

# Sicherheit bei Slack



## Sicherheit auf Unternehmensebene, um Daten zu schützen und Compliance-Anforderungen zu erfüllen.

Sicherheit auf Unternehmensebene ist in jeden Aspekt der Zusammenarbeit in Slack integriert, ohne die Benutzerfreundlichkeit zu beeinträchtigen. So können unsere Kundinnen und Kunden den größtmöglichen Nutzen aus Slack ziehen und optimale Arbeit leisten.

Diese Unternehmen vertrauen uns



### INTERNES SICHERHEITSPROGRAMM VON SLACK

Das branchenführende Sicherheitsprogramm von Slack basiert auf dem Konzept der intensiven Verteidigung: zum Schutz unserer Organisation und der Sicherheit von Daten auf jeder Ebene. Wir erwerben weiterhin Zertifizierungen, indem wir die angesehensten Sicherheitsstandards einhalten, Lösungen anbieten, mit denen Compliance-Anforderungen leichter erfüllt werden können, und rigorose Maßnahmen auf architektonischer und operativer Ebene einsetzen, um Daten zu schützen.

## Compliance-Zertifizierungen und -Vorschriften

Slack erfüllt und übertrifft einige der allgemein anerkannten Sicherheitsstandards und bietet Lösungen, unsere Kundinnen und Kunden bei der Erfüllung ihrer Compliance-Anforderungen unterstützen.

### Slack-Zertifizierungen und -Bescheinigungen



### Slack unterstützt Kundinnen und Kunden bei der Einhaltung von:



## Sicherheitsarchitektur und -praktiken

Das dedizierte Sicherheits-Team von Slack nutzt branchenübliche bewährte Methoden und Frameworks, um Daten zu schützen. Unser Sicherheitsansatz konzentriert sich auf Sicherheit, Governance, Risiko-Management und Compliance. Das beinhaltet eine Verschlüsselung im Ruhezustand und bei der Übertragung, Netzwerksicherheit und Server-Absicherung, administrative Zugangskontrolle, Systemüberwachung, Protokollierung, Warnungen und mehr.

Slack beinhaltet einen robusten Satz an Sicherheits- und Datenschutz-Produktfunktionen, mit denen die jeweils nötige Kontrolle, Sichtbarkeit und Flexibilität geboten wird, um alle Sicherheitsprobleme zu lösen, ohne an Agilität einzubüßen.

## Identitäts- und Geräte-Management

Sicherstellen, dass vor jeder Informationsübermittlung unabhängig vom Standort der Benutzerinnen und Benutzer Identitätskontrollen durchgeführt werden. Slack ermöglicht es, einzelne Benutzer und Gruppen zu verwalten, Authentifizierungen mithilfe eines Identitäts-Providers zu optimieren sowie Rollen und Berechtigungen zuzuweisen. Wir bieten Funktionen, mit denen dafür gesorgt wird, dass nur die richtigen Leute und genehmigte Geräte Zugriff auf die Daten eines Unternehmens in Slack haben.

### Identitäts- und Zugangskontrollen

- SAML-basiertes einmaliges Anmelden
- Sitzungsdauer
- Zwei-Faktor-Authentifizierung
- Benutzer- und Gruppen-Provisioning via SCIM/JIT
- Domain-Beanspruchung

### Geräte-Management

- Enterprise Mobility Management (EMM)\*
- Sekundäre Authentifizierung\*
- Sitzungs-Management
- Blockierung von Nachrichtenkopien und Datei-Downloads\*
- Standard-Browser-Steuerung\*
- Geräte mit Jailbreak oder Root-Zugriff blockieren\*
- Mindestversion der App\*

## Datenschutz

Standardmäßig verschlüsselt Slack Daten im Ruhezustand und bei der Übertragung im Rahmen der grundlegenden Sicherheitskontrollen. Wir stellen Tools bereit, die noch mehr Sichtbarkeit und Kontrolle verschaffen.

- Enterprise Key Management (EKM)
- Schutz vor Datenverlust (Data Loss Prevention, DLP)^
- Audit-Logs API
- Grid-Workspace-Auffindbarkeit
- App- und Integrationsverwaltung

## Informations-Governance

Jedes Unternehmen benötigt eine fortlaufende Strategie, um das Risiko kompromittierter Daten zu reduzieren, und hierbei gibt es keine Einheitslösung. Slack bietet Governance- und Risikoverwaltungsfunktionen, die flexibel genug sind, um alle Anforderungen von Organisationen zu erfüllen.

- Globale Aufbewahrungsrichtlinien
- eDiscovery^
- Exporte (Standard/Unternehmen)
- Benutzerdefinierte Nutzungsbedingungen

\* Mobilfunktion

^ Lösung von Drittanbieter erforderlich (unterstützt von Slack-Ermittlungs-API)