Datenschutz in Atlassian Cloud

Einführung

Daten sind das wichtigste Asset deines Unternehmens, doch es wird immer schwieriger, sie zu schützen und zu sichern. Wenn Daten nicht richtig geschützt sind, kann dich eine Datenschutzverletzung teuer zu stehen kommen. Im Jahr 2022 berichtete IBM, dass die durchschnittlichen Kosten einer Datenschutzverletzung 4,35 Millionen USD betrugen.

Welche Herausforderungen gibt es?

Verwaltung komplexer und vernetzter IT-Systeme	Die Verwaltung deiner IT-Infrastruktur macht viel Arbeit, weil die Anzahl der Produkte und Apps, die Teams verwenden, immer weiter zunimmt. Im Durchschnitt verwenden Unternehmen zwischen 100 und 200 Anwendungen, wobei viele von ihnen von Geschäftsbereichen außerhalb deiner IT-Abteilung verwaltet werden. Unabhängig von der Eigentümerschaft werden diese Apps und Produkte gemeinsam verwendet, sodass Daten zwischen ihnen fließen können, um die Zusammenarbeit zwischen funktionsübergreifenden Teams zu ermöglichen. Komplexe Umgebungen mit mehreren Apps vergrößern die Angriffsfläche und bergen Risiken, weil für die verschiedenen Apps unterschiedliche Sicherheitsstufen gelten.
Zugriff auf Daten nur durch berechtigte Personen	Wenn dein Unternehmen wächst, greifen mehr Menschen, Geräte und Anwendungen auf deine Daten zu, was das Risiko eines unbefugten Zugriffs erhöht. Es wird immer schwieriger, ein Gleichgewicht zwischen der Aufrechterhaltung der Produktivität der Mitarbeiter und der Eingrenzung der Zugangspunkte zu finden.
Anpassung an regulatorische	Für Branchen und Regionen gelten Anforderungen, die

Anforderungen	festlegen, welche Kontrollen vorhanden sein müssen, um regulatorische Verpflichtungen zu erfüllen und personenbezogene Daten zu schützen. Aber die Landschaft entwickelt sich ständig weiter und die Anforderungen sind dynamische Ziele, deren Verfolgung einige Zeit in Anspruch nimmt. Darüber hinaus wälzen diese Leitungsgremien Pflichten auf Unternehmen wie deines ab, wenn es darum geht nachzuweisen, ob diese Anforderungen erfüllt werden.
Schutz sensibler Daten	Die Daten deines Unternehmens sind alle wichtig, aber einige davon sind sensibler als andere, wie rechtliche Informationen oder Mitarbeiterdaten. Die korrekte Klassifizierung von Daten und die Anwendung geeigneter Sicherheitsvorkehrungen sind entscheidend für den Schutz vertraulicher Daten wie personenbezogenen Daten, Kreditkarten usw.
Wiederherstellung nach Ausfällen	Die Auswirkungen eines Ausfalls auf ein Unternehmen werden immer umfangreicher. Im Durchschnitt kann ein Ausfall von einer Minute ein Unternehmen 9.000 USD kosten. Multipliziert mit der Gesamtzahl der Ausfallzeiten kann ein Ausfall Hunderttausende von Dollar kosten. Aber Ausfälle wirken sich nicht nur auf deinen Umsatz aus. Sie können auch zu Geschäftsunterbrechungen, internen Produktivitätsverlusten, finanziellen Strafzahlungen und Rechtsstreitigkeiten führen.
Erkennung von Bedrohungen und die Reaktion darauf	Du kannst keine Bedrohungen kontrollieren, die du nicht sehen kannst. Dein Unternehmen muss über integrierte Funktionen zur Erkennung, Überwachung und Meldung von Bedrohungen verfügen. Viele Produkte bieten keine sofort einsatzbereiten Lösungen, weshalb Unternehmen zusätzliche Produkte verwalten müssen, die ihre bereits umfassende Liste von Anwendungen noch verlängern.
Bewertung der Sicherheit und des Datenschutzes von Marketplace-Apps	Marketplace-Apps bieten die nötige Flexibilität, damit du deine Komplettlösung anpassen und erweitern kannst. Viele Apps werden jedoch von Drittanbietern entwickelt und verwaltet. Die Installation einer App erfordert, dass mit dem Anbieter der App eine separate Geschäftsbeziehung eingegangen wird. Du solltest daher unbedingt die Apps auf deiner Instanz überprüfen, da sie mit Daten möglicherweise anders umgehen als das Produkt, das sie erweitern.

Zu diesen Herausforderungen kommen noch gute und schlechte Akteure hinzu, nämlich die Mitarbeiter.

Gute Akteure: Vielleicht hast du bereits ein eigenes Sicherheitsteam, das für den Schutz deiner Daten verantwortlich ist. Aber die meisten Mitarbeiter in deinem Unternehmen sind keine Experten. Sie denken nicht darüber nach, wie ihr eigenes Handeln zu einer Datenschutzverletzung führen kann. Zum Beispiel verwenden viele Mitarbeiter ihre Passwörter immer wieder. Sobald diese Anmeldeinformationen kompromittiert werden, können Hacker auf die Daten deines Unternehmens zugreifen.

Schlechte Akteure: Leider versuchen einige Menschen aktiv, sich unbefugten Zugriff auf deine Daten zu verschaffen und deinem Unternehmen zu schaden. In einigen Fällen können das verärgerte Mitarbeiter sein, aber auch Hacker versuchen oft, Schwachstellen in deinen Umgebungen auszunutzen.

Immer wieder ist der Faktor Mensch für Sicherheitslücken verantwortlich. Egal, ob es sich um die Verwendung gestohlener Anmeldeinformationen, um Phishing oder einfach um einen Fehler handelt, spielt der Mensch weiterhin eine große Rolle bei Vorfällen und Datenschutzverletzungen.

- *Verizon, Data Breach Investigation Report (DBIR) 2022*

Diese Herausforderungen kannst du durchaus bewältigen, du brauchst dazu aber die richtigen Tools. Deshalb haben wir Atlassian Cloud-Produkte und -Lösungen mit den speziellen Funktionen und Fähigkeiten entwickelt, die du zum Schutz deiner Daten benötigst.

Sichere Zusammenarbeit durch eine vernetzte Plattform und gemeinsame Verantwortung

Im Gegensatz zu selbstverwalteten Umgebungen funktioniert die Cloud gemäß dem Modell der geteilten Verantwortung. Das bedeutet, dass du und Atlassian gemeinsam für den Schutz deiner Daten zuständig seid.

[Modell für geteilte Verantwortung einfügen, das nur den Kunden und Atlassian anzeigt]

- **Atlassian** stellt sicher, dass die Infrastruktur, die unsere Cloud-Produkte unterstützt, sicher ist.
- **Du** verwaltest die Informationen deines Kontos sowie der Benutzer und Benutzerkonten, die auf deine Daten zugreifen, gemäß deinen Compliance-Verpflichtungen.

Wenn du eine Marketplace-App installierst, kommt ein Drittanbieter hinzu. Für die Installation der App musst du eine Geschäftsbeziehung mit einem Marketplace-Partner eingehen, die von deiner Beziehung zu Atlassian getrennt zu betrachten ist.

[Dieselbe Grafik wie oben einfügen, aber jetzt mit Marketplace. Ein Beispiel:]

In diesem Kontext spielen Atlassian und Marketplace-Partner im neuen Modell der geteilten Verantwortung beide eine wichtige Rolle:

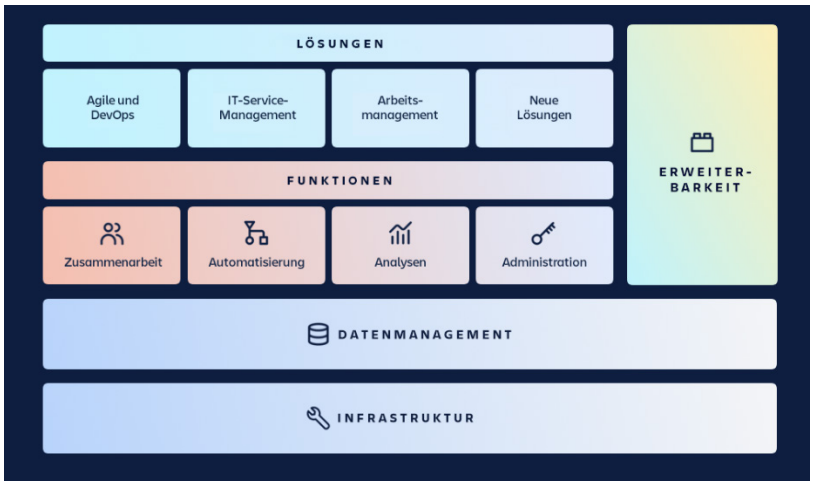
Marketplace-Partner	Marketplace-Partner sind für ihre eigene Infrastruktur verantwortlich. Sie sind verantwortlich für Folgendes: ● Entwickeln von Apps und betrieblichen Prozessen gemäß ihren gesetzlichen Verpflichtungen, den Entwicklerrichtlinien von Atlassian und den allgemeinen Best Practices der Branche für die Entwicklung und Wartung zuverlässiger, gesetzeskonformer und sicherer Apps ● Bereitstellen von Support und Informationen, um Kunden dabei zu helfen, fundierte Entscheidungen zu treffen
Atlassian	Atlassian ist verantwortlich für die Sicherheit der eigenen Infrastruktur und für die Unterstützung von Partnern und Kunden: ● Wir stellen Dokumentation, Sicherheitsstandards und Funktionen zur Verfügung, um Partnern dabei zu helfen, vertrauenswürdige Apps zu entwickeln, die den branchenüblichen Praktiken entsprechen. ● Wir arbeiten auch daran, zentralisierte Informationen und Kontrollen für eine Reihe von Vertrauensfaktoren bereitzustellen, sodass du Cloud-Apps anhand deiner Anforderungen bewerten und verwalten kannst.

DU	Du verwendest die von Atlassian und Marketplace-Partnern bereitgestellten Informationen sorgsam, um zu beurteilen, ob Apps den Richtlinien deines Unternehmens entsprechen. Du verwendest die verfügbaren Kontrollen, um deine installierten Apps zu verwalten.

Weitere Informationen zum Modell der geteilten Verantwortung findest du in unserer Zusammenfassung.

Wir haben dieses Modell auf die Atlassian-Plattform angewendet:

- Wir haben eine Infrastruktur für Unternehmen aufgebaut, die skalierbar zuverlässig und sicher ist.
- Wir haben Datenschutzkontrollen verbessert, damit du deine Daten absichern und verwalten kannst.
- Wir haben die Verwaltungsfunktionen zentralisiert.
- Unsere Plattform ist mit Tausenden von Apps und Integrationen erweiterbar.



In diesem White Paper erfährst du, wie wir Daten auf den drei Ebenen der Plattform schützen, welche Funktionen du nutzen kannst, um die Anforderungen deines Unternehmens zu erfüllen, und wie du deine Marketplace-Apps bewertest.

Abschnitt 1: Die Infrastrukturebene von Atlassian Cloud

Damit deine Teams ihre beste Arbeit leisten können, benötigen sie Zugriff auf deine Produkte und deine Daten – da sind Ausfälle keine Option. Ausfälle können trotzdem vorkommen. Deshalb musst du in der Lage sein, deine Systeme so schnell wie möglich wiederherzustellen, ohne Datenverlust zu erleiden.

Ausfälle können verursacht werden, wenn die Infrastruktur über einen längeren Zeitraum nicht betriebsfähig ist. Unabhängig davon, ob du deine Infrastruktur verwaltest oder Cloud-Produkte verwendest, ist dein Unternehmen darauf angewiesen, dass du und dein IT-Team den Service so schnell wie möglich wiederherstellt. Leider ist nicht immer klar, wie lange die Wiederherstellung dauern wird.

Wir haben die Atlassian Cloud auf einer Infrastruktur der Enterprise-Klasse aufgebaut, die zuverlässige Erlebnisse bietet. Daher musst du keine Produktivitätsverluste in deinen Teams oder Umsatzverluste für dein Unternehmen befürchten.

Was Atlassian tut: Daten schützen und Datenverlust minimieren

Die Cloud-Produkte von Atlassian werden auf der Infrastructure as a Service (IaaS) von Amazon Web Services (AWS) gehostet und in mehreren Regionen weltweit gehostet, darunter Regionen in den Vereinigten Staaten, Australien und der Europäischen Union. Jede dieser Regionen hat mehrere Verfügbarkeitszonen (VZs), die voneinander isoliert sind. Weil Daten auf andere VZs in einer Region repliziert werden, bleiben deine Daten bei einem VZ-Ausfall zugänglich, wodurch eine hohe Verfügbarkeit und ein Failover gewährleistet sind.

> ***Hinweis***: Wir bieten Datenresidenz an, wenn du Daten benötigst, die in einer bestimmten Region gehostet werden. Wenn diese Option aktiviert ist, verknüpft die Datenresidenz die abgedeckten Daten mit einer bestimmten Region.

Hochverfügbarkeit und Failover sind die erste Verteidigungslinie zur Wiederherstellung von Services, wenn es zum Ausfall auf Infrastrukturebene kommt. Wir betreiben auch ein Backup-Programm, das eine weitere Möglichkeit bietet, Daten wiederherzustellen.

Interne Systeme und wichtige Services, wie unsere Produkte, werden mithilfe der Snapshot-Funktion des Relational Database Service (RDS) von Amazon gesichert. Dadurch können wir tägliche Backups von jeder RDS-Instanz erstellen. Diese Snapshots werden 30 Tage lang aufbewahrt und mit AES-256 verschlüsselt. In Kombination mit Datenbanktransaktionsprotokollen ermöglichen die Snapshots eine Wiederherstellung zu einem bestimmten Zeitpunkt und reduzieren so das Datenverlustrisiko.

Diese Backups sind zudem sicher und unveränderlich. Backups für Produkt-SQL-Datenspeicher werden in einem Write-Once-Read-Many (WORM)-Tresor gespeichert und gesperrt. Dieser Prozess schützt Backups vor einer möglichen Löschung durch böswillige Akteure und betrügerische Software und schützt uns so vor vollständigem Datenverlust.

> ***Hinweis***
> Wir verwenden unsere Backups nicht, um vom Kunden initiierte Änderungen rückgängig zu machen, wie z. B. gelöschte Vorgänge oder Projekte. Um Datenverlust zu minimieren, musst du deshalb regelmäßige Backups deiner Daten erstellen. Weitere Informationen zu diesen Funktionen findest du im Abschnitt *Datenmanagement*.

Was Atlassian tut: Sicherheitsrisiken erkennen und beheben

Einer der häufigsten Gründe für Systemausfälle ist, dass Schwachstellen ausgenutzt wurden. Um dieses Risiko zu minimieren, nutzen wir Folgendes:

- **Externe Penetrationstests**: Sicherheitsberatungsunternehmen führen Penetrationstests für Produkte mit hohem Risiko durch, die beispielsweise Whitebox- oder codegestützt und bedrohungsbasiert sind. Die Validierung und die Ergebnisse werden in Form von Bewertungsschreiben vorgelegt und mehrmals pro Jahr veröffentlicht.
- **Atlassian Red Team**: Dieses Team ahmt echte Cyberszenarien nach, um Schwachstellen in unseren Systemen und Services zu identifizieren.
- **Bug-Bounty-Programm**: Dies ist ein wählbares Programm, das entwickelt wurde, um Schwachstellen in unseren Produkten zu identifizieren, indem wir Endbenutzer unsere Produkte testen lassen. Die Ergebnisse der Berichte werden regelmäßig veröffentlicht.

Was Atlassian tut: deine Geschäftsanforderungen erfüllen

Unser Ansatz hinsichtlich Zuverlässigkeit und Verfügbarkeit konzentriert sich nicht nur darauf, die richtigen Technologien einzusetzen. Wir haben Programme und Richtlinien eingeführt, die es uns ermöglichen, deine Geschäftsanforderungen zu unterstützen und gemäß den Branchenstandards zu arbeiten.

- **Business Continuity (BC)**: Die strategische und taktische Fähigkeit von Atlassian, Geschäftsunterbrechungen zu planen und darauf zu reagieren, um den Geschäftsbetrieb auf einem akzeptablen und vordefinierten Niveau fortzusetzen.
- **Disaster Recovery (DR)-Programm**: Prozesse, Richtlinien und Technologien, die sicherstellen, dass kritische IT-Systeme und -Services bei einem Ausfall schnell wiederhergestellt werden. Sollte es zu einem Ausfall kommen, definieren unsere RTOs und RPOs die maximale Zeit, die eine Wiederherstellung des normalen Betriebs und der Services dauern darf.

- **Service Level Agreements (SLAs)**: Finanziell abgesicherte garantierte Prozentsätze der monatlichen Verfügbarkeit für alle wichtigen Funktionen von Jira Software, Confluence und Jira Service Management mit Premium- und Enterprise-Cloud-Tarifen.
- **Simulierte Infrastrukturausfalltests:** Tests stellen sicher, dass wir nach einem VZ-Fehler mit minimalen Ausfallzeiten eine Wiederherstellung vornehmen können.

Die wichtigsten Punkte

Was Atlassian tut:

- Die Cloud-Plattform, Produkte und Lösungen von Atlassian werden in AWS-Regionen weltweit mit mehreren VZs gehostet, die Failover und Hochverfügbarkeit bieten, sodass sie widerstandsfähig gegen Ausfälle auf Infrastrukturebene sind.
- Wir führen ein Programm aus, das einen weiteren Mechanismus zur Sicherung interner Systeme und Services bereitstellt.
- Wir bieten ein etabliertes Disaster-Recovery-Programm, das es uns ermöglicht, Systeme und Services bei einem Ausfall wiederherzustellen. Unser Business-Continuity-Programm ist darauf ausgelegt, auf ungeplante Ereignisse zu reagieren und zuverlässige Produkte zu liefern, denen die Benutzer vertrauen können.
- Externe Penetrationstests, das Bug-Bounty-Programm und das Atlassian Red Team helfen dabei, unsere Widerstandsfähigkeit gegenüber dynamischen Bedrohungen zu belegen.

Abschnitt 2: Datenschutz, Management und Kontrolle

Der skalierbare Schutz deiner Daten ist eine Herausforderung. Das ist eine Tatsache. Wenn dein Unternehmen wächst, wirst du mit mehr Risiken konfrontiert, auf die du und deine Sicherheitsteams oft nur reagieren könnt. Selbst wenn du dein Team weiter ausbaust, kann dieses schnell überfordert werden.

Der Vorteil der Cloud-Nutzung ist, dass du jetzt ein weiteres Unternehmen, Atlassian, als Unterstützung hast. Denn wir sorgen dafür, dass unsere Systeme sicher bleiben, und wir haben Funktionen entwickelt, mit denen du proaktiv handeln kannst und nicht länger nur reagieren musst. Damit dies funktioniert, haben wir vor allem Lösungen entwickelt, die Folgendes direkt auf der Datenschutz-, Verwaltungs- und Kontrollebene unserer Plattform berücksichtigen:

- **Wiederherstellung**: Diese ermöglicht uns, bei Ausfällen eine schnelle Wiederherstellung zu erreichen, versehentliche Löschungen zu verhindern und Datenverluste zu minimieren, sodass Teams ihre Arbeit effizient und effektiv wieder aufnehmen können.
- **Sicherheit**: Dies sind Plattformkontrollen, die eine strikte Authentifizierung und Autorisierung, Verschlüsselung und Unterstützung mehrerer Regionen erzwingen. Dabei können Unternehmen flexibel entscheiden, ob zusätzliche Kontrollen für ihre Daten hinzugefügt und durchgesetzt werden sollen.

- **Datenschutz und Compliance**: Damit schützt du personenbezogene Daten und hast die notwendigen Kontrollen, um die regulatorischen Verpflichtungen einzuhalten.
- **Identitäts- und Zugriffsmanagement**: Damit reduzierst du das Risiko eines unbefugten Zugriffs auf Daten durch architektonische Kontrollen und kundenspezifische Funktionen.

Datenwiederherstellung

Wie im vorherigen Abschnitt erwähnt, trägt unsere Infrastruktur dazu bei, dass wir nach Ausfällen auf Infrastrukturebene eine Wiederherstellung vornehmen können. Trotzdem können andere Arten von Ausfällen auftreten, die sich erheblich auf dein Unternehmen auswirken und beispielsweise Umsatzverluste oder eine Minderung der Teamproduktivität nach sich ziehen können.

Laut dem Jahresbericht des Uptime Institute spielte menschliches Versagen bei etwa 60–80 % aller Ausfälle eine Rolle, was auf mangelnde Personalressourcen oder fehlende Schulung zurückzuführen sein könnte. Um dieses Risiko zu minimieren, musst du über eine geeignete Lösung verfügen.

Was Atlassian tut: versehentliches Löschen verhindern

Wir haben Schutzmechanismen in die Cloud-Architektur eingebaut, die verhindern, dass jemand versehentlich ein Produkt und die zugehörigen Daten löscht. Das verzögerte Löschen von Produkten wirkt wie ein Sicherheitsnetz. Anstatt das gesamte Produkt zu löschen, wird es in einen Ruhezustand versetzt, in dem du auf bestimmte Zeit nur eingeschränkten oder keinen Zugriff auf das Produkt hast. Dadurch können wir den Service für deine Produkte schnell wiederherstellen, um die Auswirkungen auf deine Teams zu minimieren. In Zukunft werden wir Funktionen zum sanften Löschen anbieten, die bestimmte Arten des Löschens verbieten und mehrere Schutzebenen bieten, um Fehler zu vermeiden.

Was du tust: Datenverlust in deinem Unternehmen reduzieren

Du solltest unbedingt regelmäßig deine eigenen Backups erstellen, um Folgendes sicherzustellen:

- **Business Continuity**: Dein IT-Team muss in der Lage sein, Daten nach einer versehentlichen Löschung wiederherzustellen (z. B. Jira-Projekte oder Confluence-Bereiche) oder Änderungen rückgängig zu machen.
- **Einhaltung von Vorschriften**: Die Richtlinien deines Unternehmens oder die regulatorischen Anforderungen, an die du dich halten musst, erfordern möglicherweise, dass du deine eigenen Datensicherungen erstellst, um die Einhaltung der Vorschriften zu gewährleisten.

- **Sammeln von Verlaufsdaten bei Rechtsstreitigkeiten**: Backups können verwendet werden, um zu zeigen, was sich in deinen Umgebungen geändert hat. Diese Informationen kannst du bei Rechtsstreitigkeiten verwenden.

Wir bieten eine sofort einsatzbereite Lösung namens Backup-Manager an, mit der du diese Backups erstellen kannst. Sie erlaubt dir, ein XML-Backup (Export) zu erstellen, das du nutzen kannst, um Daten (Import) in deiner Umgebung wiederherzustellen.

Zusätzlich zum Backup-Manager haben wir eine Plattform entwickelt, mit der Kunden mit extrem großen Datensätzen Daten schneller und zuverlässiger exportieren können. Darüber hinaus entwickeln wir neue Funktionen, die in der Atlassian-Administration (admin.atlassian.com) verfügbar sein werden und es dir ermöglichen, alle deine Daten bei Bedarf einfach zu sichern und wiederherzustellen. Als Teil dieser Arbeit haben wir kürzlich eine Befehlszeilenschnittstelle (CLI) eingeführt, mit der du Daten genauer und zuverlässiger als jemals zuvor sichern und wiederherstellen kannst!

Die wichtigsten Punkte

Was Atlassian tut**:**

- In die Atlassian-Plattform sind Schutzmaßnahmen integriert, um das Risiko zu mindern, dass ein Produkt versehentlich gelöscht wird.

Was du tust:

- Stelle mit dem Backup-Manager oder der Backup-CLI sicher, dass du deine Daten bei Bedarf immer zuverlässig wiederherstellen kannst.

Datensicherheit

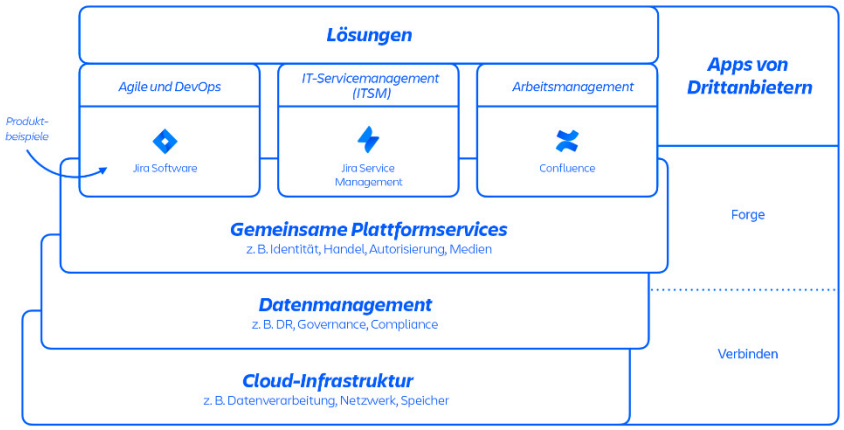
Das National Institute of Standards and Technology (NIST) definiert Datensicherheit folgendermaßen:

Ein Prozess zur Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit der Daten eines Unternehmens in einer Weise, die mit der Risikostrategie des Unternehmens vereinbar ist. Bevor sich ein Vorfall ereignet, müssen Unternehmen über eine Sicherheitsarchitektur und einen Reaktionsplan verfügen.

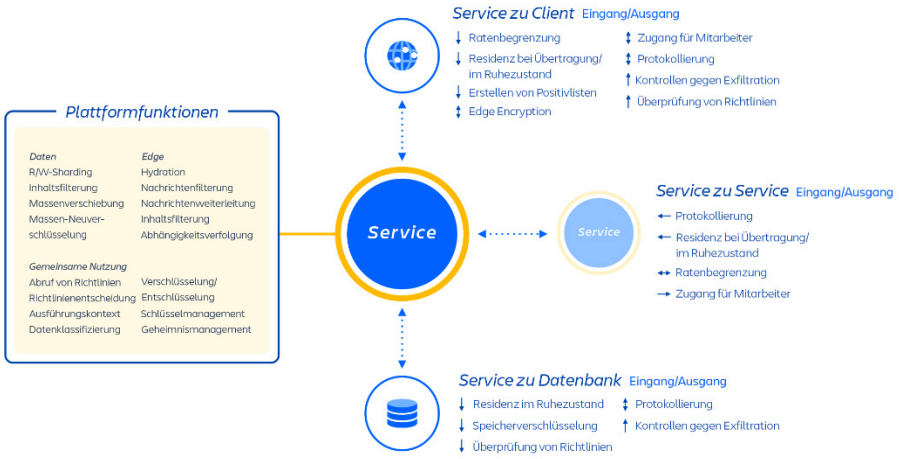
Was Atlassian tut: eine Mehrmandanten-Umgebung sicher verwalten

Wir verwenden die AWS-Architektur, um eine Reihe von Plattform- und Produktservices zu hosten, die in unseren Lösungen zum Einsatz kommen. Dazu gehören Plattformfunktionen, die von mehreren Atlassian-Produkten wie Media, Identity, Commerce und unserem Editor gemeinsam genutzt werden, sowie produktspezifische Funktionen wie Jira Issue-Service und Confluence Analytics.

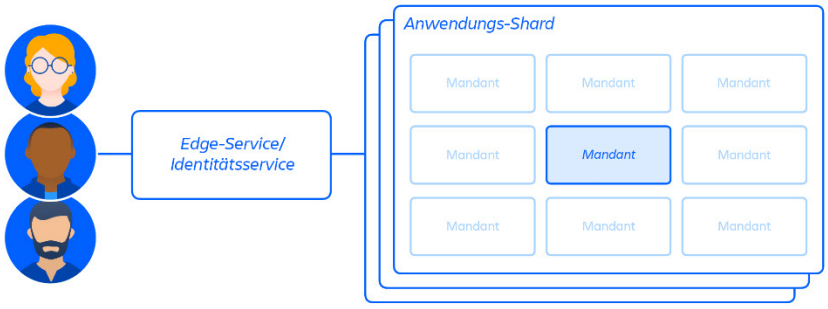
Atlassian-Entwickler stellen diese Services über eine intern entwickelte Plattform as a Service (PaaS) namens Micros bereit, die automatisch die Bereitstellung von Shared Services, Infrastrukturen, Datenspeichern und deren Verwaltungsfunktionen, einschließlich Sicherheits- und Compliance-Kontrolle, orchestriert.



Atlassian-Produkte bestehen aus mehreren containerisierten Services, die mithilfe von Micros auf AWS bereitgestellt werden. Atlassian-Produkte nutzen zentrale Plattformfunktionen, zu denen Netzwerke, Datenspeicherung, Observability und Analysen gehören. Diese Microservices basieren auf genehmigten technischen Stacks, die auf Plattformebene standardisiert sind.



Zusätzlich zu dieser Infrastruktur bieten wir eine mehrmandantenfähige Microservice-Architektur zusammen mit einer geteilten Plattform, die unsere Produkte unterstützt, aufbaut und betreibt. In einer Mehrmandanten-Architektur bedient ein einziger Service mehrere Kunden. Jeder Shard (im Prinzip ein Container) enthält die Daten für mehrere Mandanten, aber die Daten jedes Mandanten sind isoliert und für andere Mandanten nicht zugänglich.



Was Atlassian tut: Services skalieren und dabei die logische Trennung der Daten beibehalten

Unsere Kunden greifen auf eine gemeinsame cloudbasierte Infrastruktur zu, wenn sie unsere Cloud-Produkte nutzen. Wir haben daher Maßnahmen für eine logische Trennung ergriffen, damit die Aktionen eines Kunden die Daten oder Services anderer Kunden nicht gefährden.

Je nach Anwendung verfolgt Atlassian hier unterschiedliche Ansätze. Im Fall von Jira und Confluence Cloud setzen wir auf das Konzept "Tenant Context" (Mandantenkontext), um Kunden logisch zu isolieren. Dieses wird im Anwendungscode umgesetzt und über den von uns entwickelten TCS (Tenant Context Service) verwaltet. Das Konzept stellt Folgendes sicher:

- Die Daten jedes Kunden werden logisch getrennt von denen der anderen Mandanten aufbewahrt.
- Alle Anfragen, die von Jira oder Confluence verarbeitet werden, verfügen über eine mandantenspezifische Ansicht, sodass andere Mandanten davon nicht betroffen sind.

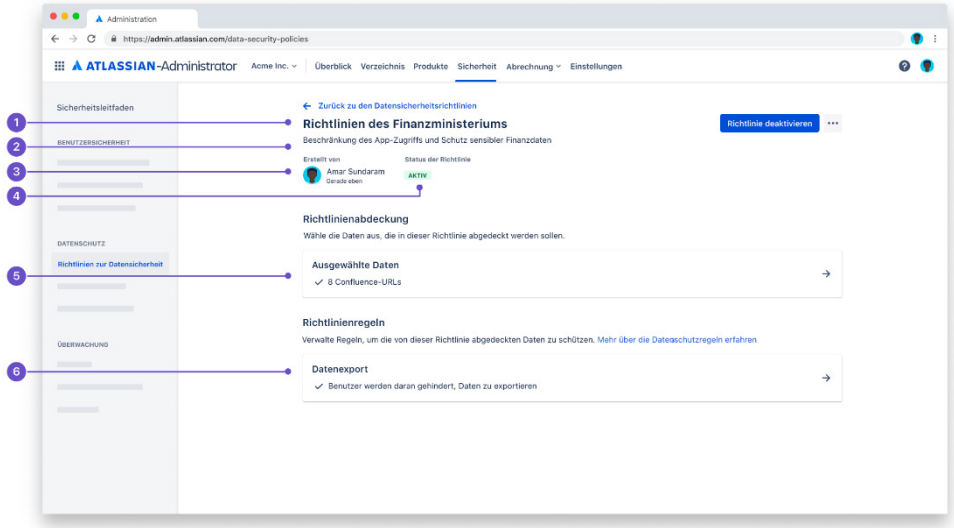
Vereinfacht gesagt speichert der TCS für die einzelnen Mandanten der Kunden einen Kontext. Der Kontext für jeden Mandanten ist einer eindeutigen ID zugeordnet, die zentral vom TCS gespeichert wird, und enthält eine Reihe von Metadaten, die mit diesem Mandanten verknüpft sind. Diese enthalten z. B. Informationen dazu, in welchen Datenbanken sich der Mandant befindet, welche Lizenzen der Mandant hat, auf welche Funktionen er zugreifen kann sowie eine Reihe anderer Konfigurationsinformationen. Wenn ein Kunde auf Jira oder Confluence Cloud zugreift, stellt der TCS die Metadaten anhand der Mandanten-ID zusammen und verknüpft diese dann mit allen Aktionen, die der Mandant im Sitzungsverlauf in der Anwendung vornimmt.

Dies schützt vor mandantenübergreifenden Datenlecks oder anderen Problemen, wie z. B. falschen Datenbankverbindungen, und bietet so quasi einen zusätzlichen Schutzmechanismus.

Was du tust: Content Governance implementieren

Wir sorgen dafür, dass nur autorisierte Personen Zugriff auf deine Daten haben. Aber damit ist noch nicht geregelt, wie Benutzer, Anwendungen und sogar Personen außerhalb deines Unternehmens mit deinen Inhalten interagieren.

Bald werden wir Datenschutzrichtlinien anbieten, die es dir ermöglichen, deine Daten zusätzlich zu schützen.



Anstatt sich darauf zu beschränken, Benutzerberechtigungen zu gewähren oder zu widerrufen, kannst du deren Aktionen einschränken. Du kannst zum Beispiel eine Richtlinie für eine deiner Sites erstellen, die es deinen Teams untersagt, Confluence-Seiten zu exportieren, wodurch das Risiko einer Datenexfiltration oder eines anderen Datenverlusts verringert wird.

Du kannst zudem nicht nur die Richtlinienabdeckung definieren, also die Anzahl der Produkte, für die die Richtlinie gilt, wenn du mehr als ein Produkt hast, sondern auch die Regeln – Sicherheitskontrollen –, die als Teil der Richtlinie konfiguriert sind. Weitere Informationen kannst du in unserer Dokumentation nachlesen.

Schütze vertrauliche Daten durch Zugriffsbeschränkungen

Datenverschlüsselung ist nach wie vor einer der wichtigsten Mechanismen, um sensible Daten zu schützen. Bei der Datenverschlüsselung werden deine Daten mit einem Chiffretext versehen, sodass niemand sie lesen kann, sofern die Person keinen Schlüssel für die Chiffre hat.

Was Atlassian tut: Daten bei der Übertragung und Speicherung verschlüsseln

Bei unseren Cloud-Produkten bringt Atlassian hauptsächlich das Modell der geteilten Verantwortung zur Anwendung. Wir verschlüsseln deine Daten während der Übertragung mit TLS 1.2+ mit Perfect Forward Secrecy (PFS) und am Speicherort mit AES-256. Wir verwenden den Key Management Service (KMS) von AWS, um unsere Verschlüsselungsschlüssel zu verwalten, sodass nur Personen mit autorisierten AWS-Rollen und -Berechtigungen auf diese Schlüssel zugreifen und deine Daten entschlüsseln können.

Was du tust: festlegen, wer deine Daten entschlüsseln kann

Dein Unternehmen benötigt womöglich weitere Verschlüsselungsfunktionen, die über die sofort einsatzbereiten Funktionen in der Atlassian-Plattform hinausgehen. Demnächst bieten wir die Bring Your Own Key (BYOK)-Verschlüsselung an, mit der du Schlüssel in deinem AWS-Konto über den AWS Key Management Service (KMS) generieren und hosten kannst. Abonniere die Cloud-Roadmap, um auf dem Laufenden zu bleiben.

Erfülle gesetzliche Anforderungen an die Datenresidenz

Unternehmen arbeiten oft in mehreren Regionen, in denen Daten an bestimmten Orten gespeichert werden müssen, um Risiken zu minimieren und sich vor unbefugter Nutzung personenbezogener Daten zu schützen. AWS verfügt ohnehin über Regionen auf der ganzen Welt, sodass wir die Anzahl der Standorte, an denen unsere Produktdaten gehostet werden können, erweitern können.

Was du tust: bestimmen, wo deine Daten gespeichert werden müssen

Standardmäßig werden alle Produkte am globalen Standort gehostet, der alle unsere AWS-Regionen einschließt. Wir bieten jedoch Datenresidenz an, damit du im Umfang enthaltene Daten einem bestimmten Standort zuordnen kannst. Aktuell bieten wir Datenresidenz in den Vereinigten Staaten, im Adun-Pazifik-Raum (APAC), in der Europäischen Union (EU), in Deutschland und in Singapur an. Um dich besser zu unterstützen, erweitern wir diese Regionen ständig.

Wie im Abschnitt "Infrastruktur" erwähnt, hat jede Region mehrere Verfügbarkeitszonen (VZs). Wenn es in der Region, in der du deine Daten gespeichert hast, zu einem VZ-Ausfall kommt, führe ein Failover auf eine andere VZ in derselben Region durch, sodass du bei einem Ausfall weiterhin deinen regulatorischen Verpflichtungen nachkommen kannst. Wir bieten kein regionsübergreifendes Failover an.

In einigen Fällen kann es vorkommen, dass bestimmte Anforderungen dich daran hindern, alle deine Daten in die Cloud zu verlegen, du deinen Teams aber trotzdem die Nutzung der Atlassian Cloud ohne diese Einschränkungen ermöglichen möchtest. Anwendungstunnel bieten

dafür ein sicheres Gateway zwischen unseren selbstverwalteten Produkten und Cloud-Produkten. Dadurch kannst du deine Atlassian-Produkte integrieren und sicher Daten und Funktionen zwischen ihnen austauschen, ohne dein Netzwerk zu gefährden oder eingehende Verbindungen oder IPs in die Positivliste aufzunehmen.

Die wichtigsten Punkte

- Was Atlassian tut:
    - Wir verwenden die AWS-Architektur, um verschiedene Plattform- und Produktservices zu hosten, die in unseren Lösungen verwendet werden. Diese Services werden über eine PaaS namens Micros bereitgestellt, welche die Bereitstellung dieser Services orchestriert. Sicherheits- und Compliance-Kontrollen werden in diesem Rahmen bereitgestellt.
    - Die Atlassian-Plattform, -Produkte und -Lösungen verwenden eine mehrmandantenfähige Microservice-Architektur mit strikter Mandantenisolierung, um den Zugriff auf Daten über den Tenant Context Service (TCS) zu verhindern. Jeder Mandant verfügt über eine eindeutige ID und Metadaten zum Schutz vor mandantenübergreifenden Datenlecks.
    - Wir verschlüsseln Daten während der Übertragung und der Speicherung, um deine Daten zu schützen.
    - Wir erweitern die Anzahl der von uns unterstützten AWS-Regionen, damit du deine regulatorischen Anforderungen erfüllen kannst.
- Was du tust:
    - Nutze BYOK, um deinen eigenen AWS-Schlüssel zu generieren und so die Anzahl der Personen zu reduzieren, die deine Daten entschlüsseln können.
    - Verwende Datensicherheitsrichtlinien, um Content Governance auf deine Daten anzuwenden und so zusätzlichen Schutz zu bieten.
    - Aktiviere die Datenresidenz, um deine Daten in bestimmten Regionen zu hosten und deine regulatorischen Anforderungen zu erfüllen.

Datenschutz und Compliance

Datenschutz und Compliance sind zwei Begriffe, die oft synonym verwendet werden.

- **Datenschutz**: Die Aufgabe des Datenschutzes ist zu gewährleisten, dass personenbezogene Daten der jeweiligen Person gehören und diese das Recht hat zu bestimmen, was, wie, wann und durch wen der Zugriff auf ihre Daten erfolgt. Es liegt in der Verantwortung der Unternehmen, die entsprechenden Anforderungen zu erfüllen, um diesen Wünschen zu entsprechen.
- **Compliance:** Compliance bezieht sich auf eine Reihe von Richtlinien, regulatorischen Anforderungen oder Gesetzen, die die Bedingungen festlegen, die erfüllt sein müssen, um als sicher, zuverlässig und privat zu gelten.

Kurz gesagt konzentriert sich Datenschutz auf den Schutz personenbezogener Daten, während die Compliance neben der Bestimmung weiterer Sicherheitsbedingungen ein Muster vorgibt, wie dies bewerkstelligt wird.

Was Atlassian tut: Compliance- und regulatorische Kontrollen in unsere Produkte integrieren

Um eine Compliance-Zertifizierung oder -Bescheinigung zu erhalten, müssen wir nachweisen, dass wir die zahlreichen Kontrollen implementiert haben, die in diesen spezifischen Frameworks beschrieben sind. Die Art der Kontrollen und die Komplexität ihrer Implementierung hängen von der Branche ab, die sie unterstützen.

Aktuell unterstützen wir die folgenden Frameworks, Gesetze und Zertifizierungen:

Jede unserer Compliance-Zertifizierungen wird von unabhängigen Dritten validiert, um sicherzustellen, dass wir alle relevanten Anforderungen erfüllen.

Auch Unternehmen, die womöglich in weniger stark regulierten Branchen tätig sind, profitieren davon, dass du dieselbe Infrastruktur mit erweiterten Kontrollen verwendest.

Was Atlassian tut: sicherstellen, dass deine Daten privat bleiben

Es ist überaus wichtig, dass du deine Daten geheim hältst, und das erfordert mehr als nur technische Kontrollen. Wir haben uns auch auf die Erstellung von Richtlinien und Programmen konzentriert, die Folgendes umfassen:

- Datenschutzrichtlinie
- Richtlinien zum Datenmanagement
- Richtlinien zum eingeschränkten Zugriff auf Daten
- Zusatz zum Datenschutz

Was du tust: deine Produkte gesetzeskonform betreiben

Zur Erfüllung deiner regulatorischen Verpflichtungen gehört, dass du deine Produkte gesetzeskonform betreibst. Wir stellen dir Funktionen wie Datenresidenz und Dokumentation zur Verfügung, um dies zu ermöglichen. Für den Fall, dass du beispielsweise HIPAA-konform arbeiten musst, haben wir einen Implementierungsleitfaden erstellt, in dem du erfährst, wie du infrage kommende Atlassian-Produkte verwendest, um sie HIPAA-konform zu betreiben.

Die wichtigsten Punkte

- Was Atlassian tut:
  - Wir integrieren Kontrollen in unsere Infrastruktur, Produkte und Lösungen, die es uns ermöglichen, die Einhaltung von Vorschriften in verschiedenen Frameworks zu erreichen, und wir werden jedes Jahr einer unabhängigen Prüfung durch Dritte unterzogen, um sicherzustellen, dass wir rechtskonform arbeiten.
  - Wir führen unser Datenschutzprogramm gemäß den Branchenstandards durch.
- Was du tust:
  - Du verarbeitest deine Daten gesetzeskonform, um deinen regulatorischen Verpflichtungen nachzukommen.

Identitäts- und Zugriffsmanagement

Gartner definiert Identitäts- und Zugriffsmanagement (Identity and Access Management – IAM) folgendermaßen:
Eine Sicherheits- und Geschäftsdisziplin, die mehrere Technologien und Geschäftsprozesse umfasst, um berechtigten Personen oder Geräten zu helfen, aus den richtigen Gründen und zur richtigen Zeit auf die richtigen Ressourcen zuzugreifen und gleichzeitig unbefugten Zugriff und Betrug abzuwehren.

Hierbei geht es kurz gesagt um den Schutz deiner Daten, indem sichergestellt wird, dass nur berechtigte Personen, Geräte und Anwendungen darauf zugreifen können. Leider sind kompromittierte Anmeldeinformationen nach wie vor eine der Hauptursachen für Datenschutzverletzungen. Deshalb haben wir einen gemeinsamen Ansatz für das Identitäts- und Zugriffsmanagement gewählt.

Was Atlassian tut: die Authentifizierung und Autorisierung von Services erzwingen

Für unsere Plattform wenden wir für den Datenzugriff das Prinzip der geringsten Rechte an. Das bedeutet, dass nur der Service Zugriff erhält, der für das Speichern, Verarbeiten oder Abrufen der jeweiligen Daten zuständig ist. Beispielsweise haben wir für unsere

Medienservices, die dir einen konsistenten Datei-Upload und -Download in allen unseren Cloud-Produkten bieten, fest zugeordneten Speicher bereitgestellt, auf den keine anderen Atlassian-Services Zugriff haben. Jeder Service, der Zugriff auf die Medieninhalte benötigt, muss mit der API für Medienservices interagieren. Demzufolge sorgt eine sichere Authentifizierung und Autorisierung auf Serviceebene außerdem für eine strikte Aufgabentrennung und den Datenzugriff nach dem Prinzip der geringsten Rechte.

Wir verwenden JSON-Web-Token (JWTs), um die Signaturberechtigung außerhalb der Anwendung sicherzustellen und damit unsere Identitätssysteme und den Mandantenkontext zur zentralen Informationsquelle zu machen. Token dürfen ausschließlich für die Zwecke verwendet werden, für die sie autorisiert sind. Wenn von dir oder jemandem in deinem Team ein Microservice oder Shard abgerufen wird, werden die Token an dein Identitätssystem übermittelt und verglichen. Durch diesen Prozess wird sichergestellt, dass das Token aktuell und signiert ist, bevor die entsprechenden Daten freigegeben werden. Sollte ein Service kompromittiert werden, begrenzen diese Autorisierungs- und Authentifizierungsregeln für den Zugriff auf Microservices den Schaden deutlich.

Natürlich wissen wir, dass Identitätssysteme manchmal kompromittiert werden können. Um dieses Risiko zu mindern, wenden wir zwei Mechanismen an. Zum einen sind der TCS und die Identitätsproxys hochgradig repliziert. Wir haben ein TCS-Sidecar für fast jeden Microservice und verwenden Sidecar-Proxys, die sich von der Identitätsautorität ableiten, sodass mehrere Tausend dieser Services gleichzeitig ausgeführt werden. Falls in einem oder mehreren Services anormales Verhalten auftritt, können wir dieses schnell erkennen und das Problem beheben.

Darüber hinaus warten wir nicht darauf, dass jemand eine Schwachstelle in unseren Produkten oder unserer Plattform entdeckt. Wir identifizieren diese Szenarien aktiv, damit sie nur minimale Auswirkungen auf dich haben. Zudem laufen eine Reihe von Sicherheitsprogrammen, damit Sicherheitsbedrohungen erkannt, gefunden und entsprechende Maßnahmen eingeleitet werden können.

Wir stellen sicher, dass Anfragen an Microservices Metadaten zu dem Kunden oder Mandanten enthalten, der den Zugriff anfordert. Dieser Vorgang wird als Tenant Context Service bezeichnet. Die Informationen hierfür kommen direkt aus unseren Bereitstellungssystemen. Wenn eine Anfrage gestartet wird, wird der Kontext im ausgeführten Servicecode, der zur Autorisierung des Benutzers verwendet wird, gelesen und internalisiert. Sämtliche Service- und damit Datenzugriffe in Jira und Confluence erfordern diesen Mandantenkontext, andernfalls wird die Anfrage abgelehnt.

Die Authentifizierung und Autorisierung von Services erfolgt über das Atlassian Service Authentication Protocol (ASAP). Eine explizite Positivliste legt fest, welche Services kommunizieren dürfen, und Autorisierungsdetails geben an, welche Befehle und Pfade verfügbar sind. Auf diese Weise werden laterale Bewegungen im Falle einer Kompromittierung eines Service eingeschränkt.

Die Authentifizierung und Autorisierung von Services sowie der Ausgang werden von diversen fest zugeordneten Proxys gesteuert. Auf diese Weise haben Schwachstellen im Anwendungscode keinen negativen Einfluss auf diese Kontrollen. Für die Remote Code Execution wäre die Kompromittierung des zugrunde liegenden Hosts und die Umgehung von Docker-Containergrenzen erforderlich, nicht nur die Möglichkeit, die Anwendungslogik zu ändern. Stattdessen markiert unsere Angriffserkennung auf Hostebene Diskrepanzen.

Diese Proxys beschränken das Ausgangsverhalten basierend auf dem beabsichtigten Verhalten des Service. Services, die keine Webhooks aussenden oder mit anderen Microservices kommunizieren müssen, wird dies untersagt.

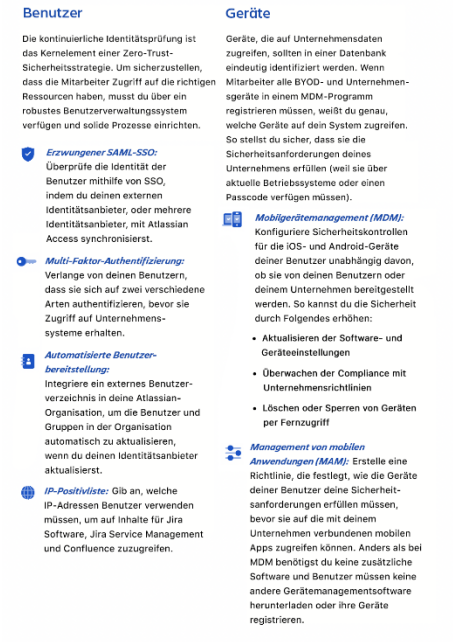
Was du tust: die Authentifizierung und Autorisierung von Benutzern und Geräten erzwingen

Atlassian Access bietet Admins IAM-Funktionen, mit denen du von der Atlassian-Administration aus Sicherheits- und Governance-Mechanismen auf deine Benutzer und Geräte anwenden und somit einen Zero-Trust-Ansatz implementieren kannst.

Benutzer Die kontinuierliche Identitätsprüfung ist das Kernelement einer Zero-Trust-Sicherheitsstrategie. Um sicherzustellen, dass die Mitarbeiter Zugriff auf die richtigen Ressourcen haben, musst du über ein robustes Benutzerverwaltungssystem verfügen und solide Prozesse einrichten.	• **Erzwungener SAML-SSO**: Überprüfe die Identität der Benutzer mithilfe von SSO, indem du deinen externen Identitätsanbieter, oder mehrere Identitätsanbieter, mit Atlassian Access synchronisierst. • **Multi-Faktor-Authentifizierung**: Verlange von deinen Benutzern, dass sie sich auf zwei verschiedene Arten authentifizieren, bevor sie Zugriff auf Unternehmenssysteme erhalten. • **Automatisierte Benutzerbereitstellung**: Integriere ein externes Benutzerverzeichnis in deine Atlassian-Organisation, um die Benutzer und Gruppen in der Organisation automatisch zu aktualisieren, wenn du deinen Identitätsanbieter aktualisierst. • **IP-Positivliste**: Gib an, welche IP-Adressen Benutzer verwenden müssen, um auf Inhalte für Jira Software, Jira Service Management und Confluence zuzugreifen. • **Sicherheit für externe Benutzer**: Verpflichte externe Benutzer, die mit

	Personen innerhalb deines Unternehmens zusammenarbeiten, zur Zwei-Faktor-Authentifizierung oder zu einer Verifizierung in Intervallen (in Kürze verfügbar).

Geräte
Geräte, die auf Unternehmensdaten zugreifen, sollten in einer Datenbank eindeutig identifiziert werden. Wenn Mitarbeiter zum Beispiel alle BYOD- und Unternehmensgeräte in einem MDM-Programm registrieren müssen, weißt du genau, welche Geräte auf dein System zugreifen. So kannst du sicherstellen, dass sie die Sicherheitsanforderungen deines Unternehmens erfüllen (weil sie über aktuelle Betriebssysteme oder ein Passwort verfügen müssen).
	• **Mobilgerätemanagement (MDM):** Konfiguriere Sicherheitskontrollen für die iOS- und Android-Geräte deiner Benutzer unabhängig davon, ob sie von deinen Benutzern oder deinem Unternehmen bereitgestellt werden. So kannst du die Sicherheit durch Folgendes erhöhen:
	  ○ Aktualisieren der Software- und Geräteeinstellungen
	  ○ Überwachen der Compliance mit Unternehmensrichtlinien
	  ○ Löschen oder Sperren von Geräten per Fernzugriff
	• **Management von mobilen Anwendungen (MAM)**: Erstelle eine Richtlinie, die festlegt, wie die Geräte deiner Benutzer deine Sicherheitsanforderungen erfüllen müssen, bevor sie auf die mit deinem Unternehmen verbundenen mobilen Apps zugreifen können. Anders als bei MDM benötigst du keine zusätzliche Software und Benutzer müssen keine andere Gerätemanagementsoftware herunterladen oder deine Geräte registrieren.



Benutzer

Die kontinuierliche Identitätsprüfung ist das Kernelement einer Zero-Trust-Sicherheitsstrategie. Um sicherzustellen, dass die Mitarbeiter Zugriff auf die richtigen Ressourcen haben, musst du über ein robustes Benutzerverwaltungssystem verfügen und solide Prozesse einrichten.

Erzwungener SAML-SSO: Überprüfe die Identität der Benutzer mithilfe von SSO, indem du deinen externen Identitätsanbieter, oder mehrere Identitätsanbieter, mit Atlassian Access synchronisierst.

Multi-Faktor-Authentifizierung: Verlange von deinen Benutzern, dass sie sich auf zwei verschiedene Arten authentifizieren, bevor sie Zugriff auf Unternehmenssysteme erhalten.

Automatisierte Benutzerbereitstellung: Integriere ein externes Benutzerverzeichnis in deine Atlassian-Organisation, um die Benutzer und Gruppen in der Organisation automatisch zu aktualisieren, wenn du deinen Identitätsanbieter aktualisierst.

IP-Positivliste: Gib an, welche IP-Adressen Benutzer verwenden müssen, um auf Inhalte für Jira Software, Jira Service Management und Confluence zuzugreifen.

Geräte

Geräte, die auf Unternehmensdaten zugreifen, sollten in einer Datenbank eindeutig identifiziert werden. Wenn Mitarbeiter alle BYOD- und Unternehmensgeräte in einem MDM-Programm registrieren müssen, weißt du genau, welche Geräte auf dein System zugreifen. So stellst du sicher, dass sie die Sicherheitsanforderungen deines Unternehmens erfüllen (weil sie über aktuelle Betriebssysteme oder einen Passcode verfügen müssen).

Mobilgerätemanagement (MDM): Konfiguriere Sicherheitskontrollen für die iOS- und Android-Geräte deiner Benutzer unabhängig davon, ob sie von deinen Benutzern oder deinem Unternehmen bereitgestellt werden. So kannst du die Sicherheit durch Folgendes erhöhen:

- Aktualisieren der Software- und Geräteeinstellungen
- Überwachen der Compliance mit Unternehmensrichtlinien
- Löschen oder Sperren von Geräten per Fernzugriff

Management von mobilen Anwendungen (MAM): Erstelle eine Richtlinie, die festlegt, wie die Geräte deiner Benutzer deine Sicherheitsanforderungen erfüllen müssen, bevor sie auf die mit deinem Unternehmen verbundenen mobilen Apps zugreifen können. Anders als bei MDM benötigst du keine zusätzliche Software und Benutzer müssen keine andere Gerätemanagementsoftware herunterladen oder ihre Geräte registrieren.

Abschnitt 3: Zentralisierter Admin

Als Admin musst du alle deine Atlassian-Produkte im Blick haben. In selbstverwalteten Umgebungen ist das aber nicht ganz einfach. Selbstverwaltete Produkte sind von Natur aus voneinander isoliert, um zu verhindern, dass von anderen Instanzen aus auf Daten zugegriffen werden kann. Allerdings fehlen dir hierdurch die Mechanismen, um zu sehen, was in deiner Umgebung vor sich geht. In der Cloud kannst du deine Daten bei Bedarf weiterhin isoliert aufbewahren. Aber eine zentrale administrative Oberfläche erleichtert dir die Verwaltung deiner Atlassian-Produkte und bietet transparentere Einblicke zum Schutz deiner Daten.

Diese zentralisierte Verwaltungsfunktion namens Atlassian-Administration basiert auf der Atlassian-Plattform und wurde mit Folgendem optimiert:

- **Überwachung und Berichterstellung**: Halte deine Sicherheits- und Compliance-Status mit Funktionen zur Erkennung und Prüfung von Bedrohungen aufrecht.
- **Produkt- und Organisationslebenszyklus-Management**: Verwalte deine Produkte und deine Organisation, um deine Anforderungen effektiv zu erfüllen.

Überwachung und Berichterstellung

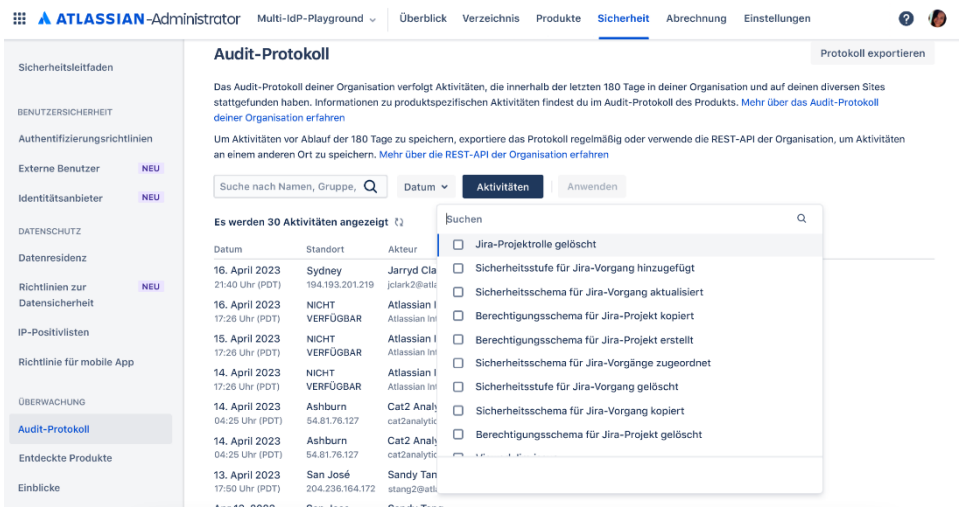
Ein Einblick in deine Instanz kann Unternehmen im großen Umfang zahlreiche Vorteile bieten. Davon abgesehen können Unternehmen jeder Größe von Tools zur Bedrohungserkennung profitieren.

Tools zur Bedrohungserkennung überwachen dein Netzwerk, um bösartige Aktivitäten zu erkennen, sodass dein Sicherheitsteam diese Gefahr schnell eindämmen kann. Die Erkennung

von Bedrohungen ermöglicht dir außerdem, Risiken zu priorisieren und Informationen in Echtzeit zu erhalten, um auf verdächtiges Verhalten zu reagieren, bevor es zu einem riskanten Vorfall mit weitreichender Wirkung kommt.

Was du tust: Ereignisse verfolgen, die in deiner Instanz stattfinden

Cloud-Produkte enthalten im Standard- und Premium-Tarif Audit-Protokolle, mit denen du wichtige produktinterne Ereignisse verfolgen kannst. Dennoch bieten sie keinen vollständigen Einblick in die Sicherheit deiner Daten in all deinen Atlassian-Produkten an einem Ort. Mit Atlassian Access stehen dir Audit-Protokolle der Organisation zur Verfügung, in denen Ereignisse wie Änderungen des Zugriffs einer Person auf deine Produkte oder Auffälligkeiten beim administrativen Zugriff aufgezeichnet werden. Im Gegensatz zu Produkt-Audit-Protokollen, deren Aufbewahrung vom Speicherplatzvolumen in deinem Tarif abhängt, werden die Audit-Protokolle der Organisation 180 Tage lang aufbewahrt, um dir zusätzliche Sicherheit zu bieten.



Wenn du für dein Unternehmen eine höhere Granularität benötigst, kannst du im Cloud Enterprise-Tarif auswählen, ob du von Benutzern erstellte Aktivitäten in deine Audit-Protokolle aufnehmen möchtest. Auf diese Weise kannst du Produktaktionen sowohl für nicht verwaltete als auch für verwaltete Umgebungen an einem zentralen Ort verfolgen. Weitere Informationen findest du in unserem Community-Beitrag zu Audit-Protokollen.

Was du tust: potenzielle Bedrohungen überwachen

Die Anwendung von Kontrollen sorgt für einen besseren Schutz deiner Daten und das Risiko von Datenschutzverletzungen durch Benutzer verringert sich. Dennoch sollten du vor allem über die Fähigkeit verfügen, deine Umgebung zu überwachen, um Bedrohungen zu stoppen, bevor sie auftreten.

Die Bedrohungserkennung gewährt dir noch mehr Kontrolle über deine Instanz, da du alltägliche Ereignisse schnell verfolgen kannst, um böswillige Aktivitäten zu identifizieren.

Einer der vielen Vorteile von SaaS-Lösungen ist, dass Teams ganz einfach mit der Arbeit loslegen können. Leider machen sie es Teams auch einfacher, neue Versionen von Produkten herunterzuladen, die nicht der Kontrolle deiner IT-Abteilung unterliegen, was eine weitere Möglichkeit für einen potenziell böswilligen Datenzugriff eröffnet. Mit der automatischen Produktfindung kannst du von der Atlassian-Administration aus nahtlos auf diese Informationen zugreifen und sofort Maßnahmen ergreifen.

Die automatische Produktfindung analysiert täglich, ob Instanzen von jemandem erstellt wurden, dessen E-Mail-Adresse an die Domain deines Unternehmens angehängt ist. Sie sendet dir täglich eine E-Mail mit diesen Daten. Über die Atlassian-Administration erkennst du, wer die Instanz erstellt hat und wie viele Benutzer sie verwenden. Du können also entscheiden, ob dein IT-Team mit deren Verwaltung beginnen soll oder ob du den Besitzer der Instanz in deine vom Unternehmen verwaltete Instanz holen möchtest.

Bald wirst du in der Lage sein, mithilfe eines inhaltsbasierten Ansatzes festzulegen, wie deine Daten in Atlassian-Produkten verwendet werden dürfen. Dieser unterscheidet sich von einem benutzerbasierten Ansatz, bei dem bestimmte Berechtigungen erteilt oder widerrufen werden, die es Benutzern oder Apps ermöglichen, bestimmte Aktionen auszuführen. Weitere Informationen erhältst du in unserer Dokumentation.

Du solltest jedoch auch wissen, wo die Daten gespeichert werden. Vor allem in großen Unternehmen haben die Teams oft keinen Überblick darüber, welche Produkte dein IT-Team unterstützt. Es ist eigentlich nicht ungewöhnlich, dass Mitarbeiter neue Produktinstanzen zur Erledigung ihrer Arbeit einrichten. Leider können diese neuen Instanzen das Unternehmen anfällig für eine Datenschutzverletzung machen. Bald wirst du mit Produktanfragen deine verwalteten Benutzer daran hindern können, neue Produkte ohne deine Genehmigung bereitzustellen. Du erhältst nicht nur mehr Kontrolle, sondern auch transparentere Einblicke in deine Benutzer.

Darüber hinaus solltest du unbedingt wissen, welche Aktivitäten die Mitarbeiter in deinen Atlassian-Produkten ausführen. Du oder jemand in deinem Team mag zwar ein Sicherheitsexperte sein, die Mehrheit der Mitarbeiter ist es aber nicht, weshalb du dich möglicherweise ungewollt zusätzlichen Risiken aussetzt.

- **Einblicke in Administration und Organisation**: Verfolge aktive Benutzer, die eine Seite angezeigt haben, betrachte aktive und inaktive Benutzer und überprüfe, für wie viele deiner verwalteten Benutzer die Zwei-Faktor-Authentifizierung gilt und wie viele nicht verwaltete Benutzer Zugriff auf deine Produkte haben.
- **CASB-Integration**: Stelle eine Verbindung zur CASB-Software McAfee MVISION Cloud her, um eine automatische Sicherheitsüberwachung und Verhaltensanalysen über dein McAfee MVISION Cloud-Dashboard zu erhalten.

Darüber hinaus haben wir die Lösung Beacon auf den Markt gebracht, die noch mehr Funktionen zur Erkennung von Bedrohungen bietet. Beacon, das sich derzeit noch in der Beta-Phase befindet, bietet Folgendes:

- **Erkennung**: Erhalte automatische Benachrichtigungen, wenn es zu ungewöhnlichen Aktivitäten in deinen Atlassian-Produkten kommt. Dies hilft dir, Bedrohungen zu erkennen.
- **Untersuchung**: Sammle detaillierte Informationen, anhand derer du die Plausibilität der Bedrohung ermitteln kannst.
- **Reaktion**: Nutze die Details aus Warnmeldungen, die Statusverfolgung und SIEM-Weiterleitung, um Bedrohungen unter Kontrolle zu bringen und Warnmeldungen nahtlos zu bearbeiten.

Wende dich an uns, um weitere Informationen zu erhalten.

Die wichtigsten Punkte

- Audit-Protokolle enthalten detaillierte Aufzeichnungen der Ereignisse in deiner Instanz. Wenn dein Unternehmen umfangreichere Aufzeichnungen erfasst, verfolgt Cloud Enterprise auch benutzergenerierte Aktivitäten. Diese Audit-Protokolle können verwendet werden, um die Sicherheit deiner Instanz zu gewährleisten und die Einhaltung von Vorschriften nachzuweisen.
- Verwende die automatische Produktfindung, um auf dem Laufenden zu bleiben, wenn jemand in deinem Unternehmen eine neue Instanz erstellt. Auf diese Weise erhältst du Sicherheitsstatus aufrecht.
- Bald kannst du mit Produktanfragen Benutzer daran hindern, eine neue Instanz zu erstellen.
- Beacon ist die intelligente Bedrohungserkennung für deine Atlassian-Produkte.

Produkt- und Organisations-Lebenszyklusmanagement

Die Atlassian Cloud-Produkte sind mit einer Atlassian-Organisation verbunden. Dadurch behältst du den Überblick über die Instanzen, die zu deiner Organisation gehören. Gerade wenn sich dein Unternehmen vergrößert, benötigst du Flexibilität, um deine Sicherheitsanforderungen zu erfüllen.

Was du tust: deine Daten auf der Grundlage der Datenanforderungen strukturieren

Während einer Unternehmensskalierung stehst du irgendwann vor einer Entscheidung. Du musst ermitteln, ob die Strukturierung deiner Atlassian-Produkte dir ausreichend Flexibilität gewährt, um deine Geschäfte auszubauen und ein geeignetes Maß an Kontrolle aufrechtzuerhalten. Unbegrenzte Instanzen geben Unternehmen genau diese Flexibilität.

Hier sind einige typische Beispiele dafür, wie Unternehmen wie deines Umgebungen mit mehreren Instanzen eingerichtet haben:

Separate Abteilungen und Governance	Gewähre Teams Autonomie, indem du für jeden deiner Geschäftsbereiche Sites erstellst. Auf diese Weise können Teams deine Sites anpassen und beispielsweise benutzerdefinierte Workflows und Apps nutzen, ohne andere Teams zu beeinträchtigen.
Wachstum durch Übernahmen und Zusammenarbeit mit externen Stakeholdern	Durch Fusionen oder Übernahmen können neue Teams zu deinem Unternehmen dazustoßen, und vielleicht möchtest du diese Teams lieber weiterhin getrennt verwalten. Du kannst diesen Teams eine eigene Site zuteilen und sie trotzdem an einem zentralen Ort verwalten.
Hochsensibles geistiges Eigentum	Einige deiner Teams haben Zugriff auf vertrauliche oder urheberrechtlich geschützte Daten. Du kannst für diese Teams separate Sites erstellen und den Zugriff einschränken, um das richtige Maß an Sicherheit zu gewährleisten.
Datenisolierung für geografisch verteilte Teams	Viele Unternehmen haben global verteilte Teams, sodass sie für bestimmte Regionen verschiedene Sites erstellen können. Vielleicht möchtest du ja eine separate Site erstellen, um deine EMEA-Teams mit strengen regulatorischen Anforderungen zu unterstützen. Erstelle separate Sites, um deine Datenschutzanforderungen zu erfüllen. Wenn du etwa über Daten verfügst, die in einer bestimmten Region verbleiben müssen, kannst du eine separate Site erstellen und die betroffenen Daten an diesem festgelegten Ort aufbewahren.

Lies unser E-Book, um mehr über unbegrenzte Instanzen zu erfahren.

Die wichtigsten Punkte

- Eine unbegrenzte Anzahl von Instanzen ermöglicht es Unternehmen, komplexe Anwendungsfälle zu erfüllen, wie zum Beispiel den Schutz hochsensibler Daten.
- Jede Instanz kann über die Atlassian-Administration vollständig an deine Spezifikationen angepasst werden, ohne dass sich dies auf andere Instanzen auswirkt, die deiner Organisation zugeordnet sind. Du kannst zum Beispiel deine

Instanzdaten auf der Grundlage deiner regulatorischen Verpflichtungen verschiedenen Regionen zuordnen.

Abschnitt 4: Atlassian Marketplace

Der Atlassian Marketplace bietet über 5.300 Apps und Integrationen, von denen mehr als die Hälfte die Atlassian Cloud-Produkte erweitern und anpassen. Atlassian bietet zwar selbst einige Marketplace-Apps an, aber die meisten Apps werden von Marketplace-Partnern als Drittanbieter entwickelt und betrieben.

Marketplace-Datensicherheit

Atlassian arbeitet daran, Marketplace-Partner bei der Entwicklung sicherer, zuverlässiger Cloud-Apps zu unterstützen, die deine Compliance-Anforderungen erfüllen. Dabei setzen wir unter anderem auf Sicherheitsanforderungen und -programme.

Was Atlassian tut: Sicherheitsanforderungen und Durchsetzung

Da Marketplace-Apps von Drittanbietern entwickelt und betrieben werden, konzentriert sich der Atlassian-Ansatz zur Marketplace-Sicherheit auf die Definition von Sicherheitsanforderungen und das Ergreifen von Durchsetzungsmaßnahmen, wie im nächsten Abschnitt näher erläutert wird. Konkret beinhaltet unser Ansatz Folgendes:

- klar definierte (und regelmäßig aktualisierte) Sicherheitsanforderungen für Cloud-Apps
- laufende Scans und Meldung fehlender Sicherheitsanforderungen von oder Schwachstellen
- geplante Maßnahmen zum Schutz der Kunden, falls erforderlich

Sicherheitsanforderungen von Atlassian an Cloud-Apps

Server- und Data Center-Apps erhalten zwar Richtlinien zur Verbesserung ihres Sicherheitsstatus, aber jeder Marketplace-Partner muss sich verpflichten, die von Atlassian definierten Sicherheitsanforderungen zu erfüllen, wenn er eine Cloud-App auf dem Marketplace anbietet. Diese Anforderungen fallen in die folgenden Kategorien:

Autorisierung und Authentifizierung	Apps müssen jede Anfrage an allen offengelegten Endpunkten authentifizieren und autorisieren.
Datenschutz	Jedes Mal, wenn eine App Endbenutzerdaten* außerhalb von Atlassian speichert, muss sie Maßnahmen ergreifen, um diese Daten zu schützen, einschließlich:

	• Sicherstellung der vollständigen Festplattenverschlüsselung im Ruhezustand; • Verwendung von TLS 1.2 (oder höher) zur Verschlüsselung des gesamten Datenverkehrs und Aktivierung von HSTS mit einem Mindestalter von einem Jahr; • sicherer Speicherung und Verwaltung von Geheimnissen (OAuth-Token, SharedSecret, API-Schlüssel usw.).
Anwendungssicherheit	Partner müssen Maßnahmen ergreifen, um Kundendaten vor Sicherheitsbedrohungen zu schützen. Sie müssen: • Domains, auf denen die App gehostet wird, verwalten und sicher konfigurieren; • alle nicht vertrauenswürdigen Daten validieren und bereinigen und alle Benutzereingaben als unsicher behandeln, um Injection-Schwachstellen zu minimieren; • bzw. dürfen keine Versionen von Drittanbieter-Bibliotheken und -Abhängigkeiten mit bekanntem als kritisch oder hoch eingestuften Sicherheitsrisiko verwenden.
Datenschutz	Apps dürfen keine Anmeldeinformationen von Atlassian-Benutzerkonten wie Benutzerpasswörter oder Benutzer-API-Tokens sammeln oder speichern.
Schwachstellenmanagement	Partner müssen Sicherheitskontaktinformationen angeben und am Schwachstellen-Management-Programm von Atlassian teilnehmen. Wenn Atlassian oder ein Sicherheitsforscher ein Sicherheitsproblem mit einer App feststellt, muss das Sicherheitsteam von Atlassian in der Lage sein, den Partner zu erreichen.
* Endbenutzerdaten = alle Daten, Inhalte oder Informationen eines Endbenutzers, auf die du oder deine App in Verbindung mit dem Atlassian Marketplace zugreifen kann, bzw. Daten, die gesammelt oder anderweitig verarbeitet werden können	

Diese Anforderungen sind für alle Cloud-Apps gemäß der Marketplace-Partnervereinbarung von Atlassian verbindlich.

Scans, Tests und Betreuung

Die Arbeit endet nicht, wenn Apps entwickelt und im Marketplace aufgelistet werden. Um die kontinuierliche Sicherheit aller Cloud-Apps zu fördern, hat Atlassian verschiedene Strategien zur Identifizierung und Verwaltung von sicherheitsrelevanten Vorgängen bzw. Schwachstellen eingeführt.

Ecoscanner

Die Ecoscanner-Plattform führt täglich Scans durch, um alle Marketplace-Cloud-Apps auf wichtige Sicherheitsanforderungen und Schwachstellen hin zu überprüfen.

Als Teil der Ecoscanner-Plattform stellt Atlassian 8 Scanner für wichtige Anforderungen zur Verfügung. Davon sind 6 als Open-Source-Tools verfügbar, mit denen Partner ihre eigenen Apps scannen können. Dadurch können Partner sicherstellen, dass neue Versionen diese wichtigen Anforderungen erfüllen, bevor Atlassian mit deren Überprüfung beginnt.

Du kannst die Entwicklerdokumentation für den Ecoscanner hier lesen, um mehr über die spezifischen besprochenen Anforderungen zu erfahren.

Software-Schwachstellenscanner von Drittanbietern

Wir nutzen auch Scanner, um Schwachstellen zu identifizieren, die von Software von Drittanbietern herrühren. Open Source ist ein mächtiges Werkzeug, und fast alle Entwickler auf der Welt verlassen sich für ihre Anwendungen auf Open-Source-Bibliotheken. Aber diese Bibliotheken weisen gelegentlich Schwachstellen auf, die sich auf ein breites Segment von Technologieunternehmen auswirken und Apps betreffen.

Wir untersuchen kontinuierlich Apps, die auf der Forge-Plattform von Atlassian erstellt wurden, auf kritische oder schwerwiegende Schwachstellen in Bibliotheken von Drittanbietern.

Im Falle einer Zero-Day-Schwachstelle, die erhebliche Auswirkungen haben kann (zum Beispiel die jüngsten Schwachstellen in log4j oder OpenSSL), prüft Atlassian, ob diese Schwachstelle in allen Marketplace-Cloud-Apps erkannt werden kann – auch in denen, die nicht auf unserer

Forge-Plattform basieren. Wenn möglich verwenden wir Scanner, um die Schwachstelle in Marketplace-Apps zu entdecken, und arbeiten mit Partnern zusammen, um sicherzustellen, dass die Schwachstelle rechtzeitig gepatcht wird. Wenn Schwachstellen nicht rechtzeitig gepatcht werden, ergreifen wir Maßnahmen zum Schutz der Kunden.

> ***Beispiel: Apache Log4j***
>
> Hier ein aktuelles Beispiel: Im Dezember 2021 wurden die Programme, Scan-Funktionen und Berichterstellungsmechanismen von Atlassian auf die Probe gestellt, als bei der Remote-Code-Ausführung in Apache Log4j-Schwachstellen offengelegt wurden. Atlassian reagierte schnell und beseitigte die Schwachstelle für alle Atlassian Cloud-Produkte.
>
> Darüber hinaus konnte das App-Sicherheitsteam von Atlassian unser gesamtes Ökosystem scannen und identifizieren, welche Apps anfällig waren, diese Schwachstellen melden und sie in Zusammenarbeit mit App-Entwicklern so schnell wie möglich beheben. Innerhalb von etwa einer Woche konnten wir bestätigen, dass alle Cloud-Apps nicht mehr von der Log4j-Schwachstelle betroffen waren und dass alle Data Center- und Server-Apps entweder gepatcht oder aus unserem Marketplace entfernt wurden.

Berichte zu externen Sicherheits-Bugs

Zusätzlich zu unseren Sicherheitsanforderungen und Strategien zur Erkennung von Schwachstellen können Marketplace-Partner, Kunden oder andere Personen außerhalb von Atlassian auch Sicherheitsprobleme im Zusammenhang mit Apps von Drittanbietern über das Jira-Projekt Atlassian Marketplace Security (AMS) melden.

Schwachstellen, die aus beliebigen Quellen wie Bug Bounty, Scannern, Sicherheitsüberprüfungen und externen Berichten stammen, werden an AMS weitergeleitet und dann vom Atlassian-Sicherheitsteam zur Behebung verfolgt.

*** Wahlprogramm: Marketplace Bug Bounty**

Partner können am Bug-Bounty-Programm für Atlassian Marketplace teilnehmen, wodurch sie Zugang zu einer vertrauenswürdigen Community aus Cybersicherheitsforschern erhalten, die ihre Apps ständig testen und alle gefundenen Schwachstellen melden.

> Tipp: Du kannst Apps, die am Bug-Bounty-Programm teilnehmen, anhand der folgenden Marketplace-Badges erkennen:
>
> - dem "Cloud Security Participant"-Abzeichen, das auf die Teilnahme am Bug-Bounty-Programm hinweist

- dem "Cloud Fortified"-Badge, das bedeutet, dass eine App am Bug-Bounty-Programm teilnimmt und auch andere Maßnahmen ergriffen wurden, um die Sicherheit und Zuverlässigkeit zu verbessern; Cloud Fortified-Apps bieten Kunden außerdem an 5 Tagen die Woche rund um die Uhr Support.

  "Durch die Priorisierung von Sicherheit und die aktive Teilnahme an Initiativen wie den Bug-Bounty- und Cloud Fortified-Programmen von Atlassian schützen wir nicht nur die wertvollen Daten unserer Benutzer, sondern bauen auch Vertrauen und Glaubwürdigkeit bei unseren Kunden auf. Unser Engagement für Sicherheit ist unerschütterlich und wir werden weiterhin intensiv daran arbeiten, unseren Benutzern die sichersten und zuverlässigsten Apps zu bieten." – John Whittaker, Vice President bei SmartBear, einem Atlassian Platinum Marketplace-Partner

Lösung sicherheitsrelevanter Probleme

Die bisher besprochenen Strategien sollen Atlassian dabei helfen, potenzielle Sicherheitsrisiken auf Marketplace zu identifizieren und zu verfolgen. Aber natürlich ist die Erkennung von Schwachstellen nur der erste Teil der Strategie, Kunden mit Apps zu schützen.

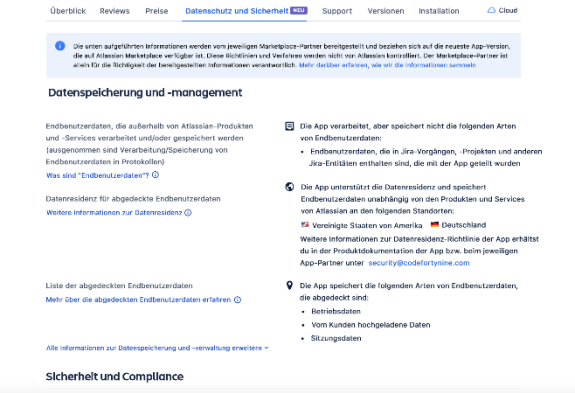
Wenn eine Schwachstelle in Marketplace-Apps erkannt wird, unterliegen alle Apps der Richtlinie zur Behebung von Sicherheits-Bugs für Marketplace-Apps, in der die Fälligkeitsdaten für sicherheitsrelevante Fehler festgelegt sind. Wenn wir feststellen, dass eine App eine Sicherheitsanforderung nicht erfüllt, benachrichtigen wir die Marketplace-Partner und setzen ihnen eine Deadline, um das Problem zu beheben. Wenn Apps diese Fristen nicht einhalten, ergreift Atlassian Maßnahmen.

Bei kritischen Vorgängen oder Vorgängen, die zu lange nicht behandelt werden, ergreift Atlassian Maßnahmen wie das Entfernen von Security-Badges und das Ausblenden der App in Marketplace. Apps, die gegen unsere Richtlinien zur Behebung von Sicherheits-Bugs für Marketplace-Apps verstoßen, werden auf unserer Seite zur Transparenz der App-Sicherheit öffentlich aufgeführt. In schweren Fällen kann Atlassian sogar eine App aussetzen, um Kundendaten zu schützen.

Unsere Botschaft an Marketplace-Partner ist also klar: Die Aufrechterhaltung der Sicherheit deiner App ist von entscheidender Bedeutung. Wenn eine App unsere Sicherheitsanforderungen nicht erfüllt, werden wir dies herausfinden und Maßnahmen ergreifen.

Was du tust: aufmerksam sein und Ereignisse melden

Atlassian verfügt zwar über Prozesse zur Unterstützung von Partnern, aber auch du musst selbst aktiv werden. Mache dich vor der Installation mit den Datenschutz- und Sicherheitsdetails einer App vertraut, die du auf der Registerkarte "Datenschutz und Sicherheit" der App in Atlassian Marketplace findest.



Beachte außerdem, dass Apps, die gegen die Richtlinien zur Behebung von Sicherheits-Bugs für Marketplace-Apps von Atlassian verstoßen, auf der Seite zur Transparenz der App-Sicherheit aufgeführt werden. Wenn du eine deiner Apps auf dieser Seite siehst, wende dich direkt an den Marketplace-Partner, um zu erfahren, um welche Art von Verstoß es sich handelt.

Denke außerdem daran, dass du die Systeme von Atlassian dazu nutzen kannst, um Schwachstellen zu melden. Wenn dir in einer App ein Fehler auffällt, kannst du den Vorgangstyp Sicherheitsschwachstelle in AMS öffnen, um Atlassian zu benachrichtigen.

Die wichtigsten Punkte

- Marketplace-Partner stimmen Sicherheitsanforderungen zu, wenn sie eine App in Atlassian Marketplace anbieten. Du solltest dich mit den Datenschutzrichtlinien einer App vertraut machen, bevor du die App installierst.
- Atlassian führt täglich benutzerdefinierte Sicherheitsscans durch, um sicherzustellen, dass alle Cloud-Apps die Sicherheitsanforderungen erfüllen. Wenn Apps die Anforderungen nicht rechtzeitig erfüllen, werden Durchsetzungsmaßnahmen gemäß der Richtlinie zur Behebung von Sicherheits-Bugs in Marketplace-Apps ergriffen.
- Zusätzlich zu diesen Programmen können sich Partner für umfassendere Sicherheitsprogramme entscheiden, wie das Marketplace-Bug-Bounty-Programm für Sicherheit oder das Cloud Fortified-Programm für Sicherheit, Zuverlässigkeit und Support.
- Kunden können App-Sicherheitsschwachstellen an Atlassian melden und sollten sich auch die Seite zur Transparenz der App-Sicherheit ansehen, wo Atlassian Apps aufführt, die der Richtlinie zur Behebung von Sicherheits-Bugs nicht entsprechen.

Marketplace-Datenschutz

Was Atlassian und Partner tun: Datenschutzverpflichtungen erstellen und diesen zustimmen

Apps müssen nicht nur die Sicherheitsanforderungen erfüllen, sondern auch eine Datenschutzrichtlinie bereitstellen, die Endbenutzer über Folgendes informiert:

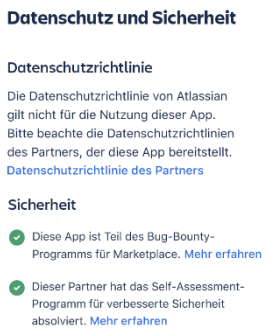
- wie ein Partner auf Endbenutzerdaten zugreift, sie sammelt und verarbeitet
- mit wem eine App oder ein Partner Endbenutzerdaten teilt
- in welchem Land oder welchen Ländern die Endbenutzerdaten gespeichert werden

Zusätzlich zu einer Datenschutzrichtlinie verlangt Atlassian von Partnern, dass sie alle erforderlichen Rechte, Genehmigungen und Einwilligungen von Endbenutzern für:

- den Zugriff
- die Erfassung
- das Speichern
- die Übertragung
- die Behandlung
- die Verwendung
- die Bekanntmachung
- die Weitergabe und
- andere Verarbeitung

aller Endbenutzerdaten haben.

Was du tust: die Datenschutzinformationen der App prüfen



In der Datenschutzrichtlinie erfährst du mehr darüber, wie die App mit Daten umgeht.

Die Datenschutzrichtlinie einer App findest du in der App-Auflistung auf marketplace.atlassian.com. Wenn du nach unten zum Abschnitt "Weitere Details" scrollst, siehst du auf der rechten Seite "Datenschutz und Sicherheit". Die Datenschutzrichtlinie der App sollte dort unter "Datenschutzrichtlinie" verlinkt sein. Du findest diese Information auch auf der Registerkarte "Datenschutz und Sicherheit" der App oben in der App-Liste, gleich neben "Support".

Auf Basis dieser Informationen entscheidest du vielleicht, dass für eine App eine Datenschutzvereinbarung erforderlich ist, die du direkt mit dem Partner abschließen musst. Wir stellen auf der Registerkarte "Datenschutz und Sicherheit" im Abschnitt "Datenschutz" einen Bereich zur Verfügung, in dem Partner ihre Standard-Datenschutzvereinbarung bereitstellen

können. Wenn diese Vereinbarung aber deinen Anforderungen nicht entspricht (oder wenn der Partner keine bereitgestellt hat), musst du dich möglicherweise direkt an den Partner wenden.

Die wichtigsten Punkte

- Marketplace-Partner erklären sich damit einverstanden, Datenschutzinformationen öffentlich zu teilen, wenn sie eine App auf dem Atlassian Marketplace anbieten.
- Du solltest dich mit den Datenschutzrichtlinien einer App vertraut machen, bevor du die App installierst.

Apps und Datenmanagement

Marketplace-Partner sind letztendlich für die Leitung ihres eigenen Geschäfts verantwortlich und werden strategische Investitionen tätigen, die auf der Nachfrage von Kunden basieren. Abgesehen von den Atlassian-Anforderungen, die in unserer Entwicklerdokumentation, den Entwicklerbedingungen und der Marketplace-Partnervereinbarung formuliert sind, treffen Partner ihre eigenen Geschäftsentscheidungen darüber, wie Apps erstellt werden und welche Funktionen sie unterstützen.

Atlassian arbeitet ständig daran, neue Tools und Anleitungen bereitzustellen, damit Marketplace-Partner die sichersten und hochwertigsten Apps priorisieren und entwickeln können.

Was Partner tun: auf die Erstellung sicherer Apps achten

Mithilfe von Dokumentation, Ressourcen, Live-Schulungen und Tools ermutigt Atlassian seine Partner, bei der Entwicklung ihrer Apps das Prinzip "Sicherheit durch Design" anzuwenden:

Geringstprivilegierter Zugriff

Die Daten, auf die eine App zugreifen muss, variieren je nach ihrer Funktion, aber im Allgemeinen empfehlen wir Partnern, den Zugriff auf die Informationen zu beschränken, die für den Betrieb erforderlich sind. Im Abschnitt "Integrationsdetails" der App-Liste oder in den

Informationen auf der Registerkarte "Datenschutz und Sicherheit" der App findest du heraus, welche Daten eine App benötigt.

Dieses Prinzip teilen wir nicht nur mit Partnern, sondern arbeiten auch daran, Administratoren mehr Kontrolle über die Bereiche oder Projekte zu geben, auf die eine App Zugriff hat, sodass du den App-Zugriff auf Daten selbst einschränken kannst. (Du kannst diese Arbeit im Abschnitt "Apps und Erweiterbarkeit" in der Cloud-Roadmap von Atlassian verfolgen).

Geringstmöglicher Datenausgang und die Nutzung der Atlassian-Infrastruktur

Apps mit komplexeren Anwendungsfällen müssen möglicherweise einige Daten extern speichern oder verarbeiten.

Apps mit einfacheren Anwendungsfällen können jedoch oft die Menge der gespeicherten Daten einschränken, für deren Sicherung sie verantwortlich sind, und Atlassian mehr Verantwortung übertragen, um die Sicherheits- und Compliance-Anforderungen der Kunden zu erfüllen.

Um die Menge an Kundendaten zu begrenzen, die die Atlassian-Umgebung verlassen, können Partner die von Atlassian entwickelten Speicheroptionen für ihre Apps verwenden:

- **Ausschließliches Speichern von Endbenutzerdaten in Jira oder Confluence**: Apps, die keinen großen Speicherbedarf haben, können manchmal Endbenutzerdaten in Jira oder Confluence speichern, was den Aufwand für die unabhängige Absicherung der Daten reduziert.
- **Nutzung von Speicher und Rechenleistung von Atlassian auf Forge**: Partner können wahlweise auch Apps auf Forge entwickeln, wo sie die Möglichkeit haben, Daten ausschließlich in der Atlassian-Umgebung zu speichern und zu verarbeiten.

Du kannst mehr darüber erfahren, wo eine App Endbenutzerdaten speichert und welche Endbenutzerdaten sie speichert, indem du die App-Liste in Atlassian Marketplace aufrufst. Dort findest du die Datenschutzrichtlinie, Dokumentation und andere von Partnern bereitgestellte Informationen zu einer App.

Was Atlassian und Partner tun: App-Daten wiederherstellen

Atlassian hostet zwar ein Backup aller Daten, die in Jira, Confluence oder auf Forge gespeichert sind, aber Marketplace-Partner sind für ihre eigenen Datensicherungs- und Wiederherstellungsverfahren für alle Daten verantwortlich, die außerhalb der Infrastruktur von Atlassian gespeichert sind.

Wir empfehlen allen Marketplace-Partnern, einen Plan aufzustellen. Wende dich direkt an einen Partner, wenn du Fragen zu einer bestimmten App hast.

Die wichtigsten Punkte

- Zusätzlich zu den Sicherheitsanforderungen und Datenschutzverpflichtungen arbeitet Atlassian ständig daran, Tools und Anleitungen bereitzustellen, damit Partner Best Practices für den Schutz von Kundendaten implementieren können.
- Sieh dir unbedingt die Registerkarte "Datenschutz und Sicherheit" und die Datenschutzrichtlinie einer App an, um mehr darüber zu erfahren, wie die App mit Daten umgeht.

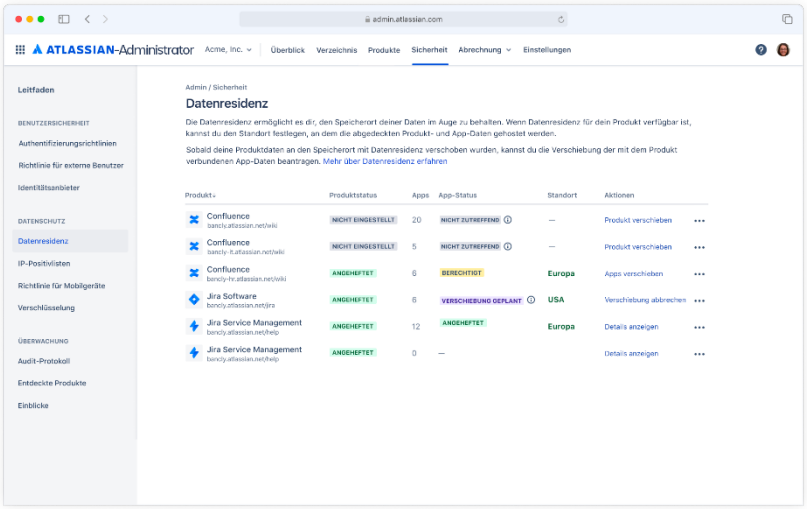
Compliance und Marketplace-Apps

Wenn dein Unternehmen gesetzliche Verpflichtungen oder interne Compliance-Anforderungen in Bezug auf den Datenschutz erfüllen muss, sollten deine installierten Apps diese Verpflichtungen unbedingt ebenfalls erfüllen. Zu diesem Zweck stellen wir unseren Partnern Informationen und Tools zur Verfügung, um ihre Investitionen in Bereichen zu unterstützen, von denen wir wissen, dass sie wichtig sind.

Was Atlassian und Partner tun: Datenresidenz

Das Prinzip "Sicherheit durch Design" soll zum einen deshalb weitergegeben werden, um die Anzahl der Apps zu minimieren, die unabhängig voneinander die Datenresidenz unterstützen müssen. Manche Apps speichern Daten ausschließlich innerhalb der Atlassian-Produkte und -Services. Da diese Apps keine extern gespeicherten Daten haben, werden deine abgedeckten App-Daten mit allen regionalen Verschiebungen des Produkts verknüpft, auf dem sie installiert sind, und folgen diesen.

Apps, die Daten extern speichern müssen, sind jedoch für die unabhängige Unterstützung der Datenresidenz verantwortlich. Marketplace-Partner mit Apps, die Daten außerhalb von Atlassian speichern, können in den meisten Fällen in die Zuordnung von Daten zu ausgewählten Regionen investieren, sodass Kunden die Datenschutzanforderungen hinsichtlich der Datenlokalisierung oder des Datentransports erfüllen können.
Wir stellen zwar unsere eigene Definition von abgedeckten Daten als Beispiel bereit, aber letztendlich entscheiden die Partner, welche Daten für die außerhalb der Atlassian-Umgebung verwaltete Datenresidenz abgedeckt sind. Sieh daher am besten in der Dokumentation zur App auf der Registerkarte "Datenschutz und Sicherheit" in der App-Liste nach oder wende dich direkt an den Partner, um mehr zu erfahren. Organisations- und Site-Admins für Jira und Confluence werden in Kürze auch in der Atlassian-Administration (admin.atlassian.com) mithilfe einer neuen Beta-Funktion die Datenresidenz für installierte Apps einsehen und verwalten können.



Auf admin.atlassian.com kannst du einsehen, welche Apps zur Datenresidenz berechtigt sind, und Verschiebungen von App-Daten planen.

Was Partner tun: gesetzliche Vorschriften einhalten

Gemäß ihrer Vereinbarung mit Atlassian sind Partner verpflichtet, die gesetzliche Vorgaben in den Regionen zu erfüllen, in denen sie tätig sind. Darüber hinaus veröffentlicht unser Datenschutzteam grundsätzliche Ressourcen, um Partnern zu helfen, ihre rechtlichen Verpflichtungen (etwa die Einhaltung der DSGVO) in bestimmten Regionen besser zu verstehen.

Was Partner tun: Compliance-Standards und Zertifizierungen bieten

Die meisten Marketplace-Partner wissen, welche Vorteile die Einhaltung von Datenschutzstandards mit sich bringt, und viele Partner haben in Zertifizierungen investiert oder investieren gerade in diese.

> *Unserer Meinung nach ist der Schutz von Kundendaten einfach eine gute Geschäftspraxis. Wir sagen, dass Sicherheit unsere Entscheidungen bestimmt, und die Zertifizierung unserer Einhaltung von branchenführenden Standards ermöglicht uns zu beweisen, dass wir das Gesagte auch so meinen. – Julia Wester, Mitbegründerin von 55 Degrees, einem Platinum Marketplace-Partner*

Um Partnern bei der Priorisierung zu helfen, bietet Atlassian Vorschläge und Unterstützung mit einer konformen Infrastruktur, sofern dies möglich ist.

Partner, die sich für die Verwendung eines von Atlassian gehosteten Speichers über die Forge-Plattform von Atlassian entscheiden, profitieren von den Investitionen von Atlassian in Compliance-Standards. Compliance-Standards erfordern zusätzliche Arbeit, die über die Infrastruktur hinausgeht, aber die Forge-Plattform von Atlassian ist bereits SOC 2-konform. Das bedeutet, dass Partner einen Vorsprung bei der SOC 2-Zertifizierung haben, wenn sie auf Forge aufbauen.

Was du tust: Partner wissen lassen, wonach du suchst

Partner werden strategische Investitionen basierend auf der Nachfrage tätigen, die sie von Kunden wie dir erhalten. Wenn du an einer App interessiert bist, die Daten extern speichert, oder du eine solche bereits verwendest und gerne hättest, dass diese App Datenresidenz unterstützt, informiere den Besitzer der App darüber. Die Kontaktinformationen findest du für die meisten Marketplace-Apps in der Marketplace-Liste.

Die wichtigsten Punkte

- Atlassian definiert nicht nur Sicherheitsanforderungen und Datenschutzverpflichtungen, sondern arbeitet auch ständig daran, Tools und Anleitungen bereitzustellen, damit Partner deine Compliance-Anforderungen erfüllen können.
- Wenn du mehr über eine App erfahren möchtest, lies dir unbedingt auf der Registerkarte "Datenschutz und Sicherheit" die Datenschutzrichtlinie der App durch. Lasse Partner auch wissen, wenn eine App eine bestimmte Anforderung erfüllen soll.

Kontrolle und Transparenz

Atlassian arbeitet daran, dir den Zugriff auf Informationen zu erleichtern, damit du fundierte Entscheidungen über die Apps treffen kannst, die du in deiner Cloud-Umgebung installierst. Zudem geben wir dir mehr Kontrolle, damit du die installierten Apps selbst verwalten kannst.

Was du tust: sicherstellen, dass Apps deinen Anforderungen entsprechen, bevor du sie installierst

Prüfe die Datenschutz- und Sicherheitsdetails der App

Wenn du sicherstellen musst, dass Apps deine Sicherheitsanforderungen erfüllen, benötigst du Informationen darüber, wie Apps mit Daten umgehen. Viele Partner sind sich dessen bewusst und verpflichten sich, Informationen bereitzustellen, die dir dabei helfen, deine Apps anhand deiner Sicherheitsanforderungen zu bewerten.

> *Wir bei Appfire legen großen Wert auf Vertrauen, und Vertrauen basiert auf Transparenz und Beständigkeit. Mithilfe unseres Trust Center können unsere Kunden unsere Apps deutlich schneller bewerten, da die Sicherheitsüberprüfung einer App auf alle Appfire-Apps angewendet werden kann. Wir möchten Kunden Komfort bieten und Vertrauen aufbauen, damit sie souveräne Kaufentscheidungen treffen können.* – Doug Kersten, Chief Information Security Officer bei Appfire

Viele Partner sind zwar der Transparenz verpflichtet, können aber unterschiedliche Herangehensweisen an die Bereitstellung von Informationen haben und diese an verschiedenen Stellen online anbieten. Das kann die Suche nach den benötigten Informationen erschweren.

Beginne deine Sicherheitsevaluierung, indem du die App im Atlassian Marketplace aufrufst. Dort findest du auf der Registerkarte "Datenschutz und Sicherheit" wichtige, von Partnern bereitgestellte Informationen, die Datenschutzrichtlinie der App und weitere Dokumentation. Damit du Informationen schneller finden kannst, arbeiten wir weiter daran, einen einheitlicheren Bereich zu schaffen, in dem du dich über die Datenschutz- und Sicherheitsdetails einer App informieren kannst.

Prüfe die Berechtigungen der App

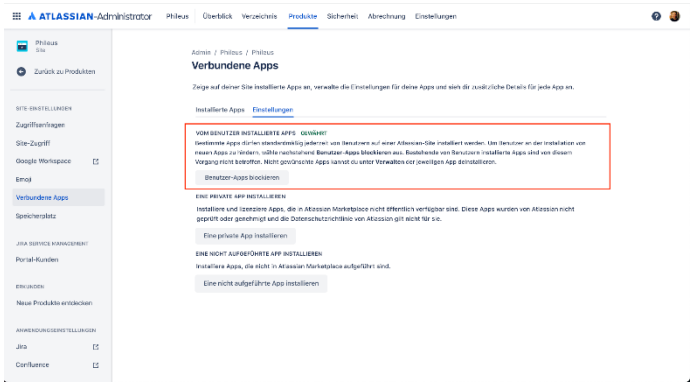
Wenn die Berechtigungen für eine Marketplace-App einmal installiert und erteilt wurden, können wir nicht verhindern, dass die App Aktionen gemäß den gewährten Berechtigungen ausführt, auch wenn du damit nicht einverstanden bist. Wir empfehlen, vor der Installation die Eignung der App und die Annehmbarkeit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

Was du tust: die Apps auf deiner Instanz verwalten

Schränke die Installationsberechtigungen ein

Die Installation von Cloud-Apps ist im Großen und Ganzen den Administratoren vorbehalten. Endbenutzer müssen eine Anfrage an ihren Admin senden, wenn sie eine App installieren

möchten. Standardmäßig können Endbenutzer jedoch OAuth 2.0 (3LO)-Apps installieren und ausführen.

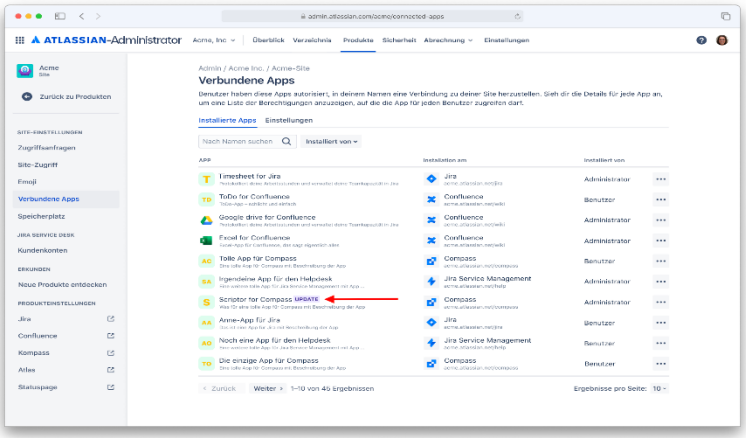


Um mehr Kontrolle über App-Installationen zu erhalten, können Site-Admins die Installationsfunktion für OAuth 2.0 (3LO)-Apps über einen Umschalter in admin.atlassian.com aus- oder einschalten.

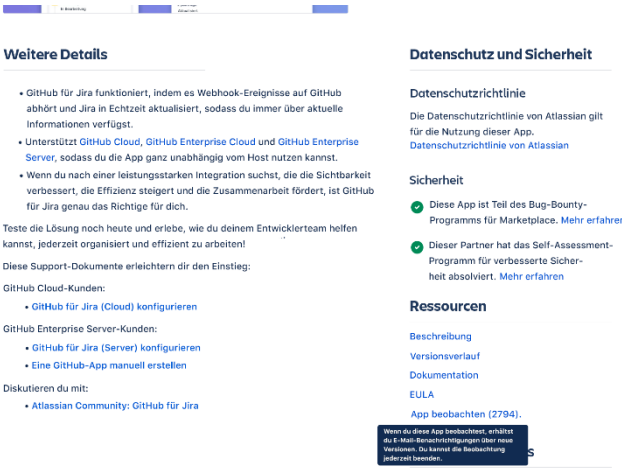
Für viele Workflows ist es natürlich von Vorteil, wenn Endbenutzer für ihre Arbeit nützliche Apps selbst installieren dürfen. Wenn du diese Funktion aktiviert lässt und trotzdem die von Endbenutzern installierten Apps im Auge behalten möchtest, kannst du in der Spalte "installiert von" nach "Benutzern" suchen und alle Apps entfernen, die ein Risiko darstellen.

Informiere dich laufend über Änderungen und halte die Apps aktuell

Da Apps ständig die Sicherheitsanforderungen prüfen und sich weiterentwickeln, um die Sicherheit zu erhöhen, lohnt es sich, darüber auf dem Laufenden zu bleiben. Du kannst dich für E-Mail-Benachrichtigungen im Marketplace-Eintrag einer App auf marketplace.atlassian.com registrieren oder in deiner Liste mit installierten Apps auf admin.atlassian.com nachsehen, für welche Apps ein Update verfügbar ist.



Apps mit verfügbaren Updates findest du auf admin.atlassian.com



Registriere dich für "App beobachten" auf marketplace.atlassian.com, um E-Mail-Benachrichtigungen zu erhalten, wenn neue Versionen verfügbar sind.

Die wichtigsten Punkte
Wenn du deine Daten bei der Nutzung von Cloud-Apps schützen möchtest, sollten du daran denken, dass Atlassian, Partner und Kunden alle eine Rolle dabei zu spielen haben. Atlassian wird weiter daran arbeiten:

- **das Sicherheits- und Datenschutzniveau auf unserem Cloud-Marketplace** durch Anforderungen, Schulungen und Tools für Partner zu erhöhen und
- **dir mehr Transparenz und Kontrolle und Kontrolle zu bieten,** damit du beim Kauf und der Verwaltung von Apps fundierte Entscheidungen treffen kannst.

Fazit

Der durchgängige Schutz deiner Daten muss von dir, Atlassian und deinen Marketplace-Partnern gemeinsam sichergestellt werden, denn jeder von uns trägt einen Teil der Verantwortung. Folgendes ist in unseren Augen dafür nötig:

- Wir hosten unsere Plattform auf einer zuverlässigen und sicheren Infrastruktur, die bei einem Ausfall schnell wiederhergestellt werden kann.
- Datenschutzkontrollen werden direkt in die Plattform integriert, wodurch Unternehmen gleich erweiterte Funktionen zur Verfügung gestellt werden, mit denen sie ihre Geschäftsanforderungen erfüllen können.
- Wir bieten Admins eine zentrale Verwaltungsansicht, die ihnen einen besseren Einblick in ihre Atlassian-Produkte gewährt und so vor möglichen Sicherheitsvorfällen schützt.
- Wir stellen Marketplace-Partnern und unserem Ökosystem geeignete Tools zur Verfügung, damit sie selbst robuste Datensicherheitsmechanismen in ihre Anwendungen integrieren können.

Wende dich an uns, um mehr über unseren Datenschutzansatz zu erfahren. Oder informiere dich beim Atlassian Migration Program, wenn du eine Migration zu Cloud in Erwägung ziehst und Atlassian Cloud bewerten möchtest.