Wrike

Security overview

Last update: March, 2019. Wrike, Inc.

Wrike is the leading collaborative work management platform helping organizations around the globe align work with the most important business objectives, create new efficiencies, and drive results.

We are dedicated to making our Wrike the most secure and reliable collaborative work management platform on the market. We are committed to protecting your personal and company data, and ensuring secure collaboration within our platform, which is why we continue to invest in the security of our services to not only meet, but exceed industry standards.

Security has always been a top priority and we have relentlessly pursued a robust and mature security strategy since the day the company was founded in 2006. Below is an overview of Wrike's security strategy, which includes a comprehensive approach across five key categories: Physical, network, system, application, and people.

Physical security

Global Presence

Wrike hosts its mission-critical servers in dedicated cages within data centers located in the US and EU:

- Coresite, our primary datacenter in the US is ISO 27001, SOC1, and SOC2 compliant. The facility is located in San Jose, California.
- Wrike's Primary European Data Center is located in Amsterdam, Netherlands and is compliant with ISO 27001 as well as ISAE 3402 standards (an equivalent to SSAE 16). This data center is specifically isolated for EU customers and their data.

These facilities feature 24/7 manned security, fully redundant power backup systems, physical access controls, biometric authentication systems, extensive seismic bracing, the latest in early-detection smoke and fire alarms, and digital surveillance systems. All server and network components are continuously monitored by internal Wrike staff and by the colocation providers.

Wrike's Disaster Recovery infrastructure resides in Google's Cloud Platform for both the US and EU regions, having great scalability and security with SSAE16 / ISAE 3402 Type II, ISO

27001, FedRAMP, PCI DSS, and HIPAA and other certifications.

Access to each system, network device, and application is limited to authorized personnel, and login details within the event logs are reviewed on a continual basis..

Uptime Over 99.9%

Over years of continuous service, Wrike has consistently met or exceeded a 99.9% uptime, ensuring customers can access their tasks and projects when needed without interruption. If Wrike is temporarily unavailable due to technical reasons or scheduled maintenance, you can log in to the standalone, read-only replica of Wrike to access all your data at https://read.wrike.com, or https://read-app-eu.wrike.com for European customers.

Continuous Data Backup

Wrike's data backup model provides near real-time database replication to ensure customer data is both backed up and available on redundant and geographically dispersed servers. Full backup is performed on a daily basis and is stored encrypted in an environment physically separated from the primary servers to ensure fault tolerance.

Network and System Security

Tenable Network Security Infrastructure

Wrike uses industry-standard network protection procedures, including network segregation using VLAN's, firewall and router technologies, intrusion detection and prevention systems, centralized log aggregation, and alert mechanisms. These procedures are used in conjunction with secure connectivity, including secure channels and multi-factors for authorized systems operations group personnel. This allows us to prevent, detect, and promptly remediate the impact of malicious traffic and network attacks.

Regular Updates and Patch Management

Ongoing internal network security audits and scanning gives us an overview for quick identification of impacted systems and services. According to our in-house patch management policy, operating systems, software, frameworks, and libraries used in Wrike infrastructure are updated to the latest versions on a regular basis. Whenever a vulnerability in a product used by Wrike or a high or critical vulnerability is publicly reported, prompt actions are taken to mitigate any potential risks for our customers — we apply hotfixes and patches promptly when available and/or implement pro-active mechanisms like configuration of firewalls or IDS/IPS.

System Integrity Protection

Wrike uses operating system-based and custom integrity check services to ensure the integrity of all critical files and system objects. A quick response to any potential unauthorized changes to the system helps insure our customers are using Wrike-approved application services.

Application Security

Application Security Process

An in-depth Application Security Lifecycle process is fully integrated into Wrike's Software Development Lifecycle (SDLC), including:

- Defined in-house security requirements, policies, and industry security best practices applied in every stage of the lifecycle.
- Ongoing security review of architectures, design features, and solutions.
- Iterative manual and automated (using static code analyzers) source code review for security weaknesses, vulnerabilities, and code quality, plus development team advisory and guidance.
- Regular manual assessment and dynamic scanning of pre-production environment.
- Security trainings conducted for IT teams according to their respective job roles.

User Authentication

Each user in Wrike has a unique, password-protected account with a verified email address. The password is validated against password policies and stored securely using a strong hashing algorithm with a unique salt for every password. 2-Factor Authentication is available as an additional security measure to protect Wrike accounts. Wrike also supports multiple methods of federated authentication, including Google Open ID, Azure, Office 365, ADFS and SAML2 to conveniently and securely gain access to a Wrike account leveraging corporate credentials. Wrike also offers advanced security settings that allow customers to manage Network Access Policy and Password Policy. More details can be found in our Help Section.

The Wrike Support Team is always happy to assist you with any Wrike-related issues. If troubleshooting or verifying an issue requires support to access your account, that access can be granted only by you. This is enabled by a system-generated security token that you provide to our support team, allowing support to delve deeper into solving your problem for a limited amount of time. This systemic approach ensures additional confidentiality for your data stored in Wrike.

Data Sharing and Role-Based Access Control

A Wrike account administrator manages and controls individual user rights by granting specific types of user licenses. Details about various user licenses, roles, and authorization controls in Wrike are documented in our Help Section.

Customer data, including tasks and folders, can only be accessed by other users within your Wrike account if those items were specifically shared with them, or if the items were placed in shared folders.

Wrike offers flexible data access control setup by allowing admins to configure Customized Access Roles, which offer the choice of more than 20 different permissions for user actions in Wrike, and can be used to specify user or group access levels to certain folders, projects and tasks. Selective sharing can be enabled to not follow the default of inheriting sharing settings, giving greater access control over specific subfolders and Subprojects. Wrike's Access Reports allow administrators to holistically review user access to sensitive data.

Monitoring User Activities

Wrike enables customers to get a report with up-to-date account activity information, including authentication events, changes in authorization and access controls, shared folders and tasks, and other security activities. The same report is available through a REST API that allows for integration with Security Information and Event Management (SIEM) and Cloud Access Security Broker (CASB) systems.

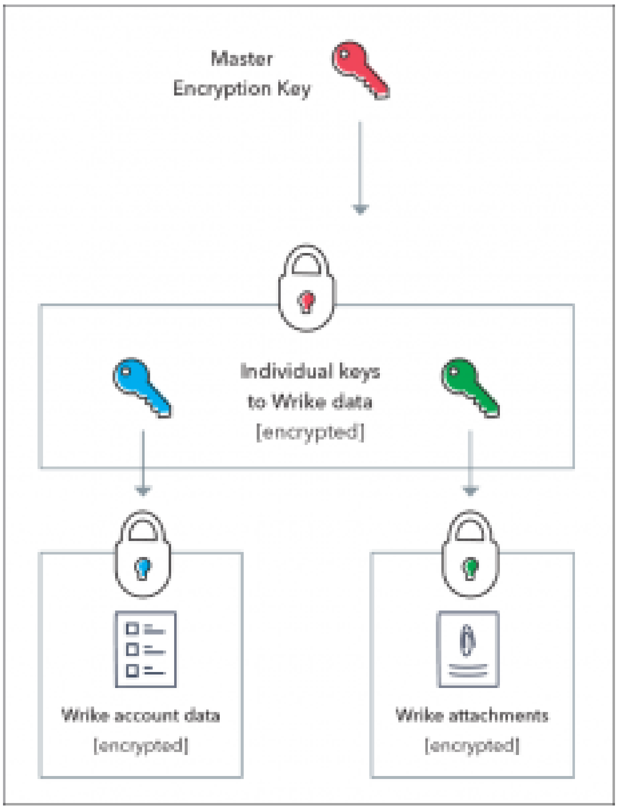
Data Encryption

Wrike uses Transport Layer Security (TLS) 1.2 with a preferred AES 256 bit algorithm in CBC mode and 2048-bit server key length with industry-leading modern browsers. When you access Wrike via web browser, mobile applications, email add-in, or browser extension, TLS technology protects your information using both server authentication and data encryption. This is equivalent to network security methods used in banking and leading e-commerce sites.

All users' passwords, cookies, and sensitive information are reliably protected from eavesdropping. User files uploaded to Wrike servers via both web application and API are automatically encrypted with AES 256 using per-file keys. If someone were to gain physical access to the file storage, this data would be encrypted and impossible to read directly. These encryption keys are stored in a secure key vault, which is a separate database decoupled from the file storage layer. In addition, all Wrike workstations and servers are encrypted at rest using file system encryption where AES 256-bit is used.

Wrike Lock

The Wrike Lock add-on for Wrike's Enterprise plan adds an additional layer of security by encrypting the encryption keys for Wrike workspace data (including tasks, folders, projects, workflows, and comments) and Wrike attachments with a master Customer-Managed Key (CMK), which is stored in Amazon Web Services' Key Management Service (AWS KMS). By using AWS KMS, the master encryption key is fully owned and controlled by the customer and stored outside of Wrike, and access to Wrike data can be monitored or revoked by the customer only. The following diagram demonstrates this:


Master Encryption Key
Individual keys to Wrike data [encrypted]
Wrike account data [encrypted]
Wrike attachments [encrypted]

Additionally, Wrike supports an emergency recovery procedure to decrypt Wrike data in the event a customer's master CMK is lost or unavailable. This is achieved by encrypting Wrike's data encryption keys with an asymmetric RSA key pair generated by the customer, where the public key is sent to Wrike to set up the procedure and the private key remains with the customer (the private key can be stored in a hardware security module).

Mobile Applications

Your Wrike workspace is accessible via Android and iOS applications, which inherit security functionality from Wrike's web-based application. These applications also have additional security features like encryption at rest, certificate pinning, checking against rooted/jailbroken devices, and application-level protections using a PIN code or fingerprint.

Account and Content Recovery

Wrike offers a backup tool which allows customer to make a backup of their data and download it to a local machine. Details about user-performed account backup can be found here.

You can also safely recover accidentally deleted items from Wrike's recycle bin. If a user is deleted by mistake, there is a possibility to recover the deletion (including some of their tasks) if you contact us within 3 business days. Some user account information can be recovered for up to a month after deletion.

People

Processes

Designing and running datacenter infrastructure requires not only technology, but also a disciplined approach to processes. This includes policies about escalation, management, knowledge sharing, risk management, and day-to-day operations. Wrike's security and operations teams have years of experience designing and operating data centers, and we continually improve our processes over time. Wrike has also developed best-in-class practices for managing security and data protection risk. All of these elements are essential parts of Wrike's security culture.

Need-to-Know and Least Privilege

Only a limited set of employees have access to our datacenter and the data stored in our databases. There are strict security policies for employee access, all security events are logged and monitored, and our authentication methods and data are strictly regulated. Access to production requires establishing a VPN channel, multi-factor authentication, a one-time password, and a personal certificate.

We limit access to customer data to employees with a job-related need, and require all these staff members to sign a confidentiality agreement. Accessing customer data is only done on an as-needed basis, and only when approved by the customer (i.e. as part of a support incident) via a support token, or under authorization from senior management and security for the purposes of providing support, maintenance, or improving service quality.

Privacy

Privacy Shield Framework

GDPR

The General Data Protection Regulation

Wrike has self-certified with US - EU Privacy Shield Frameworks, and is registered with the US Department of Commerce's Privacy Shield program as documented at www.privacyshield.gov. Wrike also provides a GDPR-compliant EU data center location focused on customer data within the EU. Additional details are available at www.wrike.com/privacy.

Compliance

AICPA SOC

bsi. ISO/IEC 27001 Information Security Management

STAR Security, Trust & Assurance Registry

Wrike is independently examined Type II SOC 2 covering for Security and Confidentiality principles, that shows our commitment to taking a mature, robust, and secure approach to products, processes, and security surrounding our customer data.

Wrike also has achieved ISO/IEC 27001:2013 certification, the scope of which covers the information security management system (ISMS) supporting information assets, development, and business operations. This ensures Wrike has an end-to-end security framework and a risk-based approach to managing information security, and illustrates Wrike's commitment to a mature and robust security strategy.

In addition, the result of our Security, Trust & Assurance Registry (STAR) Level One assessment is published on the Cloud Security Alliance (CSA) website.

Enterprise Grade Security

If you have any security questions and concerns, please contact our Sales team at **877-779-7453**, and they will provide you with additional security artefacts and external reports confirming our security maturity.