ATLASSIAN

greenique

# Atlassian Cloud-Sicherheit: geteilte Verantwortung

# Inhaltsverzeichnis

# Das Modell der geteilten Verantwortung

In der Cloud ist Atlassian dafür verantwortlich, dass die Anwendungen, die Systeme, auf denen diese ausgeführt werden, und die Umgebungen, in denen die Systeme gehostet werden, sicher sind. Atlassian sorgt dafür, dass diese Systeme und Umgebungen die relevanten Standards einhalten, zum Beispiel ISO27001, ISO27018, SOC2, DSGVO und viele andere, die im Trust Center aufgeführt sind.

Sie als Atlassian-Kunde verwalten die Daten in Ihren Konten, die Benutzer und Benutzerkonten, die auf Ihre Daten zugreifen, und kontrollieren, welche Marketplace-Apps (früher "Add-ons" genannt) Sie installieren, weil Sie ihnen vertrauen. Wenn Sie Atlassian-Anwendungen verwenden, liegt es in Ihrer Verantwortung, sicherzustellen, dass Ihr Unternehmen die Atlassian Cloud-Produkte gesetzeskonform nutzt.

Bei der Weiterentwicklung seiner Cloud-Angebote werden für Atlassian Sicherheit und Compliance weiterhin oberste Priorität haben. In diesem White Paper wird erörtert, welche Maßnahmen Atlassian zum Schutz Ihrer Daten ergreift und wie Ihr lokaler Solution Partner Ihnen auf unserem gemeinsamen Weg helfen kann.

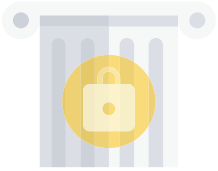
### Zuständigkeiten

| Atlassian | Gemeinsame Nutzung |
|---|---|
| • System<br>• Hosting<br>• Anwendung | • Richtlinie und Compliance<br>• Benutzer<br>• Informationen<br>• Marketplace-Apps |

# Die vier Säulen des Vertrauens bei Atlassian

Atlassian glaubt, dass alle Teams das Potenzial haben, Unglaubliches zu erreichen. Atlassian hat es zu seiner Mission gemacht, dieses Potenzial in jedem Team jeder Größe und Branche zu entfalten und mit leistungsstarker Software eine stärker vernetzte Welt zu schaffen.

Das Vertrauen der Kunden steht bei Atlassian immer im Mittelpunkt. Aus diesem Grund hat Sicherheit oberste Priorität. Atlassian verfügt über ein transparentes Sicherheitsprogramm, sodass Sie sich stets gut informiert und sicher fühlen können, wenn Sie Produkte und Services von Atlassian nutzen.



## Sicherheit

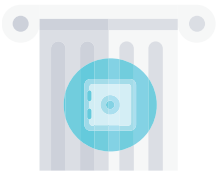
Die Cloud-Produkte, die Infrastruktur und die Prozesse von Atlassian wurden mit Blick auf Sicherheit entwickelt. Atlassian nimmt die Verantwortung für den Schutz der Daten Ihres Unternehmens ernst, und der Sicherheitsansatz von Atlassian basiert auf der Verantwortung, zu den Branchenführern im Bereich Cloud- und Produktsicherheit zu gehören.

Der Abschnitt zur **Sicherheit** im Trust Center beschreibt den detaillierten Ansatz und die proaktiven Sicherheitsprotokolle von Atlassian.

## Zuverlässigkeit

Atlassian Cloud wurde entwickelt, um Unternehmen durch die Bereitstellung einer zuverlässigen Plattform zu unterstützen, die während des Unternehmenswachstums dynamisch skaliert werden kann. Atlassian geht das an, indem es seinen Fokus bei der Produktentwicklung auf Resilienz, die Fähigkeit, Sie bei der Skalierung zu unterstützen, und auf die Leistung seiner Produkte setzt.

Atlassian fördert das Verantwortungsgefühl interner Teams, indem das Unternehmen SLAs einführt, den Status der Serviceverfügbarkeit veröffentlicht und seinen Ansatz zur Verbesserung des Qualitätssicherungsprozesses und der Leistung mit anderen teilt. Den detaillierten Ansatz von Atlassian können Sie unter **Zuverlässigkeit bei Atlassian** nachlesen.



## Datenschutz

Ihre Daten gehören Ihnen und Atlassian verpflichtet sich, die Privatsphäre Ihrer Daten zu schützen. In der **Datenschutzrichtlinie** von Atlassian wird erläutert, welche Informationen über Sie gesammelt werden und was Atlassian mit diesen Informationen macht, wie sie weitergegeben werden und wie Ihre Inhalte in Atlassian-Produkten und -Services behandelt werden. In den **Atlassian-Richtlinien für die Strafverfolgung** wird beschrieben, wie Atlassian Anfragen von Behörden bezüglich Kundeninformationen entgegennimmt, prüft und beantwortet.

Diese und weitere Informationen sind jederzeit im Abschnitt zum **Datenschutz** des Trust Centers verfügbar.

## Compliance

Ein kritischer Aspekt von Cloud-Migrationen ist die Überprüfung der Einhaltung der Vorschriften und die Beauftragung des richtigen Cloud-Partners für Ihr Unternehmen. Bei Atlassian nehmen die Compliance-Zertifizierungen in allen Regionen und Branchen aktiv zu, um Ihren Bedürfnissen gerecht zu werden. Atlassian ist bestrebt, allgemein anerkannte Compliance-Standards einzuhalten und Änderungen der Vorschriften mit einem proaktiven Ansatz aktiv zu beobachten. Atlassian lässt seinen Betrieb, seine Umgebung und seine Kontrollen von unabhängigen Beratern testen.

Der **Compliance**-Abschnitt im Atlassian Trust Center bietet umfassende Informationen über das Compliance-Programm und die ständig wachsende Liste von Zertifizierungen von Atlassian.

# Entscheidungen, Entscheidungen

## Ihre wichtigsten Entscheidungen

Die Entscheidungen, die Sie beim Einrichten der Atlassian-Produkte treffen, haben maßgeblichen Einfluss auf die Implementierung von Sicherheitsmaßnahmen.

### Zu den wichtigsten Entscheidungen gehören:

- **Domain-Bestätigung und zentrale Verwaltung:** Sie können eine oder mehrere Domains verifizieren, um nachzuweisen, dass Sie bzw. Ihr Unternehmen diese Domains besitzt. Über die Domain-Bestätigung und den Benutzeranspruch kann Ihr Unternehmen die Atlassian-Konten aller Mitarbeiter zentral verwalten und Authentifizierungsrichtlinien (u. a. Passwortanforderungen, mehrstufige Authentifizierung und SAML) anwenden. Sobald Ihre Domain bestätigt wurde, beanspruchen Sie alle Benutzer mit bestehenden Atlassian-Konten in dieser Domain. Benutzer, die in dieser Domain ein neues Atlassian-Konto erstellen, werden ebenfalls darüber informiert, dass sie ein verwaltetes Konto erhalten.
- **Zugriffsberechtigungen auf Ihre Daten:** Atlassian-Produkte sind auf Zusammenarbeit ausgelegt. Dafür sind Zugriffsberechtigungen erforderlich. Sie sollten jedoch mit Bedacht vorgehen, wenn Sie anderen Benutzern und Marketplace-Apps Berechtigungen zum Zugriff auf Ihre Daten gewähren. Wenn die Berechtigungen einmal erteilt wurden, kann Atlassian nicht verhindern, dass die entsprechenden Benutzer die im Rahmen dieser Berechtigungen möglichen Aktionen durchführen – auch wenn Sie nicht damit einverstanden sind. In einigen Produkten haben Sie die Möglichkeit, öffentlichen anonymen Zugriff auf Ihre Daten zu gewähren. Wenn Sie einen solchen Zugriff erlauben, können Sie möglicherweise nicht verhindern, dass diese Daten kopiert oder weiter verbreitet werden.
- **Zentralisiertes Benutzerzugriffsmanagement:** Wir empfehlen Atlassian-Kunden dringend, Atlassian Access für alle von ihnen verwendeten Atlassian-Produkte zu verwenden (einschließlich der Verwendung von Zwei-Faktor-Authentifizierung und Single-Sign-On), um die Verwaltung zu zentralisieren und die Sicherheit zu verbessern.

# Atlassian leistet seinen Beitrag

**Das Trust Management-Programm von Atlassian** berücksichtigt die Sicherheitsanforderungen des jeweiligen Atlassian-Kunden sowie Branchenstandards und Erwartungen. Daraus ergibt sich eine Reihe von genau auf das Unternehmen abgestimmten Anforderungen. Die Vertrauensstrategie von Atlassian basiert auf den folgenden Themen:

- Kontinuierliche Verbesserung der Sicherheit der Atlassian-Anwendungen, -Plattform und Umgebung, um einen überzeugenden Standard für Atlassian-Produkte und -Services bereitzustellen – allgemein bekannt als kontinuierliche Verbesserung.
- Wir sind offen und transparent, was unsere Programme, Verfahren und Metriken betrifft. Hierfür veröffentlichen wir unsere Planung und ermutigen andere Cloudanbieter, dies ebenfalls zu tun. Außerdem setzen wir neue Standards für unsere Kunden.
- Wir identifizieren aktuelle und zukünftige Sicherheitsbedrohungen für Atlassian und seine Kunden und reduzieren die Auswirkungen und die Dauer von Sicherheitsvorfällen.

Einzelheiten zu den Initiativen von Atlassian finden Sie im **Trust Center**, wo Sie die Zertifizierungsberichte von Atlassian für ISO 27001 und SOC2 herunterladen oder anfordern können und über einen Link zum **STAR-Fragebogen der Cloud Security Alliance (CSA)** von Atlassian gelangen. Sie können sich auch Einzelheiten zum **Atlassian Controls Framework** ansehen, das von Atlassian entwickelt wurde, um die Sicherheitsanforderungen von sieben internationalen Standards zusammenzuführen, die dem Sicherheits- und Compliance-Ansatz von Atlassian zugrunde liegen.

Der CSA STAR-Fragebogen enthält Antworten auf mehr als 300 Fragen, die im Fragebogen der Consensus Assessments Initiative (CAIQ) enthalten sind. Wie dieser Artikel deckt der CAIQ-Eintrag von Atlassian Jira, Confluence, Bitbucket, Halp, Jira Align, Opsgenie, Statuspage und Trello ab und bei Bedarf werden Einträge für andere Produkte hinzugefügt. Diese Kontrollen werden dann durch verschiedene Audits im Zusammenhang mit SOC2, ISO 27001 und PCI DSS verifiziert.

## Geteilte Verantwortung

In dem auf der ersten Seite gezeigten Sicherheitsmodell sind vier Bereiche als gemeinsame Verantwortung ausgewiesen.

**Und zwar:**

**Richtlinien und Compliance:** Der Ansatz erfüllt die Geschäftsanforderungen des Kunden in Übereinstimmung mit branchenspezifischen, behördlichen und gesetzlichen Compliance-Anforderungen.

**Benutzer:** Erstellung und Verwaltung von Benutzerkonten

**Informationen:** Die Inhalte, die Sie in der Cloud speichern

**Marketplace-Apps:** Services von Drittanbietern, denen Sie Zugriff auf Ihre Informationen und die Möglichkeit zur Integration in Atlassian-Produkte gewähren

Die Zuständigkeiten in diesen Bereichen sind folgendermaßen aufgeteilt:

### Richtlinie und Compliance

| Die Rolle von Atlassian | Ihre Rolle |
|---|---|
| • Berücksichtigung des Risikoprofils des Atlassian-Kunden bei der Beurteilung der Anforderungen von Sicherheitskontrollen<br>• Umfassendes Sicherheitsrisikomanagementprogramm und effektive Umsetzung der in der Antwort von CSA STAR beschriebenen Kontrollen<br>• Laufende Informationen für Kunden über Compliance-Zertifizierungen und darüber wie diese von Atlassian unterstützt werden<br>• Bereitstellung von Informationen für fundierte Entscheidungen zu den Atlassian-Plattformen<br>• Sicherstellung, dass das System von Atlassian über Failover und Redundanz verfügt<br>• Empfangen und Verwalten von Sicherheitsrisikoberichten im Zusammenhang mit Atlassian-Produkten<br>• Befolgung der Gesetze der verschiedenen Rechtssysteme, in deren Gebiet Atlassian tätig ist | • Kenntnis Ihres Risikoprofils und der Vertraulichkeit Ihrer Daten<br>• Beurteilung der Eignung der cloudbasierten Plattformen von Atlassian auf der Grundlage der Informationen, die wir zur Verfügung stellen<br>• Gewährleistung, dass die Plattform Ihre Compliance-Anforderungen erfüllen kann<br>• Erfüllung von vereinbarten Offenlegungs- und Meldepflichten für Datenschutzverletzungen, wenn es zu diesen kommen sollte<br>• Schutz Ihrer Endgeräte durch gute Sicherheitspraktiken<br>• Nur Hosting zulässiger Daten auf den Atlassian-Plattformen<br>• Einhaltung der Gesetze der Gerichtsbarkeiten, denen Sie unterliegen |

## Benutzer

| Die Rolle von Atlassian | Ihre Rolle |
| --- | --- |
| • Entwicklung und Einführung von Sicherheitskontrollen zur effektiven Verwaltung Ihrer Benutzer<br>• Überwachung der Atlassian-Plattformen auf bösartige oder böswillige Nutzung<br>• Bereitstellung von Funktionen für Domainverifizierung und Benutzerbeanspruchung, um eine zentrale Ansicht der Benutzer in Ihrer Cloud-Organisation zu erhalten<br>• Option auf Atlassian Access für mehr Effizienz und Kontrolle durch die Verbindung Ihres Identitätsanbieters, um (1) SSO oder 2FA/MFA verpflichtend zu machen und (2) die SCIM-Benutzerbereitstellung zu automatisieren<br>• Bereitstellung von Implementierungs- und Benutzersupport durch interne Teams von Atlassian<br>• Entwicklung von Produkten und Funktionen, die unternehmensweite Einblicke in Nutzung und Wachstum ermöglichen | • Verifizierung Ihrer Domain, wenn Sie Ihre Konten zentral verwalten möchten<br>• Genehmigung des Benutzerzugriffs auf Ihre Daten<br>• Regelmäßige Überprüfung der Liste der Benutzer mit Zugriff auf Ihre Daten und Entfernen von allen, die diesen nicht haben sollten<br>• Festlegung der Authentifizierungsrichtlinien in Atlassian Access \| Atlassian auf der Grundlage Ihrer Benutzer und Unternehmensanforderungen<br>• Wenn Sie eine verifizierte Domain haben:<br>• Implementierung strenger Benutzerzugriffsmanagement-Kontrollen wie Federated Identity Management (SAML), Zwei-Faktor-Authentifizierung und Passwortrichtlinien, je nach Bedarf, basierend auf Ihrem Risiko<br>• Überwachung der Benutzerkonten Ihrer Organisation auf schädliche oder böswillige Nutzung<br>• Einrichtung einer für Ihr Unternehmen geeigneten Passwortrichtlinie<br>• Benachrichtigungen an Atlassian über jede unbefugte Nutzung der Konten Ihrer Organisation<br>• Wenn Sie keine verifizierte Domain haben oder wenn Sie Benutzern außerhalb Ihrer Domain Zugriff gewähren:<br>• Verdeutlichung einer guten Passwortverwaltung gegenüber allen Benutzern, die Zugriff auf Ihre Daten haben<br>• Benachrichtigungen an Atlassian über jede unbefugte Nutzung Ihres Kontos<br>• Bewusstsein für die Risiken einer Anmeldung über soziale Netzwerke (siehe "Wiederverwendung von Anmeldedaten" unten) |

## Informationen

| Die Rolle von Atlassian | Ihre Rolle |
| --- | --- |
| • Zugriff auf Ihre Daten ausschließlich bei konkretem Supportbedarf<br>• Benachrichtigung über jeden uns bekannten Verstoß, der Ihre Daten betrifft<br>• Verwaltung von Backups auf Systemebene (einschließlich Ihrer Daten) | • Einrichtung Ihrer Atlassian-Produkte auf eine Weise, dass Ihre Informationen Ihren Anforderungen entsprechend zugänglich sind<br>• Erstellung von Backups Ihrer Daten |

## Marketplace-App

| Die Rolle von Atlassian | Ihre Rolle |
| --- | --- |
| • Sicherstellung, dass alle Cloud-Apps grundlegende Sicherheitsstandards erfüllen (Im Marketplace gelistete Apps werden kontinuierlich gescannt und auf Sicherheitslücken überprüft.)<br>• Überprüfung der Entwickler von Marketplace-Apps<br>• Verpflichtung der Entwickler zur Veröffentlichung ihrer Datenschutzrichtlinien (Datenschutzrichtlinien für Entwickler)<br>• Einladen von App-Anbietern/Partnern zur Teilnahme am Cloud Security Participant- oder Cloud Fortified-Programm, indem sie ihr eigenes Bug-Bounty-Programm entwickeln und den Support und die Zuverlässigkeit steigern<br>• Pflege von Forge, einem Programm, in dem Atlassian die Cloud-Apps hostet und es App-Anbietern ermöglicht, Infrastrukturinvestitionen einfacher zu nutzen, um höhere Sicherheits- und Zuverlässigkeitsstandards zu erfüllen | • Beurteilung der Eignung aller Marketplace-Apps, die Sie verwenden möchten, auf der Grundlage der dazu bereitgestellten Informationen<br>• Benachrichtigungen an Atlassian über jedes bösartige Verhalten, das in einer Marketplace-App identifiziert wurde |

# Bedrohungsmanagement

## Vorbereitung ist alles

Das Sicherheitsteam von Atlassian ist ein großer Befürworter der Bedrohungsmodellierung und verbringt viel Zeit damit, sich zu überlegen, nach welchen Szenarien Ausschau gehalten werden muss, und welche "Spiele" Atlassian ausführen wird, falls diese Szenarien eintreten. Atlassian informiert Sie über einige der Bedrohungen, die Sie bei der Nutzung ihrer Anwendungen berücksichtigen müssen. Dies trägt dann hoffentlich dazu beitragen, die oben skizzierte gemeinsame Verantwortung zu verwirklichen.

### Erraten von Anmeldedaten

Ein böswilliger Benutzer kann möglicherweise eine korrekte Kombination aus Benutzername und Passwort erraten und sich Zugriff auf Ihr Konto verschaffen. Starke Passwörter und eine mehrstufige Authentifizierung sind die besten Kontrollen, um diese Risiken einzudämmen. Wie in den Leitprinzipien erwähnt, wird Atlassian sein Bestes tun, Bedrohungen, die viele Benutzer betreffen, schnell zu bekämpfen.

### Wiederverwendung von Anmeldedaten

Wenn eines oder mehrere der Konten, denen Sie Zugriff auf Ihre Daten gewährt haben, dieselbe Kombination aus E-Mail-Adresse und Passwort an anderer Stelle im Internet verwenden, kann eine Kompromittierung dieser Site Ihre Daten für Angreifer anfällig machen. In ähnlicher Weise stellt die Genehmigung des Zugriffs für Benutzer, die sich über ein soziales Netzwerk anmelden, ein Risiko für Ihre Daten dar, falls die Sicherheit des Social-Media-Kontos dieses Benutzers verletzt wird. Ein gutes Sicherheitsbewusstsein in Ihrer gesamten Benutzerbasis (einschließlich Dritter, denen Sie Zugriff gewährt haben) und die Zwei-Faktor-Authentifizierung sind starke Kontrollen.

### Man-in-the-Middle-Angriffe

Ein Angriff, bei dem jemand versucht, sich zwischen Ihren Browser und den Server von Atlassian zu bringen, setzt voraus, dass Sie das Zertifikat des bösartigen Systems als gültig akzeptieren. Atlassian richtet seine Systeme so ein, dass dies einem Angreifer schwer gemacht wird, aber auf Sicherheitsbewusstsein und Zertifikatsprüfung sollte trotzdem nicht verzichtet werden.

## Kompromittierung von Endpunkten

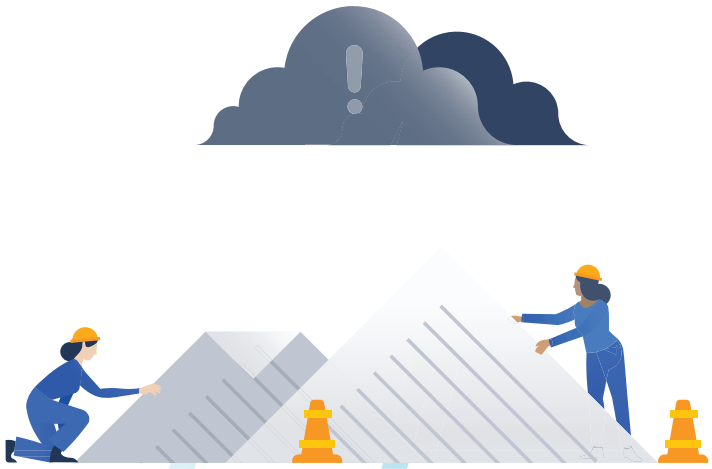
Die Kompromittierung eines Ihrer Endgeräte (egal ob Ihr Laptop, Desktop, Tablet oder Smartphone) macht alle anderen Kontrollen unwirksam. Die Verwendung aktueller Sicherheitssoftware und die vollständige Aktualisierung Ihrer Systeme sind die besten Kontrollen.

## Bösartige Marketplace-Apps

Wenn die Berechtigungen für eine Marketplace-App einmal installiert und erteilt wurden, kann Atlassian nicht verhindern, dass die App Aktionen gemäß den gewährten Berechtigungen ausführt, auch wenn Sie damit nicht einverstanden sind. Wir empfehlen, vor der Installation die Eignung der App und die Annehmbarkeit der angeforderten Berechtigungen zu überprüfen.

## Phishing oder gefälschte Websites

In einem cloudbasierten System kann jeder eine Website einrichten, die vorgibt, von Atlassian zu sein. Deshalb müssen Sie unbedingt darauf achten, dass Sie auf der richtigen Website sind, um sicherzustellen, dass Ihre Daten sicher sind. Die URL direkt in den Browser einzugeben oder einen Link mit einem Lesezeichen zu verwenden, ist hierfür eine gute Methode, und im Zweifelsfall lohnt es sich, das Zertifikat zu überprüfen.



# Gemeinsame Verantwortung und gemeinsamer Erfolg

Wenn es um die Sicherheit Ihrer Daten in Atlassian Cloud geht, sind wir alle im selben Team und haben wichtige Rollen zu spielen. Atlassian hat ein starkes Team von Sicherheitsexperten, die Tag und Nacht arbeiten, um sicherzustellen, dass Sicherheit in die Produkte integriert ist, damit eine Überwachung auf potenzielle Risiken und Angriffe und bei Erkennen eine schnelle Reaktion möglich ist. Ihre Aufgabe ist es, die Effektivität Ihrer Benutzerzugriffsverwaltung zu überprüfen, sich der von Ihnen eingegebenen Informationen bewusst zu sein, sicherzustellen, dass Ihre Endgeräte gut verwaltet werden, und zu überprüfen, ob alle Marketplace-Apps angemessen und vertrauenswürdig sind. Als Ihr fest zugeordneter Solution Partner steht Ihnen unser Team zur Verfügung für praktischen Support und Empfehlungen speziell für Ihr Unternehmen, damit Sie sich auf das Geschäftsergebnis konzentrieren können.

## Möchten Sie mehr über das Engagement von Atlassian für Datenschutz und Compliance erfahren?

Wenden Sie sich für weitere Informationen an Ihren lokalen Atlassian Solution Partner.


greenique GmbH & Co. KG

Bielefeld

service@greenique.de

+49 (0) 521 / 922 799 53

greenique.de


greenique

ATLASSIAN



ENTMIG-184_DRD-03/22