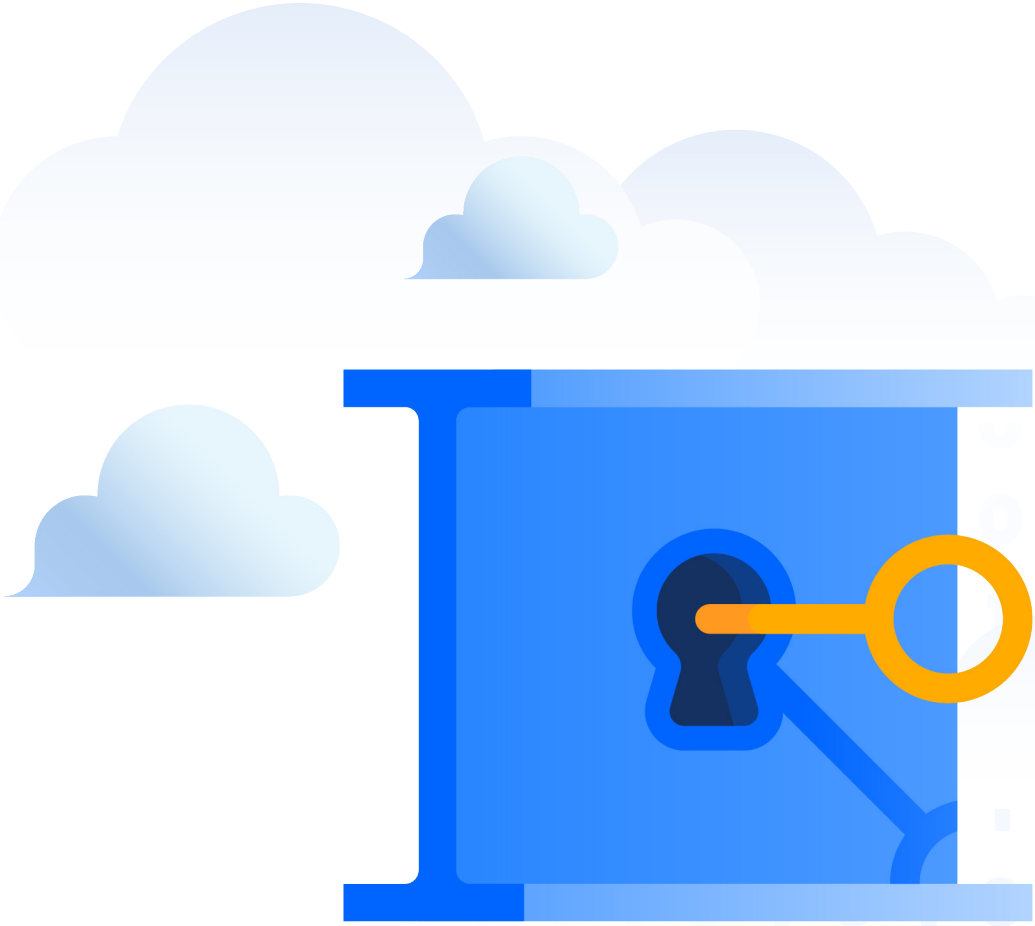
ATLASSIAN

# How to take back control over your data



INTRODUCTION

# Today, more than 92 million people are working remotely.

They are creating, accessing, sharing, and storing data wherever they go and exploring the ways in which they work best. While employees love this new sense of flexibility, enterprise leaders are struggling to address the growing risks of this new explosion of data.

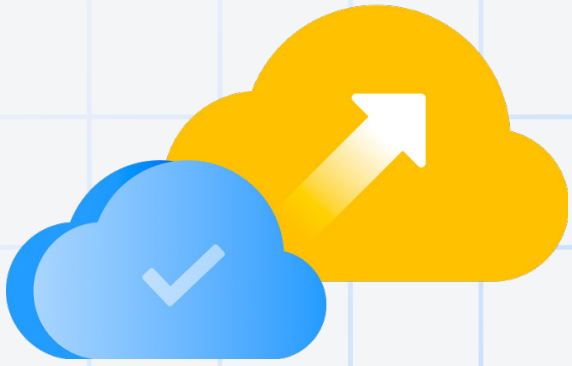
In fact, only 40% of senior executives reported having fully addressed the risks associated with these evolving environments, which is not surprising considering the impact of data breaches has increased by 15% in the last three years. Given the need for employee flexibility and the rise in risks, how can enterprise leaders balance both? Atlassian is here to help you develop an effective strategy for data protection that continues to empower your teams to do their best work.

# Safegauarding your data with Atlasstian cloud

Data protection is part of Atlassian's DNA. With hundreds of employees focused on building, maintaining, and optimizing our secure environments, we take pride in the work we've done to design an end to end strategy that ensures your data is secure, private, and compliant. However, in Cloud Enterprise, we take it a step further.

Cloud Enterprise was designed for customers who are looking to address more sophisticated use cases for security. In a recent study, IBM saw that organizations with the most advanced security capabilities delivered **43% higher revenue growth** than peers over a five-year period.

Learn about four tactics that will help you use the advanced security features we offer in Cloud Enterprise to ensure you remain protected against the most challenging threats.



# Tactic 1

## Hold the keys to your castle with advances encryption

**Two-thirds of executives** consider cybercrime their most significant threat in the coming year. And with the average cost of a data breach at $4.45 million, it's no surprise that every organization is scrambling to fortify their digital walls to ensure their data stays secure.

These threats are so everpresent that it's critical that you've designed the very foundation of your security strategy to combat these threats. Enter: BYOK (bring-your-own-key) encryption.

Data encryption is always a no-brainer. Encyrption replaces legible data (plain text) with unreadable code, known as “ciphertext”, ensuring that the plaintext is only accessible for use by authorized parties. To decrypt the ciphertext back to its original, legible form, you input the key used in the encryption algorithm.

Should someone get past the myriad of barriers we’ve put in place, even if the attacker obtains your data, they won’t be able to understand or decrypt it without access to the encryption keys. And while all of Atlassian Cloud offers encryption at rest and in transit, both of those mechanisms use keys managed by Atlassian. In Cloud Enterprise you can choose to shift that dynamic so that you own and manage the keys that encrypt your data.

With BYOK encryption, you stay in complete control of your data, get visibility in how, when, and why your data is being accessed, and finally whenever you decide that you no longer want Atlassian (or anyone else) to have access to that data, you can revoke access.

### How it works:

BYOK encryption allows you to encrypt your product data with a key you own and manage from your own AWS account. The keys are specific to your organization and can be revoked at anytime. If you decide to revoke your keys, all BYOK-enabled instances will be suspended and can only be restored within three days of revocation. Learn more by visiting **our documentation**.

# Tactic 2

## Protect against unexpected threats with multiple instances

More often than not, when you think of cyberthreats to your organization you're thinking about external hackers trying to get in. In reality, the call is often coming from inside the house. **60% of data breaches** are caused by insider threats; some are intentional, but usually it's accidental or employee negligence. One of the simplest and most effective ways to protect your sensitive data is to restrict access to instances containing sensitive data on a need-to-know basis.

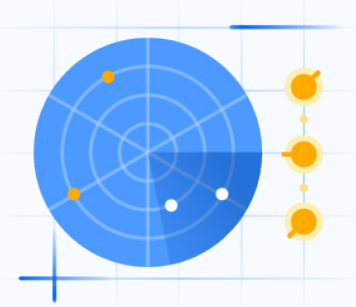
With the flexibility of Cloud Enterprise and the ability to create unlimited instances, you can keep unauthorized teams away from highly sensitive data. Depending on the complexity of your organization and data strategy, you can create numerous instances, each with its own identity and access management strategy.

The multi-instance approach is great for sensitive data but also confidential projects and mergers and acquisitions (M&A). If you are one of the **tens of thousands of organizations** that have to go through a M&A, using separate instances for your team and the recently acquired teams enables everyone to continue doing work uninterrupted. It also allows every element of your organization to continue to work securely until the new ways of working are decided upon.

The opportunities are endless, and with a neverending amount of data it's important to keep the restrictions high, even within your organization.

### How it works:

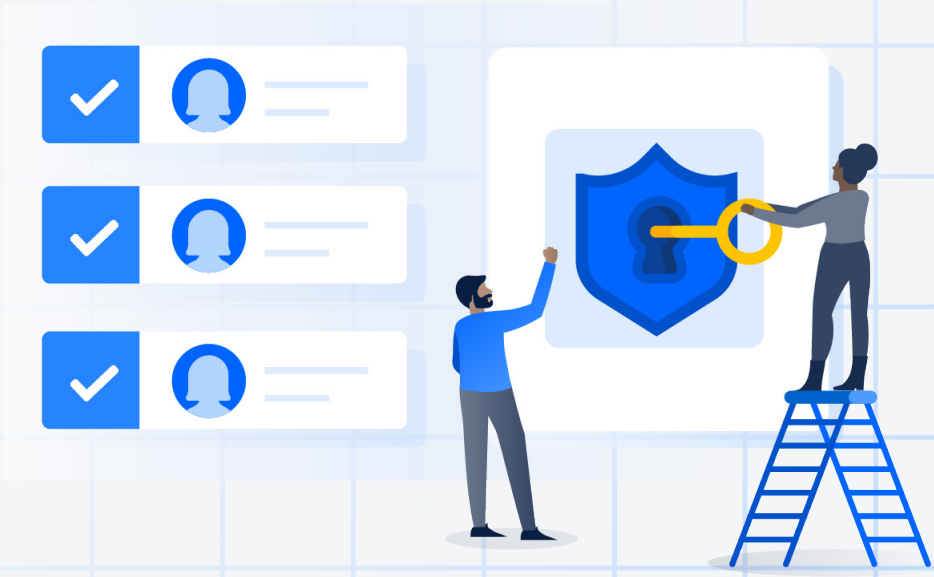
Unlimited instances is unique to Cloud Enterprise and allows you to spin up as many instances as your organizational structure requires while maintaining centralized control of your users in a single place. If you're wondering if multi-instances could benefit your organization, check out **our eBook** to learn more.



# Tactic 3

## Defend against the unknown with product requests

Almost every organization in the world considers security a top priority for their business. The consequences of a data breach or loss of customer data can be insurmountable for even the best brands in the world. The risks are so high that **Gartner predicts that information security spend will grow 11.3% this year to reach more than $188.3 billion.**



Yet, one of the trickiest problems to solve is often one of the most well-intentioned: shadow IT. It's often just employees (or teams) looking for apps that will allow them to move faster and work more efficiently to accomplish their tasks. It's so popular that **80% of employees admit to using applications without IT approval.** However, in their search for productivity, they're introduced massive risks to the organization.

What IT is unaware of, they can't control for. All the risk mitigations your teams have implemented over your known systems are missing in the environments you're unaware of. To address these risks and put admins back in control, we've built product requests. Product requests empowers your admins with the tools they need to block apps before they can cause any harm.

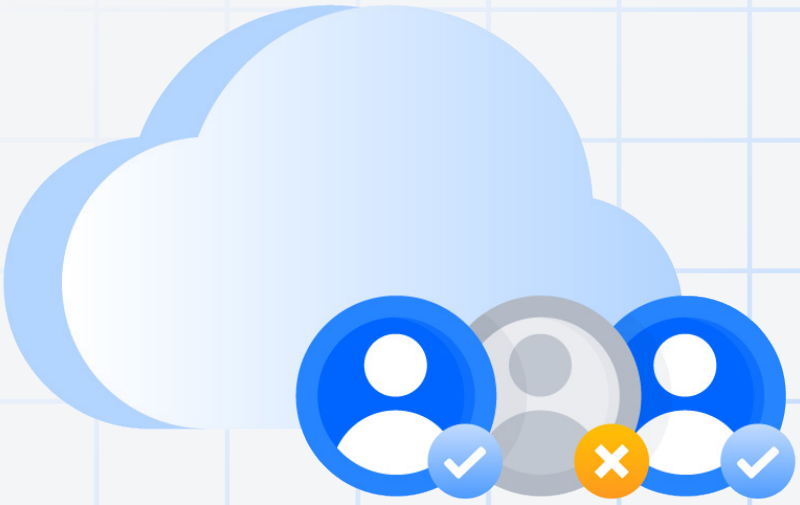
### How it works:

When an employee tries to sign up for a product, Atlassian will send that user to a page where they enter details about how they plan to use the product. Admins will review all their users' requests, from the product requests page, and either resolve or deny any instances from being created.

# Tactic 4

## Increase collaboration without compromising security with external user security

Innovation starts with collaboration. Sometimes it originates from within the same team or organization, other times it is ignited by working with an external partner or company. There are tons of reasons for your employees to want to collaborate with individuals outside of your organization, and often the results improve overall performance. In fact, a study showed that companies that promoted **collaborative working were 5 times as likely to be high performing.** The challenge lies in enabling them to do so securely.



New users introduce new risks to your environment, complicating your ability to control access and secure your organization's data. Cloud Enterprise provides you with the advanced security capabilities needed to unblock teams and ensure secure collaboration throughout your organization. With external user security, you can control authentication for users outside of your organization and enable your teams to collaborate with anyone they need to, without compromising your organization's security posture.

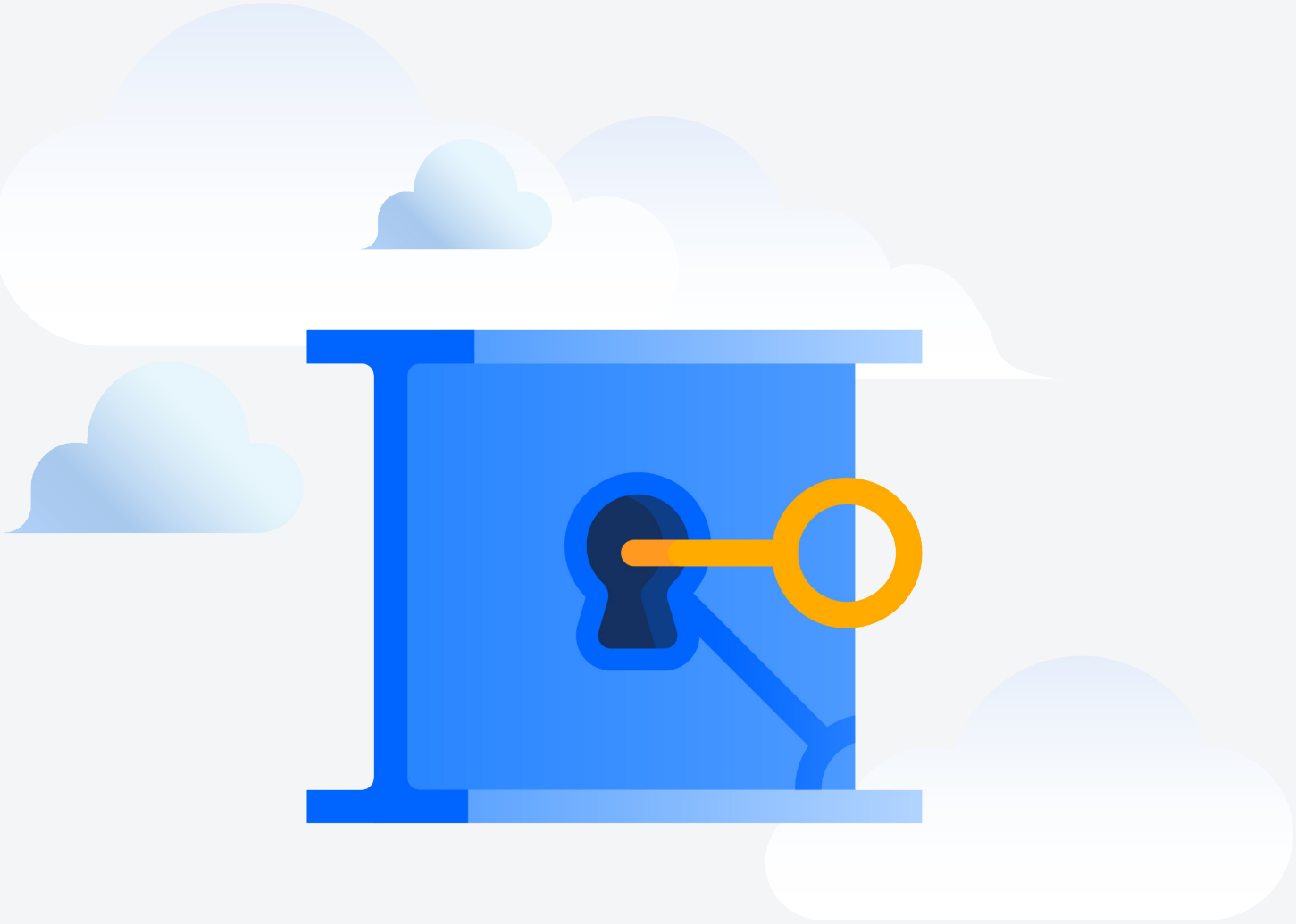
### How it works:

Using **Atlassian Access,** which is part of your Cloud Enterprise subscription you can turn on two-step verification and restrict access to features such as API tokens for users who are not part of your organization but are still collaborating with your teams.

**CONCLUSION**

## Cybercrime is a multi-billion dollar industry for hackers.

Every year, the attacks get more sophisticated and can have a significant damage on a brand's reputation and bottom line. The only way to combat these challenges and regain control over your data is to design a robust data protection strategy that tactics every facet of the way your teams operate. With Cloud Enterprise you get that just that – solution that has the flexibility and control your teams need to do their best work, securely.



Contact us to learn more about how Cloud Enterprise can help you deliver better results for your organization.

atlassian.com/enterprise/contact



ATLASSIAN