Security at Slack

slack

Table of contents

Introduction

Slack's mission is to make people's working lives simpler, more pleasant, and more productive. We believe that we need to make your data secure, and that 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's industry-leading security program is based on the concept of defense in depth: securing our organization, and your data, at every layer. Our security program is aligned with ISO 27000, AICPA Trust Service Principles, and NIST standards, and is constantly evolving with updated guidance and new industry best practices. You can see all our certificates **here**.

Slack's security team, led by our Chief Security Officer (CSO), is responsible for the implementation and management of our security program. The CSO is supported by the members of Slack's Security Team, who focus on Security Architecture, Product Security, Security Engineering and Operations, Detection and Response, and Risk and Compliance.

Protecting customer data security

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 the company, take exhaustive steps to identify and mitigate risks, implement best practices, and constantly develop ways to improve.

Secure by design

Slack's product security team has built a robust secure development lifecycle, which primarily leverages our open-sourced tool: **goSDL**.

You can read more about this process in-depth in our blog post **here**. While we strive to catch all vulnerabilities in the design and testing phases, we realize that sometimes mistakes happen. With this in mind, we have created a public bug bounty program (located **here**) to facilitate responsible disclosure of potential security vulnerabilities. All identified vulnerabilities are validated for accuracy, triaged, and tracked to resolution.

Encryption

- **Data in transit**
  All data transmitted between Slack clients and the Slack service is done so using strong encryption protocols. 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, whenever supported by the clients.

- **Data at rest**
  Data at rest in Slack's production network is encrypted using FIPS 140-2 compliant encryption standards, which applies to all types of data at rest within Slack's systems—relational databases, file stores, database backups, etc. All encryption keys are stored in a secure server on a segregated network with very limited access. Slack has implemented appropriate safeguards to protect the creation, storage, retrieval, and destruction of secrets such as encryption keys and service account credentials.

Each Slack customer's data is hosted in our shared infrastructure and logically separated from other customers' data. We use a combination of storage technologies to ensure customer data is protected from hardware failures and returns quickly when requested. The Slack service is hosted in data centers maintained by industry-leading service providers, offering state-of-the-art physical protection for the servers and infrastructure that comprise the Slack operating environment. Slack also offers data residency, which allows organizations to choose the country or region where they want to store their data at rest.

Network security and server hardening

Slack divides its systems into separate networks to better protect sensitive data. Systems supporting testing and development activities are hosted in a separate network from systems supporting Slack's production infrastructure. All servers within our production fleet are hardened (e.g. disabling unnecessary ports, removing default passwords, etc.) and have a base configuration image applied to ensure consistency across the environment.

Network access to Slack's production environment from open, public networks (the Internet) is restricted, with only a small number of production servers accessible from the Internet. Only those network protocols essential for delivery of Slack's service to its users are open at our perimeter and there are mitigations against distributed denial of service (DDoS) attacks deployed at the network perimeter. Additionally, for host-based intrusion detection and prevention activities, Slack logs, monitors, and audits all system calls and has alerting in place for system calls that indicate a potential intrusion.

Endpoint security

All workstations issued to Slack personnel are configured by Slack to comply with our standards for security. These standards require all workstations to be properly configured, updated, and be tracked and monitored by Slack's endpoint management solutions. Slack's default configuration sets up workstations to encrypt data at rest, have strong passwords, and lock when idle. Workstations run up-to-date monitoring software to report potential malware, unauthorized software, and mobile storage devices. Mobile devices that are used to engage in company business are required to be enrolled in the appropriate mobile device management system, to ensure they meet Slack's security standards.

Access control

- **Provisioning**
  To minimize the risk of data exposure, Slack adheres to the principles of least privilege and role-based permissions when provisioning access—workers are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities. All production access is reviewed at least quarterly.

- **Authentication**
  To further reduce the risk of unauthorized access to data, Slack employs multi-factor authentication for all access to systems with highly classified data, including our production environment, which houses our customer data. Where possible and appropriate, Slack uses private keys for authentication, in addition to the previously mentioned multi-factor authentication on a separate device.

- **Password management**
  Slack requires personnel to use an approved password manager. Password managers generate, store, and enter unique and complex passwords to avoid password reuse, phishing, and other password-related risks.

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 and retained for at least two years. Analysis of logs is automated to the extent practical to detect potential issues and alert responsible personnel. All production logs are stored in a separate network that is restricted to only the relevant security personnel.

Data retention and disposal

Customer data is removed immediately upon deletion by the end user or upon expiration of message retention as configured by the customer administrator. Slack hard deletes all information from currently running production systems (excluding team names and search terms embedded in URLs in web server access logs) and backups are destroyed within 14 days.

Slack's hosting providers are responsible for ensuring removal of data from disks is performed in a responsible manner before they are repurposed.

Disaster recovery and business continuity plan

Slack utilizes services deployed by its hosting provider to distribute production operations 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 significantly distant from the location of the primary operating environment. Full backups are saved to this remote location at least once per day and transactions are saved continuously. Slack tests backups at least quarterly to ensure they can be successfully restored.

Responding to security incidents

Slack has established policies and procedures (also known as runbooks) for responding to potential security incidents. All security incidents are managed by Slack's dedicated Detection and Response Team. The runbooks define the types of events that must be managed via the incident response process and classifies them based on severity. In the event of an incident, affected customers will be informed via email from our customer experience team. Incident response procedures are tested and updated at least annually.

Vendor management

To run efficiently, Slack relies on sub-service organizations. Where those sub-service organizations may impact the security of

Slack's production environment, we take appropriate steps to ensure our security posture is maintained by establishing agreements that require service organizations to adhere to confidentiality commitments we have made to users. Slack monitors the effective operation of the organization's safeguards by conducting reviews of all service organizations' controls before use and at least annually. Please view our sub-service organizations here.

External validation

- **Security compliance**
  Slack is continuously monitoring, auditing, and improving the design and operating effectiveness of our security controls. These activities are regularly performed by both third-party credentialed assessors and Slack's internal risk and compliance team. Audit results are shared with senior management and all findings are tracked to resolution in a timely manner. Please view our suite of certificates here.

- **Penetration testing**
  In addition to our compliance audits, Slack engages independent entities to conduct application-level and infrastructure-level penetration tests at least annually. Results of these tests are shared with senior management and are triaged, prioritized, and remediated in a timely manner. Customers may receive executive summaries of these activities by requesting them from their account executive.

- **Customer driven audits and penetration tests**
  Our customers are welcomed to perform either security controls assessments or penetration testing on Slack's environment. Please contact your account executive to learn about options for scheduling either of these activities.

Conclusion

We have an existential interest in protecting your data. Every person, team, and organization deserves and expects their data to be secure and confidential. Safeguarding this data is a critical responsibility we have to our customers, and we continue to work hard to maintain that trust. Please contact your account executive if you have any questions or concerns.