slack

Slack’s approach to security

Introduction

Slack is on a mission to make people’s working lives simpler, more pleasant, and more productive. To do that, we need to make sure your data is secure, and protecting it is one of our most important responsibilities. We’re committed to being transparent about our security practices and helping you understand our approach.

Organizational security

Slack has established an industry-leading security program, dedicated to ensuring customers have the highest confidence in our custodianship of their data. Our security program is aligned to the ISO 27000 standards and is regularly audited and assessed by third parties and customers.

Personnel security

Slack’s personnel practices apply to all members of the Slack workforce (“workers”)—regular employees and independent contractors—who have direct access to Slack’s internal information systems (“systems”) and / or unescorted access to Slack’s office space. All workers are required to understand and follow internal policies and standards.

Before gaining initial access to systems, all workers must agree to confidentiality terms, pass a background screening, and attend security training. This training covers privacy and security topics, including device security, acceptable use, preventing malware, physical security, data privacy, account management, and incident reporting.

Upon termination of work at Slack, all access to Slack systems is removed immediately.

Security and privacy training

During their tenure, all workers are required to complete a refresh of privacy and security training at least annually. They are also required to acknowledge that they’ve read and will follow Slack’s information security policies at least annually. Some workers, such as engineers, operators and support personnel who may have elevated access to systems or data, will receive additional job-specific training on privacy and security. Workers are required to report security and privacy issues to appropriate internal teams. Workers are informed that failure to comply with acknowledged policies may result in consequences, up to and including termination.

Dedicated security professionals

Slack has defined roles and responsibilities to delineate which roles in the organization are responsible for operating the various aspects of our Information Security Management System (ISMS). The responsibilities of each role are detailed in Slack's security documents.

At the center of administering our ISMS is Slack's Security Team. Slack has appointed a Chief Security Officer (CSO) with overall responsibility for the implementation and management of our ISMS. The CSO is supported by the other members of Slack's Security Team, which currently consists of over a dozen security professionals with more than 100 years of combined experience, focusing on Product Security, Security Operations, Computer Security Incident Response, and Risk and Compliance.

Together, these teams divide responsibilities for key aspects of Slack's security program, as follows:

- Product Security
    - Establish secure development practices and standards
    - Ensure project-level security risk assessments
    - Provide design review and code review security services for detection and removal of common security flaws
    - Manage Slack's bug bounty program
    - Train developers on secure coding practices
- Security Operations
    - Build and operate security-critical infrastructure including Slack's public key infrastructure, event monitoring, and authentication services
    - Maintain a secure archive of security-relevant logs
    - Consult with operations personnel to ensure the secure configuration and maintenance of Slack's production environment
- CSIRT
    - Respond to alerts related to security events on Slack systems
    - Manage security incidents
    - Acquire and analyze threat intelligence
- Risk and Compliance
    - Coordinate penetration testing
    - Manage vulnerability scanning and remediation
    - Coordinate regular risk assessments, and define and track risk treatment
    - Manage the security awareness program
    - Coordinate audit and maintain security certifications
    - Respond to customer inquiries
    - Review and qualify vendor security posture

All members of Slack's Security Team are active participants in the larger information security community to improve the overall state of the art of information security and to maintain their own expertise.

Policies and standards

Slack maintains a set of policies, standards, procedures and guidelines ("security documents") that provide the Slack workforce with the "rules of the road" for operating Slack's ISMS. Our security documents help ensure that Slack customers can rely on our workers to behave ethically and for our service to operate securely. Security documents include, but are not limited to:

- Fair, ethical, and legal standards of business conduct
- Acceptable uses of information systems
- Classification, labeling, and handling rules for all types of information assets
- Practices for worker identification, authentication, and authorization for access to system data
- Secure development, acquisition, configuration, and maintenance of systems
- Workforce requirements for transitions, training, and compliance with ISMS policies
- Use of encryption
- Description, schedule, and requirements for retention of security records
- Planning for business continuity and disaster recovery
- Classification and management of security incidents
- Control of changes
- Regular use of security assessments such as risk assessments, audits, and penetration tests
- Use of service organizations

These policies are living documents: they are regularly reviewed and updated as needed, and made available to all workers to whom they apply.

Audits, compliance, and 3rd party assessments

Slack operates a comprehensive information security program designed to address the vast majority of the requirements of common security standards. Please contact your Account Executive, or Support, for more information about the security standards with which Slack complies and to request copies of available reports and certifications.

Audits

Slack evaluates the design and operation of its overall ISMS for compliance with internal and external standards. Slack engages credentialed assessors to perform external audits at least once per year. Audit results are shared with senior management and all findings are tracked to resolution.

Penetration testing

Slack engages independent entities to conduct regular application-level and infrastructure-level penetration tests. Results of these tests are shared with Slack management. Slack's Security Team reviews and prioritizes the reported findings and tracks them to resolution. Customers wishing to conduct their own penetration test of Slack application may request to do so and should contact their account representative to obtain permission from both Slack and Slack's hosting provider.

Legal compliance

Slack employs dedicated legal and compliance professionals with extensive expertise in data privacy and security. These professionals are embedded in the development lifecycle and review products and features for compliance with applicable legal and regulatory requirements. Slack also has a business code of conduct that makes legal, ethical and socially responsible choices and actions fundamental to our values and defines standards for meeting those goals.

Data requests

Not unlike other technology companies, Slack receives requests from users and government agencies to disclose or delete data other than in the ordinary operation and provision of the Services. Our Data Request Policy addresses those issues and clearly outlines Slack's policies and procedures for responding to such requests for customer data.

Secure by design

SDL

Slack assesses the security risk of each software development project according to our Secure Development Lifecycle. Before completion of the design phase, Slack undertakes an assessment to qualify the security risk of the software changes introduced. This risk analysis leverages both the OWASP Top 10 and the experience of Slack's Product Security team to categorize every project as High, Medium, or Low risk. Based on this analysis, Slack creates a set of requirements that must be met before the resulting change may be released to production.

All code is checked into a version-controlled repository. Code changes are subject to peer review and continuous integration testing. For the Slack web application, Slack's Security Team operates continuous automated static analysis using advanced tools and techniques. Significant defects identified by this process are reviewed and followed to resolution by the Security Team.

Bug bounty

Slack operates a public bug bounty program to facilitate responsible disclosure of potential security vulnerabilities identified by non-Slack researchers and reward them for their verified findings. Slack monitors incoming bug reports, prioritizes true vulnerabilities and ensures their timely resolution.

Protecting customer data

The focus of Slack's security program is to prevent unauthorized access to customer data. To this end, our team of dedicated security practitioners, working in partnership with peers across all our teams, take exhaustive steps to identify and mitigate risks, implement best practices, and constantly evaluate ways to improve.

Data encryption in transit and at rest

Slack transmits data over public networks using strong encryption. This includes data transmitted between Slack clients and the Slack service. Slack supports the latest recommended secure cipher suites to encrypt all traffic in transit, including use of TLS 1.2 protocols, AES256 encryption, and SHA2 signatures, as supported by the clients. Slack monitors the changing cryptographic landscape and upgrades the cipher suite choices as the landscape changes, while also balancing the need for compatibility with older clients.

Data at rest in Slack's production network is encrypted using FIPS 140-2 compliant encryption standards. This applies to all types of data at rest within Slack's systems—relational databases, file stores, database backups, etc. Slack stores encryption keys in a secure server on a segregated network with very limited access. Keys are never stored on the local filesystem, but are delivered at process start time and retained only in memory while in use.

The Slack service is hosted in data centers maintained by industry-leading service providers. Data center providers offer state-of-the-art physical protection for the servers and related infrastructure that comprise the operating environment for the Slack service. These service providers are responsible for restricting physical access to Slack's systems to authorized personnel.

Each Slack customer's data is hosted in Slack's shared infrastructure and segregated logically by the Slack application. Slack uses a combination of storage technologies to ensure customer data is protected from hardware failures and returns quickly when requested.

Network security

Slack divides its systems into separate networks to better protect more sensitive data. Systems supporting testing and development activities are hosted in a separate network from systems supporting Slack's production website. Customer data submitted into the Slack services is only permitted to exist in Slack's production network, its most tightly controlled network. Administrative access to systems within the production network is limited to those engineers with a specific business need.

Network access to Slack's production environment from open, public networks (the internet) is restricted. Only a small number of production servers are accessible from the internet. Only those network protocols essential for delivery of Slack's service to its users are open at Slack's perimeter. Slack deploys mitigations against distributed denial of service (DDoS) attacks at its network perimeter. Changes to Slack's production network configuration are restricted to authorized personnel.

In Slack's hosted production environment, control of network devices is retained by the hosting provider. For that reason, Intrusion Detection / Intrusion Prevention (IDS/IPS) are performed using host-based controls. For example, Slack logs, monitors, and audits system calls and has developed alerts for system calls that indicate a potential intrusion.

Classifying and inventorying data

To better protect the data in our care, Slack classifies data into different levels and specifies the labeling and handling requirements for each of those classes. Slack's ISMS considers data classifications in its encryption standards, its access control and authorization procedures, and incident response standards, among other security documents. Customer data is classified at the highest level.

Data classifications are maintained as part of the asset management process. Slack inventories hardware, software and data assets at least annually to maintain correct data classification levels. Slack restricts the flow of data to ensure that only appropriately classified systems may contain Customer data.

Authorizing access

To minimize the risk of data exposure, Slack adheres to the principle of least privilege—workers are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities. To ensure that users are so restricted, Slack employs the following measures:

- All systems used at Slack require users to authenticate, and users are granted unique identifiers for that purpose.
- Each user's access is reviewed at least quarterly to ensure the access granted is still appropriate for the user's current job responsibilities.

Workers may be granted access to a small number of internal systems, such as the corporate Slack instance, by default upon hire. Requests for additional access follow a documented process and are approved by the responsible owner or manager.

Authentication

To further reduce the risk of unauthorized access to data, Slack employs multi-factor authentication for administrative access to systems with more highly classified data. Where possible and appropriate, Slack uses private keys for authentication. For example, at this time, administrative access to production servers requires operators to connect using both an SSH key and a one-time password associated with a device-specific token. Where passwords are used, multi-factor authentication is enabled for access to higher data classifications. The passwords themselves are required to be complex (auto-generated to ensure uniqueness, longer than 12 characters, and not consisting of a single dictionary word, among other requirements).

Slack requires personnel to use an approved password manager. Password managers generate, store and enter unique and complex passwords. Use of a password manager helps avoid password reuse, phishing, and other behaviors that can reduce security.

System monitoring, logging, and alerting

Slack monitors servers, workstations and mobile devices to retain and analyze a comprehensive view of the security state of its corporate and production infrastructure. Administrative access, use of privileged commands, and system calls on all servers in Slack's production network are logged.

Slack's Security Team collects and stores production logs for analysis. Logs are stored in a separate network. Access to this network is restricted to members of the Security Team. Logs are protected from modification and retained for at least two years. Analysis of logs is automated to the extent practical to detect potential issues and alert responsible personnel. Alerts are examined and resolved based on documented priorities.

Endpoint monitoring

Slack workstations run a variety of monitoring tools that may detect suspicious code or unsafe configurations or user behavior. Slack's Security Team monitors workstation alerts and ensures significant issues are resolved in a timely fashion.

Mobile device management

Mobile devices that are used to transact company business are centrally managed and required to be enrolled in the appropriate mobile device management systems, to ensure they meet Slack's security standards.

Responding to security incidents

Slack has established policies and procedures (also known as runbooks) for responding to potential security incidents. All incidents are managed by Slack's dedicated Computer Security Incident Response Team. Slack defines the types of events that must be managed via the incident response process. Incidents are classified by severity. Incident response procedures are tested and updated at least annually.

Data and media disposal

Customer data is removed immediately upon deletion or message retention expiration. Slack hard deletes all information from currently running production systems (excluding team and channel names, and search terms embedded in URLs in web server access logs). Backups are destroyed within 14 days. Slack follows industry standards and advanced techniques for data destruction.

Slack defines policies and standards requiring media be properly sanitized once it is no longer in use. Slack's hosting provider is responsible for ensuring removal of data from disks allocated to Slack's use before they are repurposed.

Protecting secrets

Slack has implemented appropriate safeguards to protect the creation, storage, retrieval, and destruction of secrets such as encryption keys and service account credentials.

Workstation security

All workstations issued to workers are configured by Slack to comply with our standards for security. These standards require all workstations to be properly configured, kept updated, run monitoring software, and be tracked by Slack's endpoint management solution. Slack's default configuration sets up workstations to encrypt data, have strong passwords, and lock when idle. Workstations run up-to-date monitoring software to report potential malware and unauthorized software and mobile storage devices.

Controlling system operations and continuous deployment

We take a variety of steps to combat the introduction of malicious or erroneous code to our operating environment and protect against unauthorized access.

Controlling change

To minimize the risk of data exposure, Slack controls changes, especially changes to production systems, very carefully. Slack applies change control requirements to systems that store data at higher levels of sensitivity. These requirements are designed to ensure that changes potentially impacting Customer Data are documented, tested, and approved before deployment.

Prevention and detection of malicious code

In addition to general change control procedures that apply to our systems, Slack's production network is subject to additional safeguards against malware.

Server hardening

New servers deployed to production are hardened by disabling unneeded and potentially insecure services, removing default passwords, and applying Slack's custom configuration settings to each server before use.

File change management

Slack maintains the configuration of its production servers by using a configuration management system (CMS) that runs frequently to check that only the authorized version of key files are deployed. This CMS will overwrite files found on servers that don't match the correct version stored in a change controlled repository.

Disaster recovery and business continuity

Slack utilizes services provided by its hosting provider to distribute its production operation across four separate physical locations. These four locations are within one geographic region, but protect Slack's service from loss of connectivity, power infrastructure and other common location-specific failures. Production transactions are replicated among these discrete operating environments, to protect the availability of Slack's service in the event of a location-specific catastrophic event. Slack also retains a full backup copy of production data in a remote location more than 2500 miles from the location of the primary operating environment. Full backups are saved to this remote location once per day and transactions are saved continuously. Slack tests backups at least quarterly to ensure they can be correctly restored.

3rd party suppliers

To run its business efficiently, Slack relies on sub-service organizations. Where those sub-service organizations may impact the security of Slack's production environment, Slack takes appropriate steps to ensure its security posture is maintained. Slack establishes agreements that require service organizations adhere to confidentiality commitments Slack has made to its users. Slack monitors the effective operation of the organization's safeguards by conducting reviews of its service organization controls before use and at least annually.

Conclusion

We take security seriously at Slack, because every person and team using our service expects their data to be secure and confidential. Safeguarding this data is a critical responsibility we have to our customers, and we work hard to maintain that trust.