

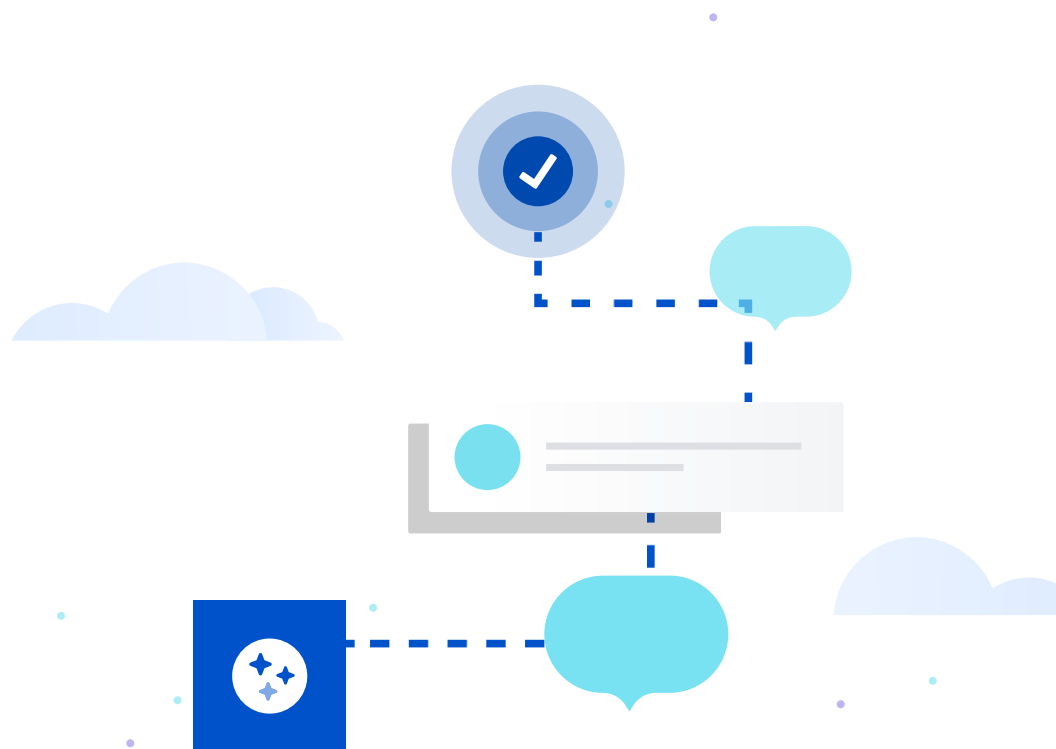


Your guide to Atlassian Cloud Enterprise

 **ATLASSIAN**

Table of contents

1	Executive summary
2	Section I: Scale your organization
3	Scale your business with Cloud Enterprise
4	Examples of how organizations set up multi-instance environments
5	Section II: Protect your data
6	Advanced compliance and privacy controls
8	Security controls
9	Identity and access management controls
11	Prevents attacks with threat detection
12	Section III: Intuitive insights and analytics
13	Critical insights to drive data-driven decisions



Executive summary

Enterprises face new challenges every day - from shifts in regulatory requirements to how to safely enable teams to work anywhere - and it only gets harder as you scale. It's your job as an admin to implement technologies that will allow your organization to adapt to these changes while still having the necessary controls to meet your business obligations. That's why modern enterprises are already using SaaS solutions.

You've already taken the first step to accelerate your business by leveraging Atlassian Cloud products - running on a connected platform.

This multi-layer platform is:

- Built on an enterprise-grade infrastructure that's performant and reliable at scale
- Fortified with robust data protection controls
- Enhanced with robust data protection controls that allow you to protect and manage your data

But as an enterprise, you need more to maintain a competitive advantage. Your products must be highly customizable to adapt to your evolving business requirements while enabling you with the controls you need to protect one of your most important assets - your data. Atlassian Cloud Enterprise is designed to provide enterprise-grade controls that you can customize to fit your needs.

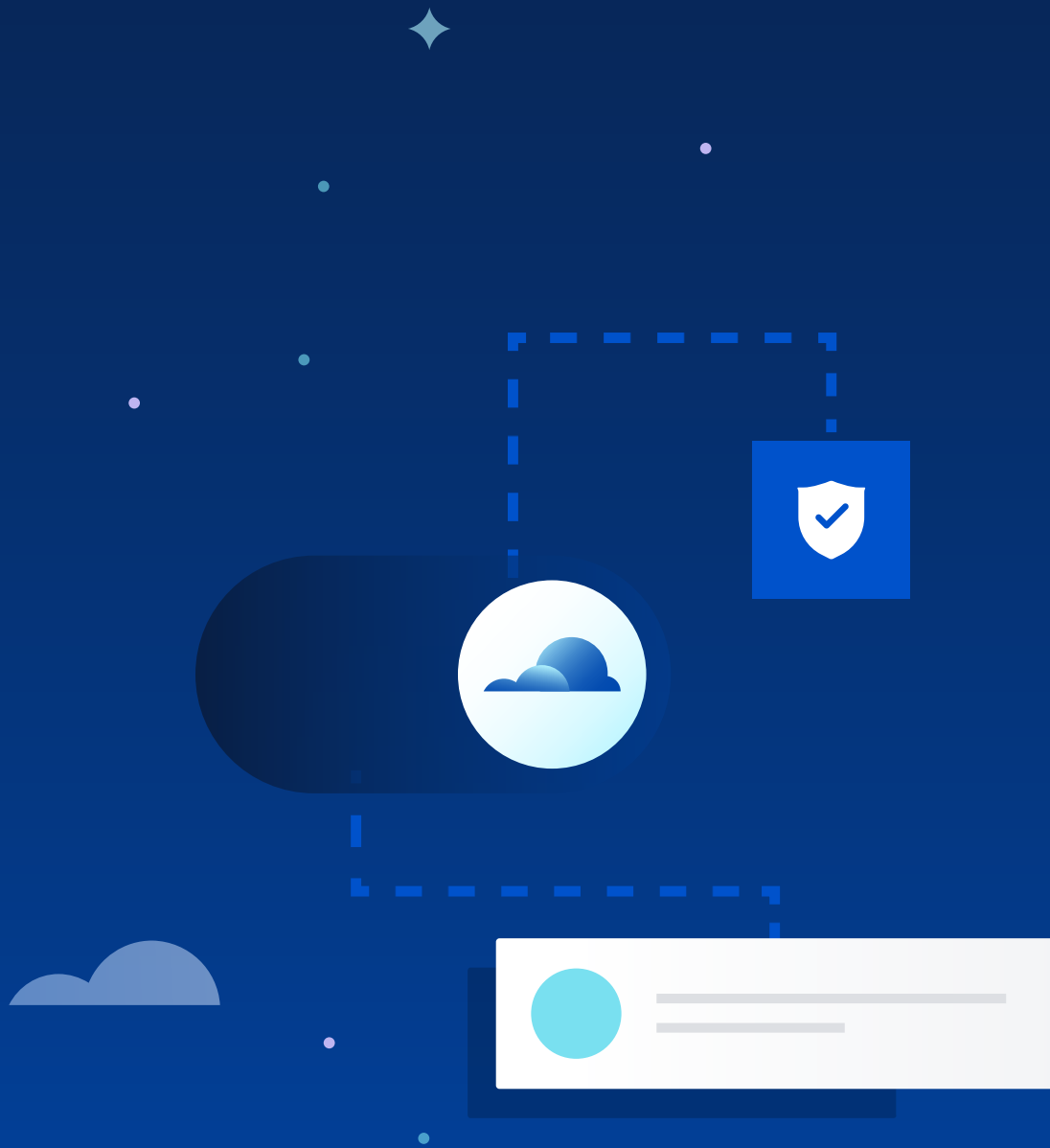
In this guide, learn more about how Atlassian Cloud Enterprise will enable you to:

- Scale your Atlassian products to address and meet your unique business requirements.
- Protect your users, data, and detect threats before they happen.
- Unlock your data to get critical insight into your organization.



01

Scale your organization



Scale your business with Cloud Enterprise

Scale can sometimes be a loaded term. Some people will say it's all about the size of your user base, while others may say it's about being able to scale your requirements, such as compliance and security controls. Truthfully, it's both.

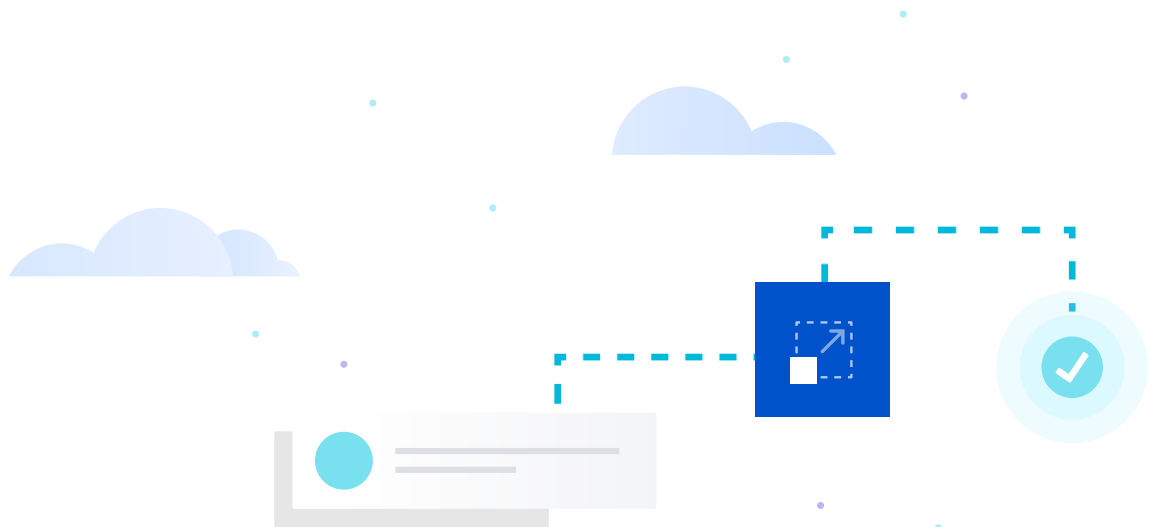
While several dimensions play a role in how your organization approaches scale, you need to be able to 1) support all of your teams and 2) build an environment that will allow your teams to scale their work.

Unlike Cloud Standard or Premium plans, you get access to unlimited instances of Jira Software, Confluence, and Jira Service Management with Cloud Enterprise. So, instead of consolidating or creating instances for administrative ease, you can set up instances more meaningfully.

Performance and reliability go hand and hand with scale. As an enterprise, you need products that are operational and going to be performant so your teams do their job seamlessly. No one likes waiting for a page to load. Cloud Enterprise offers a **financially backed uptime guarantee of 99.95%** across key experiences to give you ease of mind.

“ We rely on Jira and Confluence for mission-critical collaboration workflows, such as coordinating complex supply chains for distributing Covid-19 vaccines. Atlassian Cloud Enterprise enables us to standardize on one cloud platform while enabling our various subsidiaries and business units to customize instances based on specific workflows, apps, and more.

LEADING HEALTHCARE COMPANY



Here are some common examples of how organizations like you have set up multi-instance environments:



Separate departments and governance

Grant teams autonomy by creating sites for each of your business units (BUs). This allows teams to customize their sites. For example, teams can apply customized workflows and apps without impacting other teams.



Growth through acquisition, collaboration with external stakeholders

New teams may join your organization through mergers or acquisitions, and you may want to continue administering those teams separately. You can give those teams their own site and still administer them in a central location.



Highly sensitive intellectual property

Some of your teams have access to sensitive or proprietary data. You can create separate sites for those teams and limit access to maintain the right level of security.



Data Isolation for geo-dispersed teams

Many organizations have globally distributed teams, so you can create different sites for specific geos. For example, maybe you want to create a separate site to support your EMEA teams with strict regulatory requirements.

Each instance can have up to 35,000 users for Jira Software, 50,000 users for Confluence, and 10,000 agents for Jira Service Management. And we're only getting larger. We're running an early access program for 20,000 agents on Jira Service Management and 50,000 users for Jira Software.

[Read our ebook to learn more about multiple instances.](#)



02

Protect your data



Protect your data with enterprise security and governance controls

Protecting your data only gets more difficult with more people, tools, and devices accessing your products. On top of this, **hackers are finding new ways to breach products every day**, so it's critical that you implement a structure that's going to protect your organization.

To truly safeguard your data, you must have features that address these three areas of security:

- Advanced compliance and privacy controls
- Security controls
- Identity and access management

Advanced compliance and privacy controls

Your organization may have industry or regulatory requirements that you must prove you're complaint against. Often, these requirements come in the form of compliance certifications - providing a blueprint for what controls we at Atlassian need to build into the infrastructure, systems, and services that our products use, the operational practices that we need to abide by, and how you need to administer your environment.

As you expand your business into new geographies or industries, you may face meeting a new set of different and even more stringent requirements than what you're used to. Don't worry - we've got you covered.

The infrastructure powering our cloud platform is built with scalable compliance controls, so we can quickly adjust to changes that occur in the regulatory landscape. This approach also allows us to continue **meeting different regulated industries' obligations**.

Some industries - especially those in highly regulated industries such as financial services - require organizations to prove their compliance through audit trails - a detailed breakdown of activities and events within your instances. This requires increased visibility into your instance, which you only get with Cloud Enterprise and Atlassian Access.

Standard and Premium Cloud products contain audit logs that you track key in-product events. Still, they don't provide full visibility into the security of your data across all of your Atlassian products in one location. With Atlassian Access, you can access organization audit logs, which track events such as changes to someone's access to your products or shifts in administrative access. Unlike product audit logs that are dependent on the amount of storage your plan has, organization audit logs are retained for 180 days to provide you additional assurance.

And if your organization requires even more granularity, with Enterprise Cloud, you can choose to include user-created activities in your audit logs. This allows you to track product actions for both unmanaged and managed in a central location. For more information, [check out our audit log Community post](#).

“ Many people think innovation and compliance are contradictory. But we have to do both of them. We drive innovation by being compliant and showing that we can adhere to regulations.

SOFTWARE AG



The screenshot shows the Atlassian Admin interface for 'Multi-IdP-Playground'. The 'Security' tab is active, displaying the 'Audit log' section. The page includes a search bar, a filter for 'Activities', and a table of 30 activities. A search dropdown is open, showing a list of activities with checkboxes.

Date	Location	Actor
Apr 16, 2023 21:40 PDT	Sydney	Jarryd Cla jclark2@atli
Apr 16, 2023 17:26 PDT	Unavailable	Atlassian I Atlassian Int
Apr 15, 2023 17:26 PDT	Unavailable	Atlassian I Atlassian Int
Apr 14, 2023 17:26 PDT	Unavailable	Atlassian I Atlassian Int
Apr 14, 2023 04:25 PDT	Ashburn	Cat2 Anal cat2analytic
Apr 14, 2023 04:25 PDT	Ashburn	Cat2 Anal cat2analytic
Apr 13, 2023 17:50 PDT	San Jose	Sandy Tan stang2@atli

Enterprise Cloud, user-created activities in audit logs

Security controls

It's important that you're putting safeguards around your data too. One of the most common safety nets that people put around their data is encryption.

Data encryption works by applying a ciphertext around your data so that no one can read it unless they have a key to the cipher. With your cloud products, Atlassian primarily handles this under the shared responsibility model. We encrypt your data in transit using TLS 1.2+ with perfect forward secrecy (PFS) and at rest using AES-256. We use the AWS Key Management Service (KMS) to manage our cipher keys, so only people with authorized AWS roles and permissions can access these keys and decrypt your data.

However, you may want more control over who can access your data. Coming soon - Cloud Enterprise will offer bring your own encryption (BYOK), which will enable you to generate and host keys in your AWS account via the [AWS Key Management Service \(KMS\)](#).

This will allow you to reduce the number of people authorized to access your encrypted data, reducing the risk of a data breach. To stay up-to-date, subscribe to the [cloud roadmap](#).

While encryption primarily focuses on protecting your data in backend systems, you need to consider how your teams interact with your data. For example, not everyone within your organization needs to be able to access highly sensitive legal information. We're building data security policies to help you govern how your users, apps, or even people outside your organization can interact with content.

Soon, you'll be able to take a content-based approach to governing how your data in Atlassian products can be used. This differs from a user-based approach that relies on giving or revoking specific permissions that allow users or apps to perform certain actions. For more information, [read our documentation](#).



But you also need to be aware of where data is being stored. Especially at large enterprises, it can become more challenging for teams to know what products your IT team supports. So it's not uncommon for people to spin up new product instances to help them get work done. Unfortunately, these new instances can inadvertently open you up to a data breach. Coming soon, you can stop your managed users from provisioning new products without your approval with [product requests](#). Not only will you have more control, but you'll also get more visibility into your users.

Identity and access management controls

Atlassian Cloud makes it easier for your teams to work how they want to work - whether by accessing their products anywhere through their phone or integrating with the other tools they use daily to get work done. And while you get user management capabilities out-of-the-box, you need a strong identity and access management capabilities to ensure that only the right people can access your data.

79%


of critical infrastructure organizations didn't deploy a zero-trust architecture


[According to the 2022 IBM data breach report](#), 79% of critical infrastructure organizations didn't deploy a zero-trust architecture. Atlassian secures access to its corporate network, internal applications, and cloud environments through Zero Trust, but you must adopt a similar strategy with your organization. To learn more, read our guide - [Understanding Zero Trust Security: Why It Matters and Where To Start](#).


[Atlassian Access](#) enables admins with IAM features and capabilities that allow you to apply security and governance over your users and devices from within the Admin Hub - allowing you to implement a zero-trust approach. And did we mention that you get Access included with Cloud Enterprise?


Users

Continuous identity verification lies at the heart of a zero-trust security strategy. To ensure employees have access to the right resources, you'll need to have a robust user management system and set up strong processes.

 **Enforced SAML SSO:** Verify users' identity using SSO by syncing your external identity provider - or identity providers - to Atlassian Access.

 **Multi-factor authentication:** Require your users to authenticate in two distinct ways before they gain access to any corporate systems.

 **Automated user provisioning:** Integrate an external user directory with your Atlassian organization to automatically update the users and groups in your Atlassian organization when you make updates in your identity provider.

 **IP allowlisting:** Specify which IP addresses users must use to access content for Jira Software, Jira Service Management, and Confluence

Devices

Devices accessing corporate data should be uniquely identified in a database. By having employees register any bring-your-own-device (BYOD) and corporate devices in an MDM program, you'll know exactly which devices are accessing your system and ensure that they meet your enterprise's security needs (by having up-to-date operating systems or requiring a passcode).

 **Mobile device management (MDM):** Configure security controls for your users' iOS and Android devices, whether provided by your users or your organization. This allows you to enhance security by:

- Updating software and device settings
- Monitoring compliance with organizational policies
- Remote wiping or locking devices

 **Mobile application management (MAM):** Create a policy that specifies how your users' devices need to meet your security requirements before they can access the mobile apps connected to your organization. Unlike MDM, you don't need additional software; users don't need to download additional device management software or enroll their devices.

Prevents attacks with threat detection

Applying controls will help you protect your data, and users will reduce the risk of a data breach. Still, one of the most important tools you need in your arsenal is the ability to monitor your environments to stop threats before they ever happen.

Threat detection adds an additional level of oversight to your instance so that you can track day-to-day events quickly to identify any malicious activities. Because security is critical to enterprises, Enterprise Cloud and Atlassian Access have robust threat detection features.

One of the many advantages of SaaS solutions is that it's easy for teams to get started. Unfortunately, that also makes it easier for teams to download new versions of products outside your IT department's governance, which presents another way for data to be accessed. With Automatic Product Discovery, you can seamlessly access this information from the Admin Hub and take immediate action.

Automatic Product Discovery runs a daily analysis to see if instances are created by anyone with an email address attached to your organization's domain. It sends you a daily email with this data. Through the Admin Hub, you'll see who created the instance and how many users are using it so you can decide if you want your IT team to begin managing it or work with the instance owner to get them on your company-managed instance.

It's also important to know what activities people are doing within your Atlassian products. While you or someone on your team may be a security expert, most people are not, and they may unintentionally expose you to additional risk.



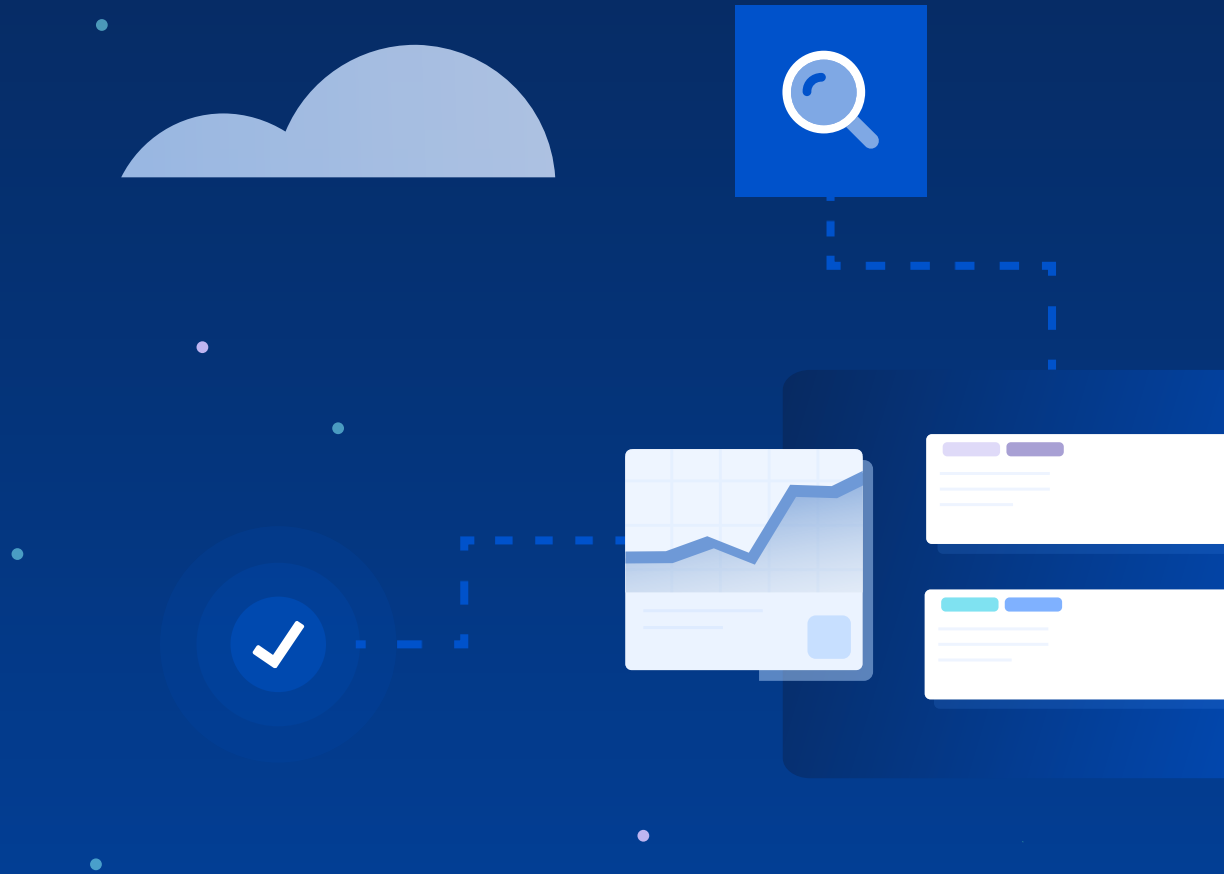
Org and admin insights: Track active users who have viewed a page, view active vs. inactive users, and see how many managed users have two-step verification applies relative to users who have access to your products who are unmanaged



CASB integration: Connect to the CASB software McAfee MVISION Cloud to get automatic security monitoring and behavioral analytics through your McAfee MVISION Cloud dashboard

03

Intuitive insights and analytics



Critical insights to drive data-driven decisions

While having access to data is important in maintaining your security and compliance posture, it's also paramount for growing your competitive advantage as you scale your organization.

You and your teams are generating a lot of data across multiple systems, products, and even devices - all of which contain critical insights into your business. For example, you can see the average time a development team spends in each phase of the software development lifecycle and determine how to allocate resources during the next release to deliver value faster based on data pulled from Jira Software tickets.

“ We have real-time data at the team level and strategic level to make even better decisions, track milestones, and understand what we need to do to deliver.

DISH WIRELESS

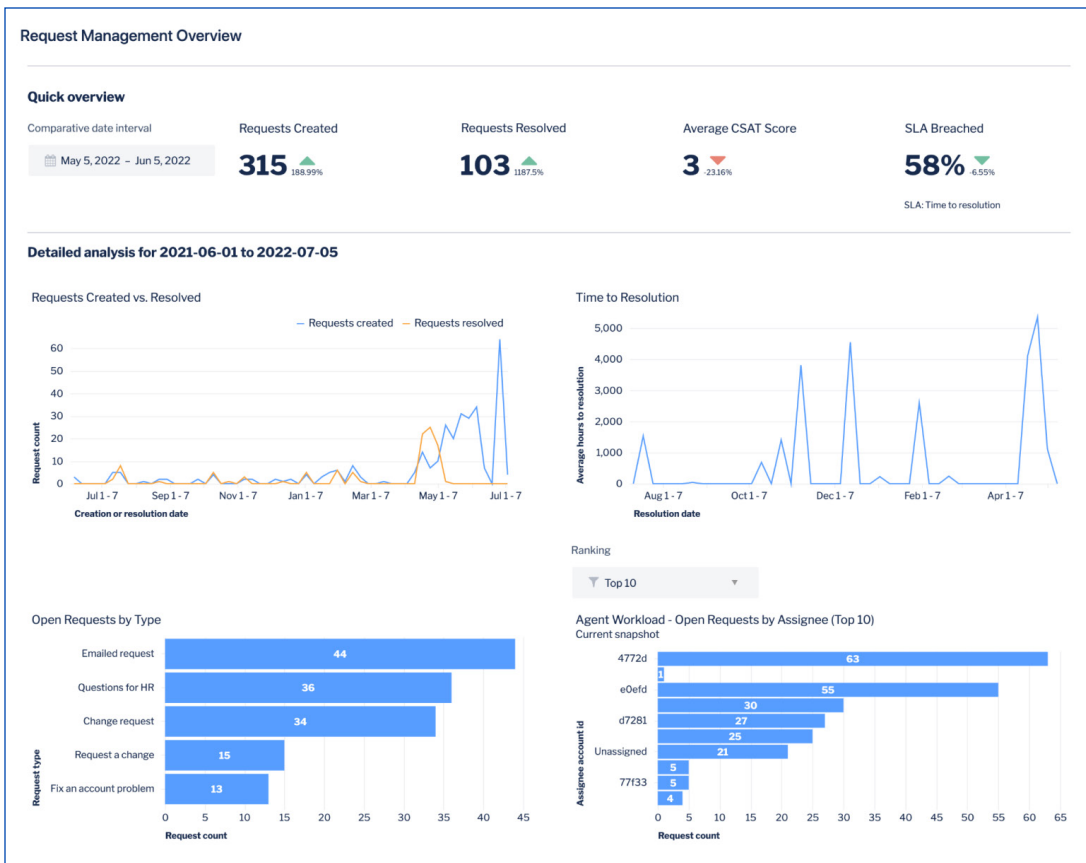
However, data is often siloed amongst teams and products, making it difficult to access. Enter Atlassian Analytics. [Atlassian Analytics](#) - included with Enterprise Cloud - enables you to visualize data across your Atlassian products and data sources to help you gain insight into how work gets done across your teams.

With all of your data in one place, you can look at:

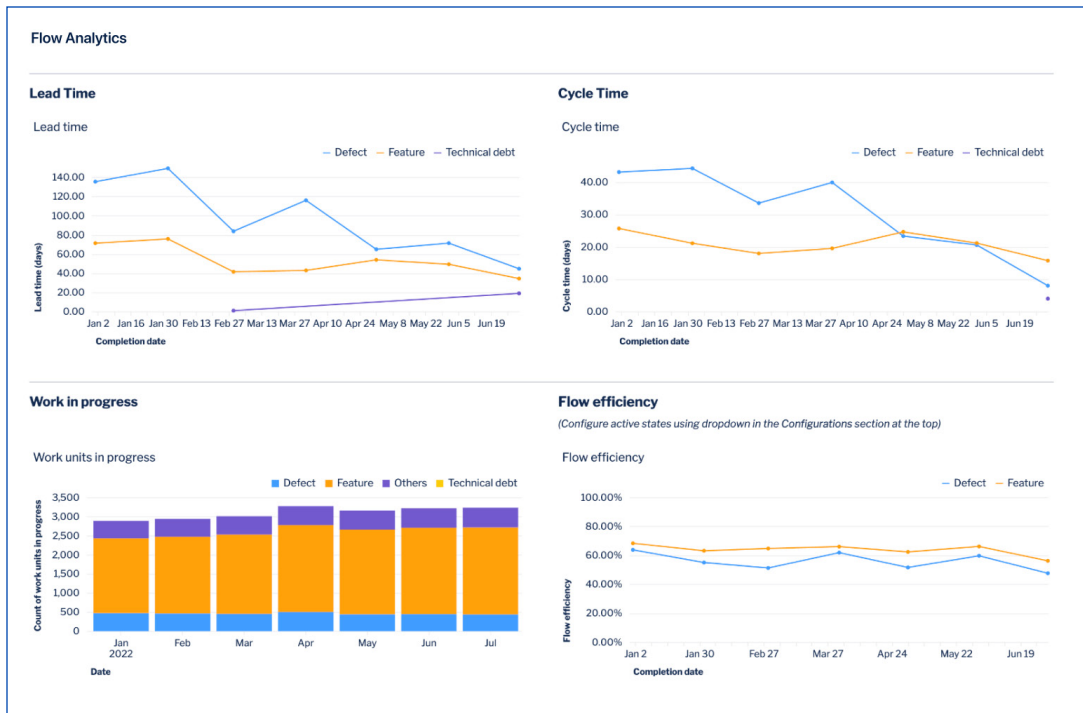
- **Goals:** What is your organization trying to achieve at different levels - as a team, a team of teams, and the whole company?
- **Teams:** Who is working on what, and who needs to collaborate?
- **Work:** Where are your bets placed? What projects will help you achieve your organization's goals?

i Atlassian Analytics comes backed with out-of-the-box goodies, including:

- Pre-built dashboards for service management, asset management, and DevOps use cases
- Custom data analysis with an easy-to-use visual SQL interface
- Multiple options for visualizing your data, from tables to pie charts, bar charts, and more
- Database connectors to query non-Atlassian data sources, including Snowflake, Amazon, Google, Microsoft, and SQL.
- Collaboration features with the ability to share, comment, and manage permissions down to the chart level



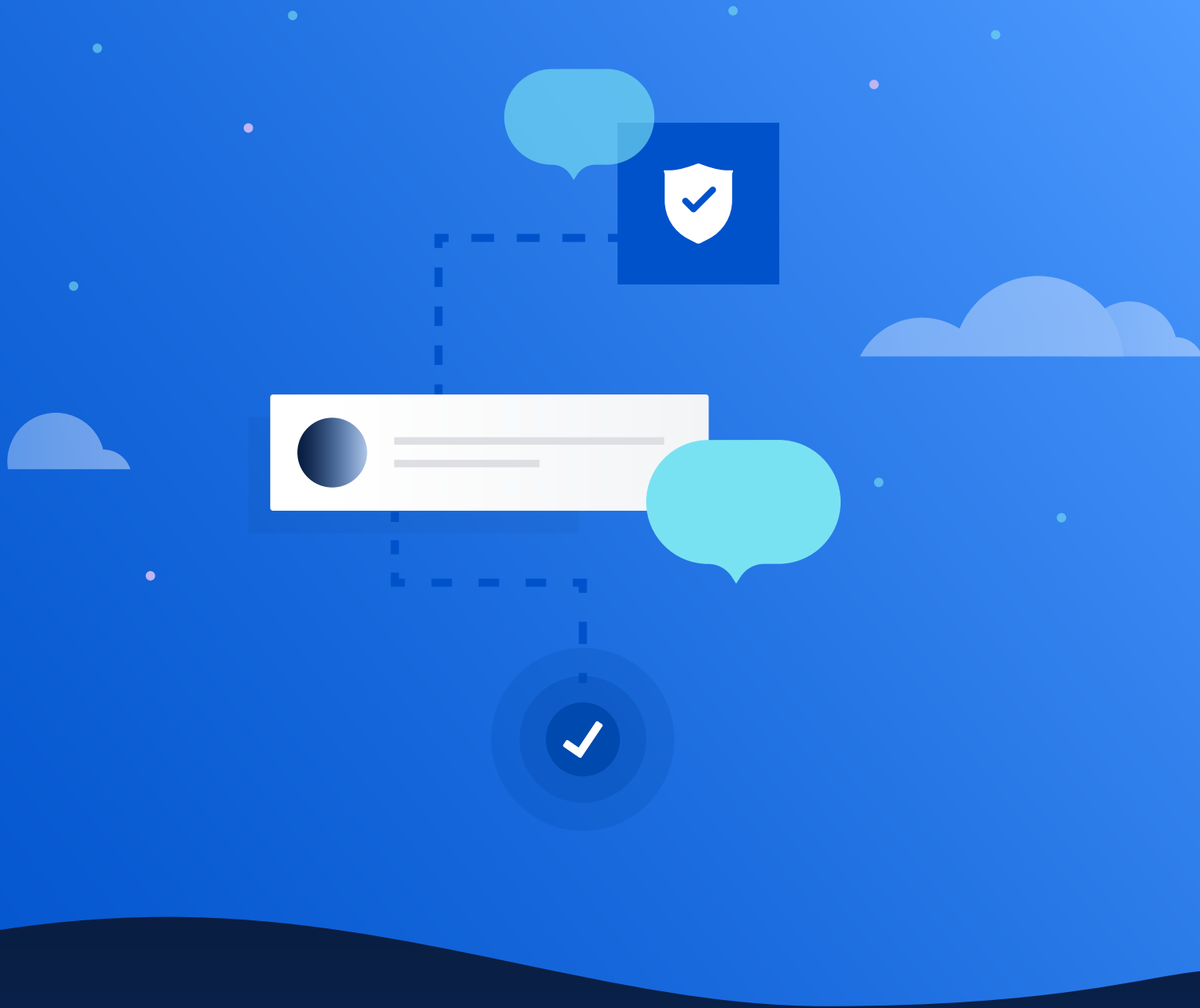
IT Service Management



DevOps

All you need to do is connect a data source from which you want to pull data, and you can begin using the dashboard and chart templates to start reporting on your common business use cases.

Atlassian Analytics also seamlessly connects to the [Atlassian Data Lake](#), which stores all of the data from your Atlassian Cloud products in a single location that you can query for better analysis. Pre-modeled and enriched data fields - eliminating the need for manual and complex data modeling processes. In short - you don't need to transform your data just to gain insights. And soon, you'll be able to access data into the BI tool of your choice.



Ready to learn more?

Contact us at [Contact Atlassian for Enterprise Solutions | Atlassian](#)

 **ATLASSIAN**

©2022 Atlassian. All Rights Reserved.
CSD-4347_DRD-04/23