ATLASSIAN

So erreicht Atlassian Cloud Sicherheit und Compliance in Unternehmen

Ein detaillierter Einblick in die Verpflichtung von Atlassian zu globalem Datenschutz, Zertifizierungen, Compliance und mehr.

Inhaltsverzeichnis

In der heutigen, sich schnell weiterentwickelnden digitalen Landschaft hat die Cloud unbegrenzte Skalierungsoptionen geschaffen und geografisch verteilten Remote-Teams die Möglichkeit gegeben, zusammenzuarbeiten. Allerdings hat die steigende Anzahl von Geräten und Kanälen für den Zugriff auf Cloud-Anwendungen auch das Risiko von Datenschutzverletzungen erhöht. Deshalb ist die unbedingte Einhaltung von weltweiten Datenschutzvorschriften eine Notwendigkeit geworden. Atlassian möchte sicherstellen, dass über 190.000 Kunden von den Vorteilen der Cloud-Skalierung profitieren können und in Sachen Sicherheit und Datenschutz gleichzeitig höchste Ansprüche erfüllt werden. In diesem White Paper wird unser 5-Punkte-Ansatz erläutert, mit dem Atlassian Cloud-Produkte hinsichtlich Sicherheit und Compliance für Unternehmen gerüstet werden sollen.

Sicherung der Atlassian Cloud-Architektur mit einem Zero-Trust-Ansatz

Atlassians Ansatz für Cloud-Sicherheit beginnt auf der Ebene der Netzwerkarchitektur. Das Unternehmen implementiert Kontrollen auf jeder Ebene der Cloud-Umgebung und nutzt eine Zero-Trust-Sicherheitsstrategie für den Zugriff auf das Unternehmensnetzwerk, die Systeme und Services.

End-to-End-Datensicherheit mit erweiterten Kontrollen für Datenresidenz und Verschlüsselung

Der Schutz von Kundendaten hat eine hohe Priorität bei Atlassian, daher hat das Unternehmen zahlreiche Sicherheitsvorkehrungen getroffen, um Kunden diese Sorge abzunehmen. Alle Kundendaten werden auf einer branchenführenden Amazon Web Services-Plattform mit Redundanzen auf mehreren Ebenen gehostet. Als weitere Kontrollmaßnahme bietet Atlassian Datenresidenzoptionen, also die Möglichkeit, Produktdaten an bestimmte geografische Regionen zu binden. Außerdem werden Kundendaten im Ruhezustand und während der Übertragung verschlüsselt und es wird weiterhin in erweiterte Kontrollen, wie Bring-Your-Own-Key-Verschlüsselung (BYOK), investiert.

Kontinuierliche Investitionen in die Einhaltung globaler Datenschutzvorschriften

Datenschutzfunktionen sind in allen Produkten von Atlassian integriert. Darüber hinaus kümmert sich das Risk and Compliance-Team von Atlassian in Ihrem Auftrag ständig darum, dass sämtliche Cloud-Produkte neben globalen Standards wie SOC, ISO, DSGVO auch branchenspezifische Vorschriften einhalten.

Integrierte Kontrollen für das Identitäts- und Zugriffsmanagement

Mithilfe der integrierten Kontrollen von Atlassian können IT-Administratoren unter anderem Authentifizierungsprotokolle auf Enterprise-Niveau wie SAML-Single-Sign-On und mehrstufige Authentifizierung durchsetzen. Administratoren können außerdem Authentifizierungsrichtlinien für verschiedene Benutzerkreise anpassen und die Benutzerbereitstellung bzw. die Aufhebung derselben automatisieren. Dies mindert das Risiko von nicht autorisiertem Zugriff und erlaubt die Durchsetzung von Sicherheitskontrollen für die mobile Nutzung und Unterstützung für das Mobilgeräte- und mobile App-Management (MDM/MAM).

Proaktive Bedrohungsüberwachung und -prävention

Atlassian bietet umfassende Sicherheitstests und Schwachstellenmanagement-Programme, um Bedrohungen zu verhindern. Außerdem profitieren Kunden mit Atlassian Access von Unternehmens-Audit-Protokollen, die detaillierte Einblicke in die Aktivitäten von Administratoren liefern, wie beispielsweise Änderungen an Benutzern, Gruppen und Berechtigungen innerhalb des Unternehmens. Damit lassen sich verdächtige Aktivitäten einfacher ermitteln.

Sehen wir uns die oben genannten Sicherheitselemente im Einzelnen an.

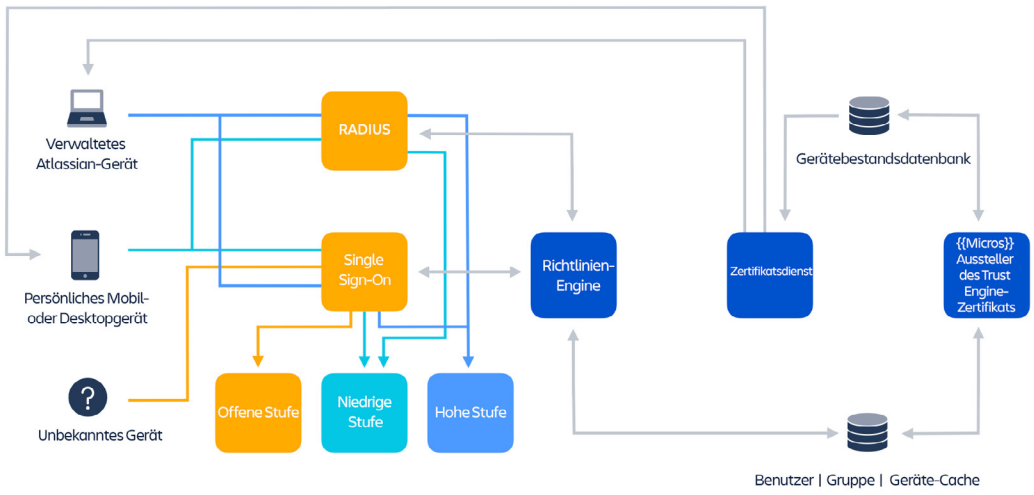
Sichere Cloud-Architektur

Atlassian nutzt **einen mehrschichtigen Ansatz** für Sicherheit, indem die Cloud-Infrastruktur in Zonen, Umgebungen und Services unterteilt wird und auf jeder dieser Ebenen Kontrollen implementiert werden. Das Unternehmen schränkt den Mitarbeiter-, Kundendaten-, CI/CD- (Continuous Integration and Deployment) und DMZ-Netzwerkdatenverkehr (Demilitarized Zone) ein, der durch jede Zone fließen darf. Außerdem werden Positivlisten für die Authentifizierung verwendet, um zu kontrollieren oder explizit zu autorisieren, welche Services miteinander interagieren dürfen.

Zero-Trust-Ansatz

Was den Netzwerkzugriff angeht, verfolgt Atlassian einen detaillierteren Ansatz und nutzt ein System, das als **Zero-Trust** bezeichnet wird – vertrauen Sie auf nichts, verifizieren Sie alles. Dieses berücksichtigt nicht nur die Anmeldeinformationen zur Authentifizierung, sondern auch die Vertraulichkeit von Ressourcen, wenn es um die Art des Zugriffs in unseren Netzwerken geht. Je nachdem, wie vertraulich eine Ressource ist, macht Atlassian diese auf unterschiedlichen Sicherheitsstufen für den Zugriff verfügbar: offen, niedrig oder hoch.

- Auf Ressourcen mit offener Sicherheitsstufe kann nach erfolgreicher Benutzerauthentifizierung im Atlassian-Netzwerk zugegriffen werden.
- Für Ressourcen mit niedriger Sicherheitsstufe sind eine Benutzerauthentifizierung und die Nutzung eines zuverlässigen Unternehmensgeräts erforderlich (dieses kann entweder von Atlassian bereitgestellt oder bei dem Mobile Device Management-Programm registriert sein).
- Ressourcen mit hoher Sicherheitsstufe erfordern eine Benutzerauthentifizierung und der Zugriff darauf ist nur über ein von Atlassian bereitgestelltes Unternehmensgerät möglich.



Disaster Recovery und Business Continuity

Natürlich ist uns allen bewusst, dass Störungen auftreten können. Deshalb plant Atlassian diese aktiv ein und erstellt für die Prozesse Pläne für die Disaster Recovery (DR) und Business Continuity (BC). Um die DR- und BC-Anforderungen zu erfüllen, werden in allen Produkten Redundanzen eingebaut. Die Site Reliability Engineers testen diese Redundanzen regelmäßig, um eventuell vorhandene Lücken zu identifizieren. Jedes Atlassian-Team arbeitet mit einem Disaster Recovery-Champion zusammen, der sicherstellt, dass die DR in alle vom Team produzierten Projekte integriert ist. Zudem werden regelmäßig Disaster Recovery-Tests durchgeführt, um die Prozesse und Technologien zu verbessern.

End-to-End-Datensicherheit

Laut IBM kostet eine Datenschutzverletzung ein durchschnittliches Unternehmen 3,86 Millionen US-Dollar, etwa für die Erkennung und Eskalation, für entgangene Geschäftschancen, für Benachrichtigungen und nachträgliche Behebungsmaßnehmen. Allein der Gedanke daran bringt Sicherheitsführungskräfte zum Schaudern. Deshalb zeichnen sich alle Atlassian Cloud-Produkte durch ihre Sicherheitsmerkmale aus. Diese umfassen die sichere Aufbewahrung und Verschlüsselung sowie den vertraulichen Umgang mit Kundendaten. So behalten Kunden so viel Kontrolle über ihre Daten wie möglich.

Branchenführende Hosting-Infrastruktur

Atlassian-Produkte und Daten werden mit Amazon Web Services (AWS) gehostet, einem branchenführenden Cloud-Hosting-Anbieter. Im Netzwerk von AWS werden Kundendaten in **mehreren unterschiedlichen geografischen Regionen gehostet**, etwa in Städten entlang der Ost- und Westküste der USA, in der Europäischen Union und im Asien-Pazifik-Raum. Die Daten werden immer in anderen geografisch isolierten Rechenzentren (sogenannten Verfügbarkeitszonen) repliziert, sodass ein Ausfall einer Verfügbarkeitszone keine negativen Auswirkungen auf Atlassian-Kunden haben wird.

> Durch die Auslagerung der Infrastruktur und der damit verbundenen Wartungsarbeiten konnte CHG Healthcare bisher fast 120.000 US-Dollar und bis zu 30 Stunden pro Woche einsparen. Diese kann das Unternehmen jetzt für Innovationen anstatt für die Administration nutzen. Da sich Atlassian jetzt um das Patching und um Sicherheits-Updates kümmert, muss sich CHG zudem keine Gedanken mehr um Schwachstellen machen.

Kontrolle der Datenresidenz

Aufgrund der Einführung von geografischen Datenvorschriften wie der Datenschutz-Grundverordnung (DSGVO) der EU hat Atlassian es Kunden noch einfacher gemacht, zu kontrollieren, wo ihre Daten aufbewahrt werden. Mithilfe der **Datenresidenzfunktion** (die in allen kostenpflichtigen Tarifen enthalten ist), können IT-Administratoren jetzt von Benutzern generierte Produktdaten, beispielsweise Confluence-Seiten und Jira-Tickets oder -Kommentare, in bestimmten Datenregionen speichern.

Atlassians Datenresidenzoptionen geben Kunden eine bessere Kontrolle. Wenn beispielsweise nur ein bestimmter Anteil der Unternehmensdaten an eine bestimmte Region gebunden werden muss, können IT-Administratoren diesen in einer **eindeutigen Produktinstanz** isolieren, um Datenisolierung und Compliance sicherzustellen.

Aktuell werden Datenresidenz in der Europäischen Union und in den USA unterstützt. Atlassian plant aber, **die unterstützten Regionen** bis Mitte 2022 auf Australien, das Vereinigte Königreich, Kanada und Japan auszuweiten. Im Rahmen dieser Bemühungen, die Produkte kontinuierlich zu verbessern, soll auch bis Ende 2021 die **Datenresidenz für Drittanbieter-Apps** unterstützt werden.

Um die Leistungsanforderungen von Benutzern auf der ganzen Welt zu erfüllen, werden Benutzerkontodaten weltweit repliziert. Demzufolge gibt es für Benutzerkontodaten gegenwärtig keine Datenresidenz. Weder die DSGVO noch Schrems II verlangen diese. Den Verordnungen kommt es stattdessen darauf an, dass für europäische Daten Schutzmaßnahmen eingerichtet werden, wenn diese Europa verlassen. Aus diesem Grund hält sich Atlassian an Standardvertragsklauseln, um sicherzustellen, dass sämtliche Benutzerdaten angemessen und entsprechend der DSGVO geschützt sind. Weitere Informationen dazu, wo und wie Daten speichert werden, erhalten Sie im **Atlassian Trust Center**.

Verschlüsselung von Daten während der Übertragung und im Ruhezustand

Wenn es um Cloud-Sicherheit geht, sollte die **Verschlüsselung von vertraulichen Daten** für alle Beteiligten eine Mindestvoraussetzung sein. Im Rahmen der Bemühungen, sämtliche Ebenen der Cloud-Architektur abzusichern, bietet Atlassian Verschlüsselung für Daten im Ruhezustand für alle Kundendaten und Anhänge in Jira Software Cloud, Jira Service Desk Cloud, Jira Work Management, Confluence Cloud, Statuspage, Opsgenie und Trello.

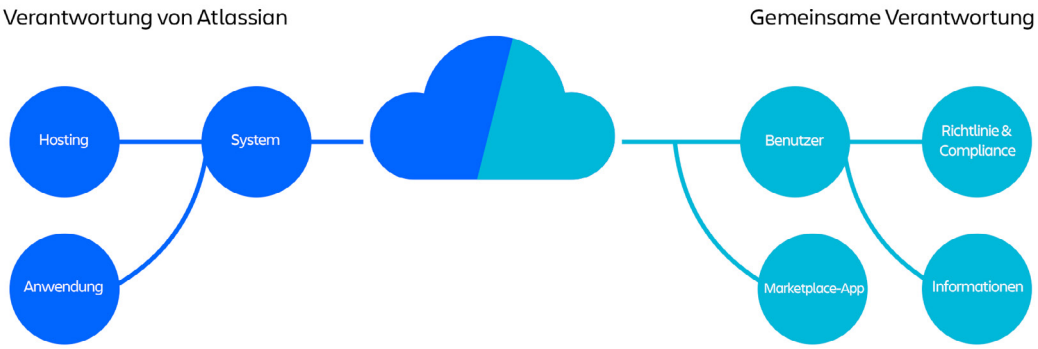
Jegliche auf Servern liegende inaktive Daten werden mithilfe des branchenüblichen Advanced Encryption Standard 256 im Ruhezustand verschlüsselt. Kundendaten, die über öffentliche Netzwerke übertragen werden, werden mithilfe von Transport Layer Security 1.2+ mit Perfect Forward Secrecy verschlüsselt, das eine starke Verschlüsselung und lange Schlüssel gewährleistet. Mithilfe dieser Maßnahmen können Daten vor einer nicht autorisierten Offenlegung oder Modifikation während der Übertragung geschützt werden.

Demnächst für Atlassian Cloud Enterprise verfügbar: BYOK-Verschlüsselung

Für Unternehmen, die sich mehr Kontrolle wünschen, plant Atlassian die Einführung der **Bring-Your-Own-Key-Verschlüsselung (BYOK)** für Jira und Confluence bis Anfang 2023. Damit erhalten Unternehmen die Möglichkeit, ihre eigenen kryptografischen Schlüssel über den Schlüsselmanagementservice von Amazon Web Services zu verwalten. Mit BYOK können nicht nur Zugriffsberechtigungen gewährt oder widerrufen, sondern auch alternative Kontrollen eingesetzt werden, um Vorschriften bezüglich der Datensicherheit zu erfüllen.

Zusammenarbeit zum Schutz von Daten

Atlassian übernimmt die volle Verantwortung für die Sicherheit, Leistung und Verfügbarkeit der Systeme, ist aber auf die Mitwirkung der Kunden angewiesen, um alle ihre Daten zu schützen.



Es gibt vier Bereiche mit geteilten Verantwortlichkeiten, auf die wir Benutzer hinweisen möchten:

Richtlinie und Compliance
Atlassian hat die **Datenschutzrichtlinie** und **verschiedene Vorschriften**, an die sich Atlassian hält, öffentlich gemacht. Letztendlich ist aber der Benutzer dafür verantwortlich, dass das System die Unternehmens- und Compliance-Anforderungen erfüllt.

Benutzer
Atlassian-Produkte sind sowohl auf eine offene Zusammenarbeit als auch den Schutz von Daten ausgelegt. Benutzer sollten sicherstellen, dass sie Mitarbeitern und externen Benutzern angemessene Berechtigungen für ihre Atlassian Apps und -Daten gewähren.

Informationen
Sämtliche Inhalte, die Sie in Confluence Cloud, Jira Cloud, Trello und Bitbucket Cloud speichern, stehen allen Benutzern und Apps mit entsprechenden Berechtigungen zur Verfügung. Sorgen Sie dafür, dass unsere Atlassian-Produkte und -Instanzen so eingerichtet sind, dass Berechtigungen für den Zugriff auf Daten auch den Inhalten entsprechen.

Marketplace-Apps
Entwickler von Drittanbieter-Apps für Atlassian Marketplace werden unabhängig verifiziert und **Apps regelmäßig auf Schwachstellen überwacht**. Mit **Forge** bietet Atlassian jetzt außerdem eine Cloud-Plattform, mit der Drittentwickler unternehmensfertige Apps mit denselben erstklassigen Sicherheitsfunktionen erstellen können, die Atlassian für seine Produkte anbietet. Allerdings ist es auch an Ihnen, Services von Drittanbietern zu bewerten, mit denen Sie arbeiten. Schließlich werden Sie diesen Apps Zugriff auf Daten gewähren, die in Ihren Atlassian-Produkten gespeichert sind.

Einhaltung von globalen Datenschutzvorschriften

Durch die Nutzung einer Cloud-Plattform wie Atlassian Cloud Enterprise können IT-Administratoren die Überwachung und Sicherstellung der Compliance im gesamten Technologieportfolio einer anderen Partei überlassen.

Datenschutzprogramm

Atlassians Datenschutzprogramm soll Kunden ein hohes Maß an Schutz bieten. Das bedeutet, dass die Bemühungen über gesetzliche Vorschriften hinausgehen und Atlassian den Datenschutz in allem berücksichtigt.

Atlassian entwickelt seine Cloud-Produkte entsprechend allgemein anerkannter Datenschutzstandards und -zertifizierungen. Atlassian-Mitarbeiter, die Kundendaten verarbeiten, werden regelmäßig in Sicherheits- und Vertraulichkeitsprotokollen geschult. Atlassian-Kunden sollen mittels Kontrollen mehr Souveränität gegeben werden. Organisationsadministratoren in Kundenteams können Benutzerprofile einfach verwalten und sogar **die Löschung von Konten verwalteter Benutzer** über die Admin-Konsole vereinfachen. Dabei werden ihre personenbezogenen Daten aus allen Organisationen und Sites gelöscht, die für den Zugriff auf Jira Cloud, Confluence Cloud, Bitbucket Cloud und Trello genutzt werden. Nicht verwaltete Endbenutzer dürfen außerdem die Löschung ihrer personenbezogenen Daten verlangen, indem sie **eine Anforderung zum Löschen ihres Kontos initiieren**.

Am Ende jedes Jahres veröffentlicht Atlassian zudem **einen alljährlichen Transparenzbericht, der Informationen dazu enthält, welche behördlichen Anfragen in diesem Jahr erhalten wurden und wie das Unternehmen darauf reagiert hat. Atlassian ist** transparent**, was behördliche Anfragen zu Benutzerdaten, die Entfernung von Inhalten oder die Sperrung von Benutzern angeht. Die** Richtlinien und Verfahren **für die Reaktion auf behördliche Anfragen werden stets befolgt. Um Kundeninformationen von Atlassian zu erhalten, müssen Strafverfolgungsbehörden den Rechtsweg gehen, der für die nachgefragten Informationen angemessen ist und beispielsweise eine Vorladung, eine gerichtliche Anordnung oder einen Haftbefehl vorlegen. Weitere Informationen hierzu finden Sie im** Trust Center.

AKTUELLE ZERTIFIZIERUNGEN

Atlassian ist sich bewusst, dass seine Kunden unterschiedliche Compliance-Anforderungen haben. Deshalb werden die Produkte so entwickelt, dass sie **mehrere branchenführende Standards und Vorschriften** einhalten. Aktuell erfüllen Atlassian-Produkte folgende Normen:

- System and Organization Controls (SOC) 2, SOC 3
- ISO/IEC 27001, ISO/IEC 27018
- Payment Card Industries Data Security Standard (PCI DSS)
- Voluntary Product Accessibility Template (VPAT 508)
- DSGVO

Verpflichtung zur Einhaltung der DSGVO

Atlassian Cloud-Produkte werden gemäß den vielen Sicherheits- und Datenschutzstandards entwickelt, die den Anforderungen der DSGVO entsprechen. Sehen wir uns an, wie Atlassian sich verpflichtet hat, im Bereich Datenschutz und -sicherheit federführend zu sein, und demzufolge dafür gesorgt hat, dass die Produkte die Vorgaben der DSGVO erfüllen.

Internationale Datenübertragungen

Aufgrund des jüngsten Schrems II-Urteils stellt Atlassian aktuell einen vorab signierten **Zusatz zum Datenschutz** zur Verfügung, der eine vollständige Ausgabe der Standardvertragsklauseln enthält und als zulässiger Mechanismus für die rechtmäßige Übertragung personenbezogener Daten an Atlassian Cloud-Produkte außerhalb des Europäischen Wirtschaftsraums dient. Dieser Zusatz enthält spezielle Bestimmungen, die Kunden dabei helfen, die DSGVO-Vorgaben einzuhalten. Darüber hinaus investiert Atlassian weiterhin entsprechend den **DSGVO-Leitlinien** in moderne Verschlüsselungsfunktionen wie BYOK, um personenbezogene Daten zu schützen.

Individuelle Datenschutzrechte und Einwilligung

Um die DSGVO-Vorschriften über das Recht des Einzelnen auf die Löschung von Daten einzuhalten, wird es Administratoren auch leichter gemacht, die personenbezogenen Daten von Benutzern aus Atlassian Cloud-Produkten zu löschen. Sowohl verwaltete als auch nicht verwaltete Endbenutzer können verlangen, dass ihre personenbezogenen Daten gelöscht werden, und Organisationsadministratoren können die **Löschung von Konten ganz einfach über das** Administratorportal von Atlassian vornehmen.

Auswahl und Einwilligung

Endbenutzer in der EU genießen transparente Einblicke und können auswählen, wie Atlassian ihre Daten verwendet, indem an allen Erfassungsstellen ihre Einwilligung für Cookies und Marketingbotschaften eingeholt werden. Auf diese Weise können Benutzer genau nachvollziehen, wie ihre Daten erfasst und verwendet werden, und sie erhalten Auswahloptionen dazu, wie sie diese mit Atlassian teilen möchten.

Kundendaten und Dritte

Atlassian arbeitet mit externen Serviceanbietern zusammen, die Services im Zusammenhang mit Websites, Anwendungsentwicklung, Hosting, Wartung, Backup, Speicherung, virtueller Infrastruktur, Zahlungsverarbeitung, Analyse und anderen Zwecken bereitstellen. Diese Serviceanbieter haben eventuell Zugriff auf personenbezogene Daten oder verarbeiten diese, damit sie diese Services bereitstellen können.

Atlassian benachrichtigt die betroffenen Kunden über die Nutzung von Subunternehmern, die ihre personenbezogenen Daten bearbeiten könnten, bevor es zur Verarbeitung kommt. Eine Liste mit externen Subunternehmern, mit denen Atlassian zusammenarbeitet, finden Sie auf der Seite **Unterauftragsverarbeiter von Atlassian.** Besucher sind eingeladen, einen RSS-Feed zu abonnieren, um Benachrichtigungen darüber zu erhalten, wenn Atlassian neue Auftragsverarbeiter hinzufügt.

Geplante Compliance-Maßnahmen

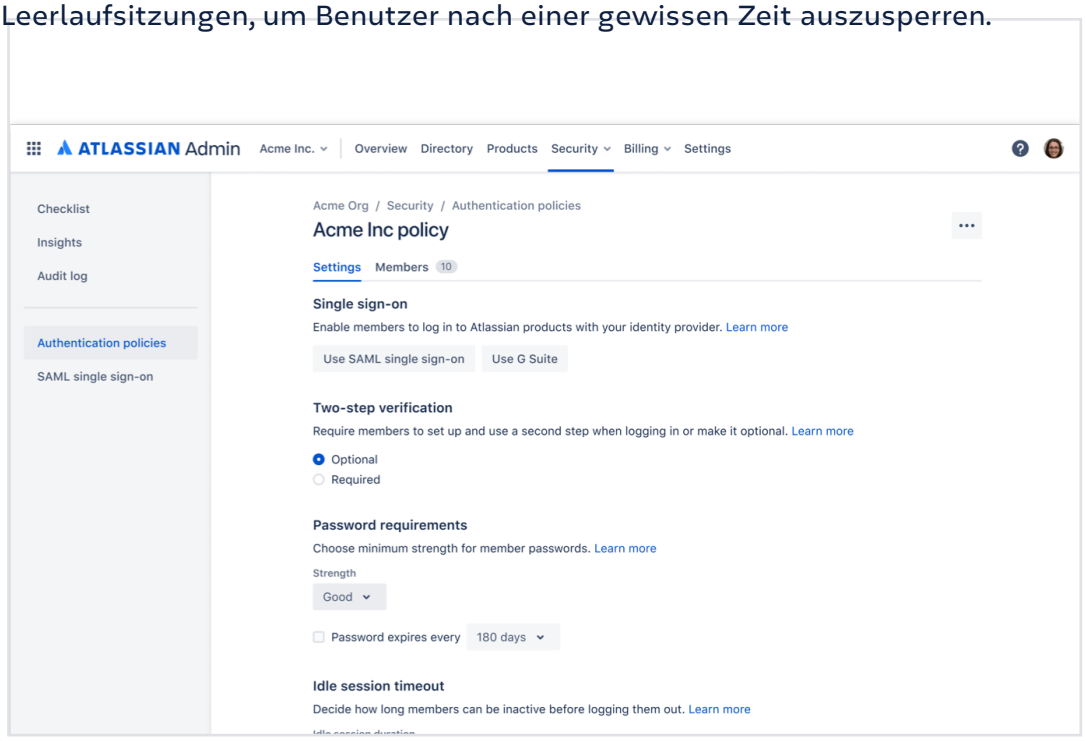
Um Kunden in den regulierten Branchen besser unterstützen zu können, investiert Atlassian weiterhin in die Erfüllung branchenspezifischer Compliance-Anforderungen. Bis Mitte 2022 soll Atlassian Cloud Enterprise die **Vorschriften der Finanzdienstleistungsbranche** in den USA, in Deutschland (Bundesanstalt für Finanzdienstleistungsaufsicht, oder BaFin) und in Australien (Australian Prudential Regulation Authority) erfüllen. Für US-amerikanische Unternehmen im Gesundheitswesen will das Unternehmen bis Mitte 2022 die Einhaltung des **HIPAA-Gesetzes (Health Insurance Portability and Accountability Act)** für Jira Software Cloud und Confluence Cloud erreichen.

Integriertes Identitäts- und Zugriffsmanagement

Auch wenn Ihr Unternehmen Branchenvorschriften eingehalten und sichergestellt hat, dass alle Kundendaten verschlüsselt sind, ist Ihre Unternehmenssicherheit nur so stark wie Ihr schwächstes Glied in der "Mitarbeiterkette". Laut **Kaspersky** war im Jahr 2019 die Ursache von 52 % aller Datenschutzverletzungen in Unternehmen der Missbrauch von IT-Ressourcen durch Beschäftigte. Aus diesem Grund hat Atlassian Administratoren mit umfassenden integrierten Kontrollen ausgestattet, mit denen sie den unternehmensweiten Zugriff absichern können, während die Cloud-Produkte genutzt werden.

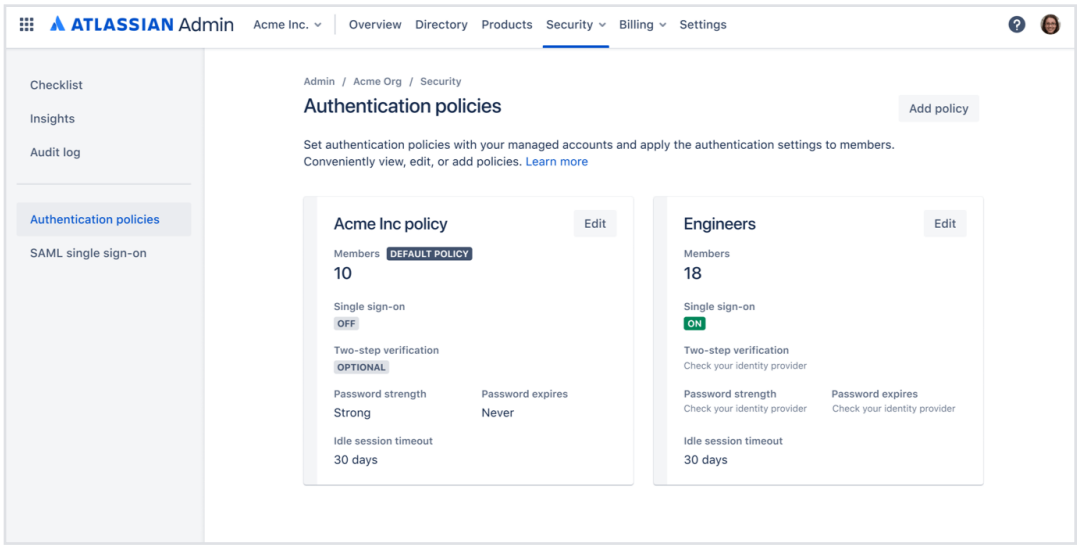
Authentifizierungsprotokolle auf Enterprise-Niveau

Atlassian ermöglicht es Unternehmen, ihre Sicherheitsrisiken durch die Implementierung von Authentifizierungsprotokollen in allen ihren Atlassian-Produkten einzuschränken. Über Atlassian Access –der zentralen Sicherheits- und Verwaltungslösung, die ohne Zusatzkosten im **Cloud Enterprise-Tarif** enthalten ist – können Administratoren mithilfe des bestehenden Identitätsanbieters ihres Unternehmens eine SAML-SSO-Authentifizierung einrichten. Damit können Mitarbeiter mit einer einmaligen sicheren Anmeldung Zugriff auf mehrere Atlassian-Produkte und -Instanzen erhalten. Administratoren können außerdem als zusätzliche Sicherheitsmaßnahme eine Zwei-Faktor-Authentifizierung durchsetzen, bei der Benutzer während der Anmeldung einen 6-stelligen Code eingeben müssen, der an ihr Telefon gesendet wurde. Weitere Kontrollen umfassen Folgendes: eine Mindestpasswortstärke für Benutzer, das erzwungene Ablaufen von Passwörtern nach einem bestimmten Zeitraum und die Durchsetzung von Leerlaufsitzungen, um Benutzer nach einer gewissen Zeit auszusperren.



Anpassbare Authentifizierungsrichtlinien

Anstelle eines Universalansatzes können Administratoren einen flexiblen Ansatz nutzen, um Authentifizierungsrichtlinien nach Bedarf für verschiedene Benutzerkreise anzupassen. Sie können beispielsweise eine Standardpasswortrichtlinie für alle Benutzer einrichten, aber eine mehrstufige Authentifizierung für einen bestimmten Benutzerkreis zwingend erforderlich machen, der auf eine Produktinstanz mit streng vertraulichen Daten zugreift.



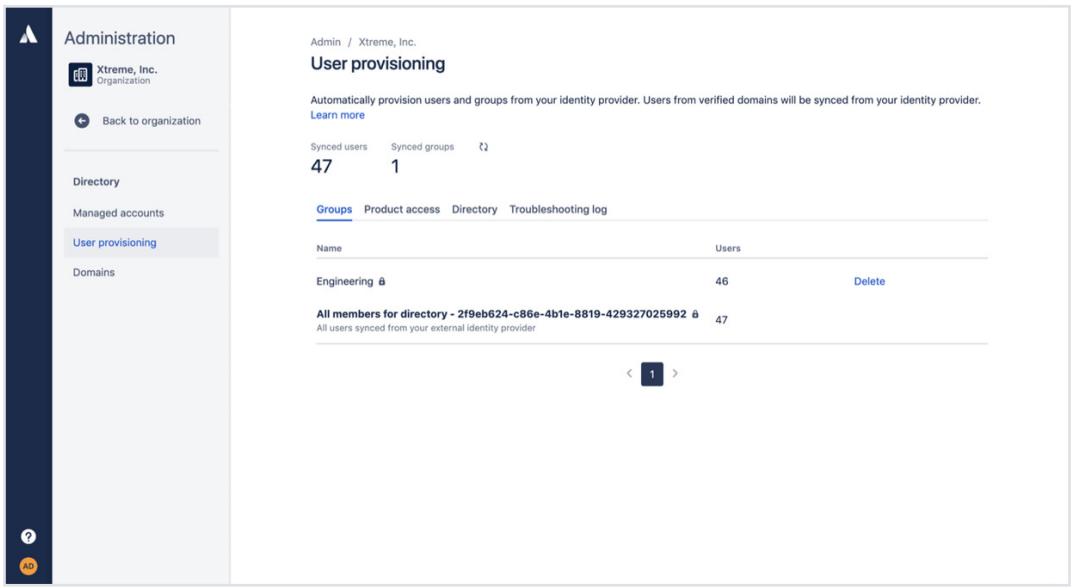
Mobilgeräte- und App-Management

Mit der zunehmenden Remote-Arbeit und der Nutzung des BYOD-Konzepts, bei dem Benutzer ihre eigenen Mobilgeräte mitbringen, greifen viele Benutzer über mobile Apps auf Atlassian-Produkte zu. Um Datenlecks oder unbefugten Zugriff über mobile Apps zu verhindern, können Administratoren jetzt spezifische Sicherheitsprotokolle durchsetzen, beispielsweise die Einschränkung von Copy-and-Paste-Vorgängen, das Blockieren von Screenshots oder das Anfordern von Gesichts-/Fingerabdruckscans oder einer anderen biometrischen Authentifizierung beim Anmelden. Gegenwärtig unterstützt Atlassian die Integration in führende MDM-Software (Mobile Device Management), um Sicherheitsprotokolle für die Jira-Produktfamilie und mobile Confluence- und Trello-Apps durchzusetzen, die auf vom Unternehmen verwalteten Geräten verwendet werden. Bis Juli 2021 möchte Atlassian die Unterstützung für das mobile App-Management erweitern. Denn dieses wird es Administratoren ermöglichen, mobile Sicherheitsrichtlinien über die **Admin-Konsole des Unternehmens** auf verwalteten Geräten und persönlichen Mobilgeräten zu konfigurieren.

Automatisierung der Bereitstellung und Aufhebung der Bereitstellung von Benutzern

Laut **Osterman Research** können ganze 89 % der ehemaligen Mitarbeiter immer noch auf mindestens eine Anwendung ihres früheren Arbeitgebers zugreifen, nachdem sie das Unternehmen verlassen haben. Fast ein Drittel dieser Ehemaligen haben diese Möglichkeit genutzt, um Unternehmensinformationen anzusehen, und jeder 16. hat diese Informationen mit Außenstehenden geteilt. Bei großen Unternehmen kann es schon einmal vorkommen, dass die Entfernung von Benutzeridentitäten aus dem System vergessen wird. Dieser Vorgang ist aber wichtig, um die Cloud-Sicherheit zu gewährleisten.

Um dieses Problem zu lösen, bietet Atlassian Access die Möglichkeit, den Prozess der Benutzerbereitstellung bzw. der Aufhebung derselben zu automatisieren. Access lässt sich entweder über unsere bestehenden Integrationen mit führenden Identitätsanbietern oder über SCIM-API (System for Cross-domain Identity Management) für benutzerdefinierte Integrationen mit dem **Benutzerverzeichnis** eines Unternehmens synchronisieren. So kann Benutzern automatisch Zugriff gewährt werden, wenn sie zum Team dazustoßen. Je nachdem, welcher Gruppe (Entwickler-, HR- oder Marketingabteilung) die Mitarbeiter in Ihrem Benutzerverzeichnis hinzugefügt werden, erhalten sie automatisch Zugriff auf das Atlassian-Toolset, das ihr Team benötigt. Wenn sie das Team wechseln, ändern sich ihre Berechtigungen. Und wenn sie das Unternehmen verlassen, werden ihre Zugriffsberechtigungen komplett widerrufen.



So nutzte Canva die Sicherheitsfunktionen von Atlassian für seine Zwecke

Als sich die Belegschaft der Designplattform Canva auf 1.000 Mitarbeiter weltweit vergrößerte, verließ sich das Unternehmen auf Atlassian Cloud-Funktionen, um die Sicherheit in allen Cloud-Apps zu gewährleisten und seinen Mitarbeitern gleichzeitig flexibles Arbeiten zu ermöglichen. Mitarbeiter im gesamten Unternehmen nutzen Jira Software und Confluence, um ihre Arbeit zu erledigen, und dank der Funktionen von Atlassian Access kann Canva den Zugriff auf verschiedene Produktinstanzen (wie der Instanz des HR-Teams in Jira Service Management) ganz einfach einschränken und die Sicherheitseinstellungen von Mitarbeitern verwalten.

"Es wird genau kontrolliert, wer HR-Informationen einsehen darf, und es gibt strenge Sicherheitsmaßnahmen", so Jeff Lai, Internal Infrastructure-Experte bei Canva. "Dank dieser strengen Features trauen wir uns, diese Art von Informationen in Jira Service Management aufzubewahren."

Canva verwendet auch die automatisierte Funktion zur Benutzerbereitstellung bzw. zur Aufhebung derselben in Atlassian Access, um neuen Mitarbeitern problemlos Zugriff auf die Systeme und Dokumente von Canva zu gewähren. Canva nutzt den externen Identitätsanbieter Okta, um Daten mit Access zu synchronisieren. Und neue Mitarbeiter erhalten noch vor ihrem Eintrittstag die Berechtigung, eine eingeschränkte Anzahl Canvas-Inhalte einzusehen. Mithilfe der SSO-Funktion von Access und der erzwungenen Zwei-Faktor-Authentifizierung können externe Auftragnehmer auch auf eine begrenzte Anzahl Systeme von Canvas zugreifen.

"Sie sehen ausschließlich die Dokumente, die wir ihnen senden, weil der Zugriff über die Zugriffszuordnung von Benutzergruppen eingeschränkt ist", erklärt Lai. "Alle im Unternehmen haben auch Zugriff auf den Bearbeitungsverlauf. Das ist eine weitere Sicherheitsebene, durch die sichergestellt wird, dass niemand etwas mit den Dokumenten anstellt."

Proaktive Bedrohungsüberwachung und -prävention

Auch die strengsten Sicherheitsmaßnahmen können Bedrohungen nicht ganz verhindern. Deshalb hat Atlassian einen mehrdimensionalen, sich ständig weiterentwickelnden Ansatz für die Prävention von Bedrohungen und das Schwachstellenmanagement gewählt. Atlassian verwendet automatisierte und manuelle Prozesse, um Schwachstellen in allen Cloud-Produkten zu identifizieren, zu überwachen und zu beheben. Außerdem sorgt das Unternehmen dafür, dass die IT-Teams seiner Kunden mit ähnlichen Tools ausgestattet werden.

Bug-Bounty-Programm

Atlassians Bug-Bounty-Programm spornt über 60.000 Cybersicherheitsforscher dazu an, die Produkte einem Penetrationstest zu unterziehen und eventuell gefundene Schwachstellen zu kennzeichnen. Sobald eine Schwachstelle protokolliert wurde, wird ein Ticket dafür erstellt und dem für das Produkt verantwortlichen Systembesitzer oder Entwicklerteam zugewiesen.

Konsistente Produkttests

Im Rahmen der CI/CD-Pipeline (Continuous Integration/Continuous Deployment) von Atlassian müssen Techniker für alle Container, die in den Entwicklungs-, Staging- oder Produktionsumgebungen eingesetzt werden, einen vollständigen Containersicherheitsscan ausführen.

Wenn Änderungen an vorhandenem Code vorgenommen werden, verwenden Atlassians Techniker einen "Peer Review, Green Build"-Prozess, um sicherzustellen, dass die Änderungen keine Probleme verursachen. Im Rahmen dieses Prozesses müssen alle Änderungen von mindestens einem Fachkollegen überprüft werden, bevor diese Codeänderung ausgeliefert wird.

Da viele Atlassian-Produkte auch auf Open-Source-Bibliotheken basieren, wird eine Kombination aus intern entwickelten, kommerziellen und Open-Source-Tools verwendet, um eventuelle Abhängigkeiten in den besagten Bibliotheken automatisch zu scannen und zu identifizieren. Diese könnten nämlich mit Sicherheitsschwachstellen in Zusammenhang stehen.

Proaktive Sicherheitserkennung

Da sich Cybersicherheitsbedrohungen ständig weiterentwickeln, hat sich Atlassian dafür entschieden, mithilfe der Plattform für Sicherheitsvorfälle und Ereignismanagement proaktive, geplante Suchen nach schädlichen Aktivitäten durchzuführen. Das Security Intelligence-Team führt regelmäßig Suchvorgänge nach Aktivitäten durch, die auf Atlassian oder seine Kunden abzielen.

Alle entdeckten Bedrohungen werden protokolliert, untersucht und dazu verwendet, die Erkennung zukünftiger Bedrohungen zu verbessern. Das Security Intelligence-Team führt wiederholte Erkennungen durch, um neue und bestehende Bedrohungen besser zu bekämpfen. Dadurch kann die heutige Bedrohungslandschaft besser nachvollzogen und ermittelt werden, wie sie in Zukunft aussehen wird.

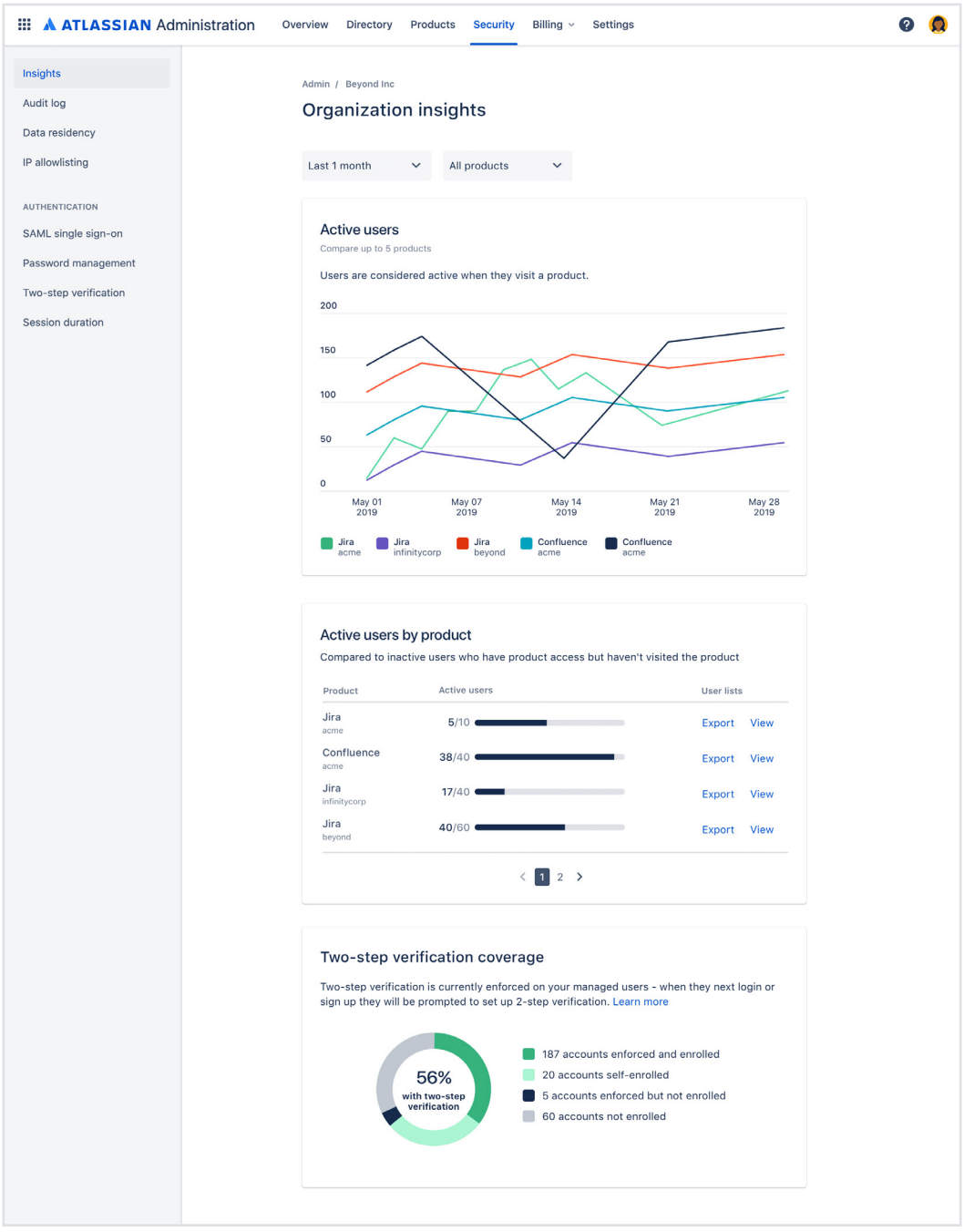
Sicherheitseinblicke für Administratoren

Atlassian glaubt an die proaktive Überwachung der Systeme im Hinblick auf Bedrohungen und Schwachstellen und möchte seinen Kunden deshalb die Möglichkeit geben, das gleiche zu tun. Aus diesem Grund hat Atlassian es Administratoren leicht gemacht, potenzielle Sicherheitsprobleme in ihren Atlassian-Produkten nachzuverfolgen.

Das Unternehmens-Audit-Protokoll von Atlassian Access dient als umfassendes Protokoll aller Administratoraktivitäten in Ihrer Atlassian Cloud-Organisation. Organisationsadministratoren können genau nachverfolgen, welche Site-Administratoren auf bestimmte Produktinstanzen zugreifen können und wann sie die Berechtigung dazu erhalten haben. Bei einem Datenverlust, etwa von unternehmenseigenen oder vertraulichen Daten, können Administratoren den Benutzerzugriff bei Bedarf einschränken und Aufzeichnungen zu Benutzeraktivitäten anzeigen, um Auffälligkeiten zu identifizieren.

> Wir verfügen über viele streng vertrauliche Daten rund um unser geistiges Eigentum, und diese möchten wir schützen. Das Büro unseres Chief Information Security Officer muss wissen, wer Zugriff darauf hat und was Benutzer mit den Daten machen können. Atlassian Access stellt sicher, dass die richtigen Personen Zugang zu den richtigen Dingen haben, und die falschen Leute keinen Zugang zu den falschen Dingen.
>
> **JIM TOMPKINS**
> **Programmmanager, Rockwell Automation, Atlassian-Enterprise-Kunde**

Auch das Tool für Unternehmenseinblicke ist in Atlassian Access enthalten. Es erlaubt Administratoren, sich einen Überblick über den Sicherheitsstatus von Benutzern aller Atlassian-Produkte zu verschaffen. Mithilfe von Unternehmenseinblicken können Administratoren nachverfolgen, bei wie vielen verwalteten Benutzern SAML-SSO oder die Zwei-Faktor-Authentifizierung tatsächlich aktiviert ist. Sie können auch anzeigen, wie viele Benutzer ein Produkt pro Tag oder Monat nutzen, und so besser nachvollziehen, welche Benutzer tatsächlich einen Zugriff und Berechtigungen benötigen.



Sichere Skalierung in der Cloud mit Atlassian

Sicherheitsfunktionen sind ein fester Bestandteil der Atlassian Cloud-Produkte und Sicherheitspraktiken und -prozesse sind fest in der Unternehmenskultur verankert. Atlassian Cloud Enterprise bietet eine bewährte Lösung für Unternehmen, die eine sichere, konforme und datenschutzorientierte Plattform benötigen, die sie bei der Skalierung unterstützt und Folgendes bietet:

- Unterstützung der Datenresidenz
- Verschlüsselung während der Übertragung und im Ruhezustand
- Einhaltung branchenführender Vorschriften wie SOC, ISO, DSGVO und vieles mehr
- Sämtliche Sicherheitsfunktionen von Atlassian Access sind ohne Zusatzkosten integriert, z. B. SAML-SSO, erzwungene Zwei-Faktor-Authentifizierung, benutzerdefinierte Authentifizierungsrichtlinien, automatisierte Benutzerbereitstellung bzw. Aufhebung derselben, Unternehmens-Audit-Protokolle, Unternehmenseinblicke usw.
- SLA für die Reaktion auf kritische Sicherheitsprobleme in 30 Minuten
- Telefonsupport rund um die Uhr durch ein fest zugeordnetes erfahrenes Team

Erfahren Sie, wie Ihr Unternehmen mit Atlassian Cloud Sicherheit auf Enterprise-Niveau erreichen kann.

Wenden Sie sich noch heute an Ihren lokalen Solution Partner.

ATLASSIAN

Benötigen Sie Hilfe? Wir haben die Lösung für Sie.

Wenden Sie sich an Ihren Atlassian Solution Partner, um mehr über Lösungen von Atlassian zu erfahren.

Partnername

- Standort
- E-Mail-Adresse
- Telefonnummern
- Website

ATLASSIAN