Security at Grammarly

Whitepaper

AS OF JULY 31, 2020

Contents

Introduction

Grammarly's AI-powered writing assistant helps more than 20 million people write more clearly and effectively every day. In building a product that scales across multiple platforms and devices, Grammarly works to empower users whenever and wherever they communicate.

Across global offices—from its headquarters in San Francisco to offices in Kyiv, New York, and Vancouver—Grammarly's values-driven team collaborates to support our expanding user base and to work toward developing our writing assistant into a truly comprehensive communication partner. Our growth and further investment in cutting-edge language research have been helped along by more than $200 million in funding, led by General Catalyst.

Grammarly's client applications are powered by secure infrastructure in the cloud to ensure fast and reliable processing. Since the software's first release, in July 2009, we have continually improved our product and architecture to speed up text processing, improve our algorithms, and safeguard user data. Maintaining customer trust is critical for our mission of improving lives by improving communication—security and user privacy are of the highest priority.

In this document, we aim to explain 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, Apple Safari, Mozilla Firefox, and Microsoft Edge (including tailored integration for Google Docs)
- Grammarly for Microsoft Office (add-in on Windows and macOS)
- The Grammarly Editor (for all major browsers)
- Native desktop apps (for Windows and macOS)
- The Grammarly Keyboard (for iOS and Android)
- Grammarly for iPad (Grammarly Keyboard/Grammarly Editor integration)

Core infrastructure

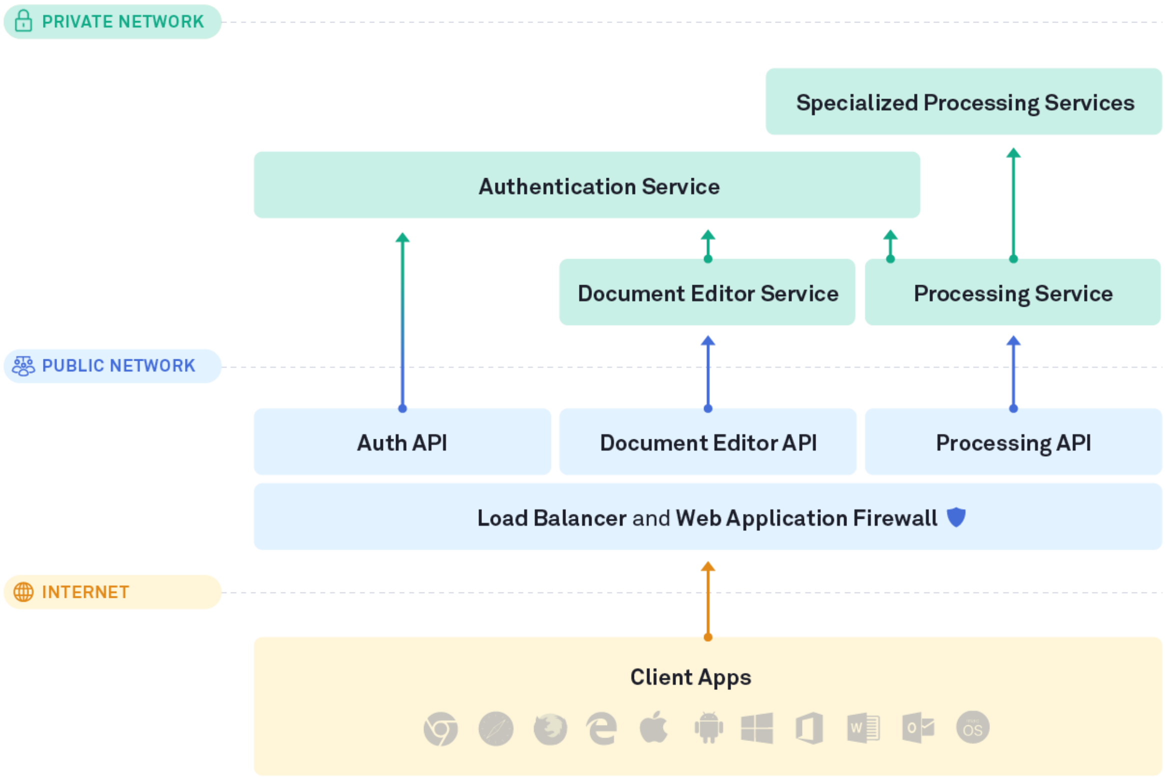
All Grammarly server-side infrastructure is hosted in an industry-leading secure cloud platform through Amazon Web Services (AWS) in the United States, primarily in the US East region (North Virginia), with a secondary site located in the US West region (Oregon). Only a small number of Grammarly's servers and network ports can be accessed through the internet, and these are behind load balancers and a web application firewall (WAF). All components that process user data operate in Grammarly's private network inside our secure cloud platform.

Grammarly is registered for AWS Enterprise Support, the highest possible tier of AWS support. This means Grammarly receives the fastest possible AWS response levels along with weekly review by AWS technical account managers, who assist with support issues and provide proactive operational guidance.

Text processing infrastructure

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

- **Authentication Service** that authenticates Grammarly users by login and password, SSO via SAML, or social sign-on with Google or Facebook
- **Document Editor Service** through 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 the mobile keyboard) and provides Grammarly's writing suggestions



Data encryption and isolation

Data is encrypted in transit and at rest:

- Connections between client applications and the back-end Grammarly infrastructure are protected by up-to-date encryption protocols, including TLS 1.2.
- Grammarly customer data is encrypted at rest in AWS using AES-256 server-side encryption.
- Passwords are stored in encrypted databases with applied bcrypt hashing.
- Grammarly utilizes AWS Key Management Services (KMS) for database encryption and key management. Access to the cryptographic keys is restricted to authorized personnel.

Each Grammarly user's data is segregated logically from other users' data. A user must be logged in to their Grammarly account—and any client request must be authenticated and authorized—in order for the user to access their 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 pass background checks and agree to Grammarly's Acceptable Use Policy, Internal Data Security, and Privacy Policy. All Grammarly employees complete privacy and security training during onboarding that covers topics such as data privacy, physical security, data and information security, and incident reporting.

Upon termination of work at Grammarly, a 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 and team

Grammarly employs a team of security professionals—comprising in-house employees and retained security consultants—who oversee and run Grammarly's security program. This team supports 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 other best security practices
    - 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 log analysis
    - Provide a platform for secure deployment, monitoring, and patching of Grammarly's production services
    - Manage endpoint-device-protection tools and services
    - Coordinate external penetration testing

    - Conduct ongoing vulnerability assessments
    - Respond to security incidents
- Compliance and risk management
    - Coordinate audits and maintain security certifications
    - Develop and maintain Grammarly's information security management system
    - Respond to customer inquiries
    - Review and qualify vendor security posture
    - Coordinate BCP/DRP activities
    - Manage privacy program

To effectively execute its security program, Grammarly has a dedicated Security team, which consists of trained specialists in the following areas:

- Application Security (AppSec)
- Security Operations (SecOps)
- Governance, Risk, and Compliance (GRC)

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.

A third party is engaged annually to conduct an external network penetration test as well as an AWS security and corporate infrastructure security assessment. The findings from the third-party security assessments are reviewed by the Security team, categorized by their severity, and tracked to resolution.

Vulnerability assessment

Grammarly's Security team performs vulnerability assessments of Grammarly services as follows:

- Services before deployment to production are verified with a software composition analysis (SCA) service.
- AWS infrastructure is scanned continuously using native AWS security tools, such as Inspector, GuardDuty, Macie, and others.
- Public-facing web services are scanned continuously by web-application scanners.
- Post-release vulnerability assessments are performed by various vulnerability-management solutions.

Patch management

Grammarly regularly applies security patches to service infrastructure. The IT team subscribes to regular feeds and channels dedicated to notifications of critical updates for the asset types used at Grammarly. Critical patches are applied as soon as reasonably possible according to Grammarly's Patch Management Procedure.

Security monitoring

Grammarly uses a set of instruments and processes for the detection of malicious, suspicious, or otherwise illegitimate actions within its own infrastructure, services, and applications. The company logs and retains administrative access, use of privileged accounts, and system calls on service critical servers in Grammarly environments. Analysis of these logs is automated when practical to detect potential issues and alert responsible personnel. Access to audit logs is restricted to the limited number of personnel who require this access to conduct their duties.

Incident management

Grammarly executes procedures for incident management that minimize downtime, service degradation, and security risks to customers and internal users.

Security events are identified and communicated to Grammarly's Security team through established channels. The Security team then defines the type of event, establishes its severity, and responds to it according to approved service-level agreements (SLAs) based on industry best practices. Security events that may impact privacy are subject to additional analysis and response by Grammarly's Legal team.

Secure software development

Grammarly's engineering and platform teams use industry-leading managed services for roles and access policies, account management, certificate management, encryption and key management, secrets management, security logs collection and monitoring, firewalls, and network access lists. All code is checked in 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 fixes are applied promptly.

Every development team has a regular cadence of security check-ins with the Security team and the Platform team, which is responsible for providing an optimal infrastructure toolkit to help engineers focus on product development.

Grammarly's services are designed, developed, deployed, and tested against known security vulnerabilities, including those listed by the Open Web Application Security Project (OWASP). Guidelines for secure development and testing are maintained and communicated to all engineers.

Disaster recovery

Grammarly uses services deployed by its cloud hosting provider, AWS, to distribute production operations across multiple availability zones located on the east and west coasts of the US.

Grammarly has a General Disaster Recovery Plan (DRP) to guide teams to recover after disruptions caused by unexpected events in compute capacity, applications, infrastructure, or data. The General DRP is maintained by dedicated teams at Grammarly and is reviewed and tested annually.

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 executes a due diligence program and evaluates the vendor's security posture. Grammarly validates that personal information is removed from third-party systems after there is no longer any legal basis for its storage.

Selected third parties are subject to continuous monitoring by a vendor-risk-management service. A list of the most significant third parties used by Grammarly can be found here.

Business model

Grammarly does not sell or rent users' personal data or share personal data with third parties to enable them to deliver advertisements. Grammarly only makes money by offering a paid product to consumers and businesses.

Protecting customer data

Authorizing employee access

Access to all Grammarly internal systems requires employees to authenticate via a single-sign-on system with mandatory multi-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, reviewed, 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 specific work tasks.

Endpoint protection

All Grammarly workstations are required to run endpoint-management software that enforces secure configurations, password rules, and encryption. It also facilitates a lock-when-idle function and allows for control to be taken remotely if a device is compromised or lost. Employee workstations run monitoring agents from an industry-leading vendor to detect possible malware and suspicious behaviors. Grammarly's Security team collects device logs and monitors workstation alerts.

Legal compliance

Grammarly complies with the EU General Data Protection Regulation (GDPR) for the collection, use, and retention of personal information. For more detail, see Grammarly's Privacy Policy.

Grammarly employs dedicated legal and privacy counsel with extensive expertise in data privacy and security. These professionals review Grammarly product offerings 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's systems 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 systems. Where appropriate, Grammarly uses private keys and restricts network access to particular employees.

While Grammarly’s product may track anonymized aggregate statistics by website domain, it doesn’t collect browsing history from specific users while they browse the web. During a text-editing session using the browser extension, Grammarly services need to know the website domain to enable or deactivate 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.

Processed and stored data

Documents that users save in the Grammarly Editor (https://app.grammarly.com) are stored by Grammarly so users can access them again when desired. Documents are stored until they are deleted by the user through the Grammarly Editor.

Grammarly services access only the text written while using a Grammarly client application. Additionally, Grammarly is blocked from accessing anything typed in text fields marked "sensitive," such as credit card forms or password fields.

Data retention and disposal

Deleting documents from the Grammarly Editor will permanently delete them from our systems. Customer data is deleted immediately from production services upon user deletion. Grammarly deletes user’s texts from backups 14 days after their removal from the Editor. During this period, deleted documents could be reviewed and restored by the user by navigating to their document version history.

Grammarly’s hosting service provider is responsible for ensuring that the removal of data from disks is performed in a responsible manner before they are repurposed.

Account deletion

Enterprise customers and individual users have the ability to end their Grammarly subscription at any time. At the end of an enterprise subscription, any documents stored in the Grammarly Editor are deleted from end user accounts, which become free Grammarly accounts. In accordance with the Privacy Policy, when an individual user deletes their account, the user's personal data is deleted from the internal and external services.

In certain limited circumstances, Grammarly may retain data to comply with legal obligations and for fraud detection and prevention.

Conclusion

We know that security is of the utmost importance to you, and keeping data secure is a responsibility we take incredibly seriously. Please contact Grammarly support or your Grammarly account executive if you have any questions regarding Grammarly's security.