in to his or her Grammarly account and any client request must be authenticated and authorized in order for the user to access his or her data.

Organizational security

Security policies and training

Grammarly's employee security practices apply to full- and part-time employees and contractors who have access to Grammarly's internal systems or have access to Grammarly's offices.

Before gaining access to internal systems, all employees must agree to Grammarly's Internal Data Security and Privacy Policy. All employees are required to complete privacy and security training annually. The training covers a wide range of privacy and security topics, including acceptable data use, phishing and social engineering, use of company-owned devices, best practices to prevent malware, requirements around physical security, and incident reporting.

Upon termination of work at Grammarly, the former employee's access to Grammarly systems is removed immediately by the IT department using a standardized procedure, including disabling all accounts.

Grammarly's security program

Grammarly employs a professional security team — comprising in-house employees and retained security consultants — who own and run Grammarly's security program. We support the three pillars of our security program through a variety of initiatives and best practices:

- Product security
    - Train developers on secure application development practices and security
    - Provide design and code reviews for detection of possible security flaws
    - Manage Grammarly's public bug bounty program
- Infrastructure and operations security
    - Manage firewalls, website certificates, and other pieces of security infrastructure
    - Gather security-relevant logs and maintain tools for logs analysis
    - Provide a platform for secure deployment, monitoring, and patching of Grammarly's production services
    - Manage endpoint device protection tools and services
- Compliance and risk management
    - Coordinate penetration testing
    - Manage tools for vulnerability scanning
    - Coordinate audits and maintain security certifications
    - Follow predetermined incident reporting protocols
    - Respond to customer inquiries

- Review and qualify vendor security posture

Penetration testing and bug bounty program

Grammarly initiated a private bug bounty program with HackerOne in September 2017 and launched its public program in December 2018. Grammarly runs a successful public bug bounty program for security vulnerabilities and commits to high response efficiency for triaging and resolving bug reports. Customers wishing to conduct their own penetration tests of Grammarly's applications may request to do so and should contact their Grammarly account representative. More information about Grammarly's bug bounty program, including our response efficiency, is available on our HackerOne program page.

Secure software development

Grammarly's development and platform teams use industry-leading managed services for roles and access policies, account management, certificate management, encryption and keys management, secrets management, security logs collection and monitoring, firewalls and network access lists. All code is checked into a version control system. Code changes undergo peer review and automatic integration testing. Grammarly applications, libraries, and other development artifacts are automatically scanned for known vulnerabilities, and the fixes are applied promptly. Every development team has a regular cadence of security check-ins with the security and platform team.

Protecting customer data

Authorizing employee access

Access to all Grammarly internal systems requires employees to authenticate. Authentication to internal systems is managed via a single-sign-on system with mandatory 2-factor authentication. Only company-managed devices can connect to the Grammarly corporate network.

Grammarly adheres to the principle of least privilege. Requests to access internal systems are documented and approved by the respective managers and service owners. Grammarly management systematically reviews employees' access to the systems that hold or process customer data and revokes access if access is no longer needed to perform the work.

Legal compliance

Grammarly complies with the EU General Data Protection Regulation (GDPR) as well as the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. For more details, see Grammarly's Privacy Policy.

Grammarly employs dedicated legal and privacy counsel with extensive expertise in data privacy and security. These professionals review Grammarly products and processes for compliance with applicable legal and regulatory requirements.

Customer data privacy

Grammarly respects the privacy of user data, as specified in Grammarly's Privacy Policy. Committed to the GDPR principles, Grammarly never collects Personal Data without a lawful basis, limits the amount of collected and processed data, and deletes the data when it is no longer needed for the services outlined in Grammarly's Privacy Policy (e.g., to provide and improve our services). Users can request a Personal Data report through this link. Grammarly users can remove their Personal Data from Grammarly at any time by logging into their account, accessing the Settings page, and then deleting their account. Enterprise customers can contact their account representative for deletion.

Grammarly has a set of policies and technical controls that prevent employees from accessing customer data that is stored or processed by Grammarly systems. Access to production systems is restricted to dedicated engineers who develop these systems and ensure their reliability and uptime. Production systems that work with user content are deployed in a separate infrastructure isolated from all other Grammarly services. Where appropriate, Grammarly uses private keys and restricts network access to particular employees.

While Grammarly may track anonymized, aggregate statistics by website domain, Grammarly doesn't collect browsing history from specific users while they browse the web. During a text editing session using the browser extension, Grammarly needs to know the website domain to enable or disable domain-specific services and writing suggestions. Information such as web server access logs or IP addresses is collected only for a limited time and only to provide specific services to the user, such as fraud prevention.

Third-party vendors

Grammarly relies on a number of third-party vendors for specific services and functions, such as hosting our servers, email communication, customer support services, and analytics. Prior to using a third-party vendor, Grammarly evaluates the vendor's security posture. Grammarly ensures that personal information is removed from third-party systems after there is no longer any legal basis for its storage, per GDPR mandates. Note that Grammarly does not sell or rent users' personal data nor share personal data with third parties to enable them to deliver their advertisements.