



**4 ways Atlassian Cloud
helps you scale, from
any size to enterprise**

INTRODUCTION

With companies today increasingly going remote and scaling globally, operating in the cloud has never been more appealing. Moving more systems to the cloud offers organizations the flexibility to better support dispersed teams and scale their business up or down more easily, with fewer overhead costs and no downtime. It also allows IT staff to focus their efforts away from backend support – such as monitoring security risks, provisioning users, and installing security patches – to the work that truly impacts their bottom line: Building new products for your business and your customers.

Moving to a cloud-first approach clearly has its benefits for organizations, but it can also present challenges – which may be magnified by a time crunch. For many companies, the move to a cloud-based system needs to happen quickly, whether due to sudden, explosive growth or the desire to minimize downtime during data movement. In 2020, in fact, 59 percent of enterprises expected their cloud usage to exceed prior plans due to the COVID-19 pandemic, according to a Flexera survey.

Regardless of the circumstances behind the shift, all organizations should also be aware of four critical cloud challenges for enterprises: cybersecurity management, software scalability, the need for centralized governance, and the ability to customize software for different use cases. In the table below, you'll find just a few examples of the challenges and potential solutions involved in adopting a cloud-first strategy.

Table of Contents

2	Summary
2	Enterprises need strong cybersecurity management in the cloud
3	Growing organizations need software that scales
4	IT managers need centralized software governance and control
5	Growing teams require flexible solutions for their unique use cases
8	Enterprises need strong cybersecurity management in the cloud
12	Growing organizations need software that scales
16	IT managers need centralized software governance and control
20	Scaling Safely and Securely in the Cloud

Summary

1 Enterprises need strong cybersecurity management in the cloud

THE CHALLENGE

According to a [Crowd Research Partners survey](#), 90 percent of security professionals are worried about cloud security, especially when it comes to data loss, privacy, and breaches of confidentiality. And rightfully so: A shift to remote work and rapid growth can often increase security risks. According to [McAfee](#), 52 percent of companies that use cloud services have experienced at least one security breach. Throughout the transition from a private or hybrid cloud to a cloud-first approach, enterprises need to keep a keen eye on security risks and work with a partner that provides strong cybersecurity management..

THE ATLISSIAN SOLUTION

Atlassian offers [enterprise-grade security](#) across its full suite of products, and 24/7, dedicated support staff to our [Cloud Premium and Cloud Enterprise](#) clients. We keep our security program in compliance with the highest industry standards, encrypt our cloud products both in transit and at rest, and offer enterprises organization-wide protection using Security Assertion Markup Language (SAML) single sign-on and two-factor authentication through Atlassian Access.

2 Growing organizations need software that scales

THE CHALLENGE

Of the 94 percent of enterprises that use the cloud today, **69 percent** use a hybrid private-public cloud solution. Within these organizations, many employees rely on a host of external tools and shadow IT that haven't been approved by their internal IT teams.



What is shadow IT?

“Shadow IT” refers to any IT that’s used within an organization but isn’t administered by that same organization internally. This can include everything from productivity or messaging apps to cloud storage or physical devices. Since shadow IT isn’t introduced by the organization’s IT department, it may not meet internal security standards and can pose a security risk to the organization.

When diverse internal tools haven’t been properly connected and employees can’t rely on a centralized source of truth for their work, these dispersed systems can lead to confusion and disgruntled teams. In fact, according to [McKinsey](#), the average employee already spends nearly one full day a week hunting down internal information. The average large enterprise actually uses over 1,200 cloud services – **with 98 percent of them qualifying as shadow IT**, according to a Gartner report – which makes employees’ frustration understandable.

In moving to a cloud-first solution, it’s paramount that IT managers do away with shadow IT and dispersed, disconnected tools, and instead set up a centralized software system for employees that can easily be scaled. Without one, scaling challenges can lead to a loss of productivity, a lack of transparency across your organization, and a culture of burnout.

THE ATLIASSIAN SOLUTION

When you work with [Atlassian Cloud](#), you gain the ability to scale without limits or ballooning infrastructure costs. Over the last two years, we've [quintupled the user limits](#) on our cloud products without lowering performance, and we offer unlimited horizontal scale to Cloud Enterprise clients with over 10,000 users.

Despite Atlassian's high performance at enterprise scale, we also allow organizations to use our tools in a fully customizable, flexible way. On our Cloud Enterprise plan, IT managers can set up unlimited instances of Atlassian cloud products across their organization, allowing teams to benefit from both organization-wide instances and team-specific instances.

3

IT managers need centralized software governance and control

THE CHALLENGE

With multiple cloud apps making up a large portion of enterprises' workflows today, chances are that most IT managers don't have complete visibility into the full range of tools their employees are using. In fact, according to a Cisco survey, most CIOs estimate that their organization uses an average of [51 cloud services](#) – when, in reality, the actual average sits closer to 730 (and goes all the way up to 1,200 for large enterprises). The use of shadow IT in enterprises not only poses a security risk, but can also make it challenging for IT managers to control software infrastructure, user provisioning, reporting, and deployment across the organization.

In today's remote and cloud-first world, IT manager roles have evolved to take on a more strategic and central role in vetting new software, defining requirements when evaluating contract renewals, and monitoring and governing cloud servers. At the same time, cloud providers have expanded their services to include the monitoring of cloud products. To maintain control when unifying products in the cloud for a cohesive, centralized experience, IT managers should look for cloud providers whose solutions centralize the monitoring, governance, and control of cloud products.

THE ATLISSIAN SOLUTION

With over **10 cloud products**, we understand the need for IT managers to have full visibility and control over their software. Rather than monitoring multiple, disparate products in the cloud, IT teams can take back their valuable time by using Atlassian Access, a central hub for software governance. Atlassian Access allows IT teams to seamlessly monitor software usage across their entire organization, automate user provisioning and de-provisioning, and set stringent security requirements teamwide.

4 Growing teams require flexible solutions for their unique use cases

THE CHALLENGE

Part of the challenge of transitioning to a cloud-first approach is finding a scalable solution that fits diverse teams' needs. Different teams have unique workflows and requirements, and no single piece of software will be able to accommodate every team's needs out of the box (that's likely the reason why your average enterprise relies on 730 cloud tools across its workforce). However, the key to successfully and safely scaling in the cloud today lies not in endlessly expanding your SaaS toolbox, but in including fewer but more flexible tools.

While many software tools focus on specific niches, in recent years platform providers have led the way in offering broad, flexible tools that support teams across an organization, from marketing and customer support to business operations and finance. Platforms that may have started as more niche tools – including Salesforce, SAP, and Microsoft 365 – have since broadened their offerings, and now provide specialized and customizable tools for different departments while maintaining organization-wide collaboration and transparency. Rather than having diverse teams work with their own specialized set of niche tools, organizations should look for broad platform providers whose tools allow for plenty of customization, flexible integrations, and purpose-built functionality.

THE ATlassian SOLUTION

We know that no two teams have the same needs, so we've built our solutions to support that need for flexibility. Atlassian offers third-party app integrations that can solve a wide range of use cases. Atlassian products can be paired with second- and third-party apps and integrations that allow for endless customization and flexibility across teams, with specialized solutions for everything from email and messaging to code review and security. Over 1,000 integrations already exist for different use cases – such as automated Slack notifications when Jira tickets are logged – and for any solutions that don't yet exist, developers can always create, buy, and sell their own unique solutions in [the Atlassian Marketplace](#).

According to a survey conducted by [TechValidate](#), **97 percent of IT organizations said Atlassian's scalability is better than the competition's**. Here's what our customers are saying:

“ [The] benefit of Atlassian [cloud] is that it allows us to support the variety of needs from customers seamlessly and efficiently.”

NATHANAEL DAVIS, DIRECTOR OF BUSINESS SUPPORT AND QUALITY ASSURANCE, ARIZONA STATE UNIVERSITY

“ We chose Atlassian Cloud Premium to support our organization as we continue to scale in cloud, reducing the cost of administrative overhead.”

ALASDAIR THOMSON, SENIOR MANAGER OF IT DEVELOPMENT AND OPERATIONS, REDFIN

These are all real challenges that enterprises should keep in mind as they transition to the cloud. Fortunately, with the right solution, a move to the cloud can be safe, flexible, and infinitely scalable.

Over **180,000 customers** worldwide use Atlassian to empower their teams, increase collaboration, and drive change at scale. With 24/7 support, endless customization options, and the security and scalability enterprises require, Atlassian is building its best-in-class cloud platform to serve any organization's needs.



01

Enterprises need strong cybersecurity management in the cloud

One of the thorniest challenges fast-growing organizations face today is safely managing company and customer data.

One only has to look at the headlines to shudder at the repercussions of a large-scale data breach. In 2020, [credit reporting agency Experian](#) experienced a data breach that affected an estimated 24 million South Africans and close to 800,000 businesses, according to Business Insider. Look further back, and similar data breaches have affected everyone from Equifax to Target, with pricey penalties to match.

Clearly, for businesses dealing with sensitive customer information, data security isn't just a "nice-to-have" feature. It's the very foundation upon which consumer trust and your company's reputation are built, and – along with the obvious concerns of customers – missing the mark can lead to hefty penalties and significant revenue loss.

Outside of enterprises, customers are also increasingly aware of the risks of data breaches, and many have a growing need to control their own data. After all, data breaches can expose any of the following:

- **Personally identifiable information (PII)**, including names, addresses, email addresses, phone numbers, bank account numbers, and more
- **Private data** about a company or individual, such as revenue numbers, income, debt, health concerns, and beliefs
- **Identity data**, such as login credentials, biometrics, social security numbers, passport numbers, and driver's license numbers
- **User-generated data**, which refers to private or proprietary documentation, such as confidential company plans, messages, images, and more

Aside from customer expectations around data security, enterprises also face multiple external data management challenges, such as federal and international compliance laws. Depending on what industry your enterprise belongs to and what countries it services, there are different compliance rules you must meet. For instance, any cloud products used by American federal agencies must meet [Federal Risk and Management Program \(FedRAMP\)](#) certification, while any American company handling health information digitally must ensure that they're compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Depending on the audiences you serve, your compliance challenges may also extend globally: any companies handling the data of EU citizens must comply with the [General Data Protection Regulation \(GDPR\)](#), and since 2015, telecom companies in Germany have had to [store metadata within Germany](#) by law.

Solution: Enterprise-grade security and compliance

Clearly, security is table stakes for enterprise cloud platforms today. At Atlassian, our product promise is to keep our customers up to date with the [latest compliance regulations](#), so we've obtained and comply with all of the latest industry standards and regulations – including System and Organization Controls (SOC) 2, SOC 3, Payment Card Industries Data Security Standard (PCI DSS), ISO/IEC 27001, ISO/IEC 27018, the Voluntary Product Accessibility Template (VPAT 508), and GDPR. [Data residency](#) is also offered across Atlassian cloud plans, with in-scope data hosted within the realms of the European Union and the United States as needed.

By meeting new compliance regulations and monitoring external security risks, the benefit of using a cloud provider means being constantly up to date on security measures without ever needing to manually update software. Security is the foundation of our offering, and our dedicated security team consistently performs rigorous security testing, automated scanning, and third-party audits of our software. [Through our partnership with Bugcrowd](#), a trusted provider of crowdsourced security testing, we have nearly 60,000 cybersecurity researchers constantly testing our products and reviewing our code.

Across our full suite of products, we also use encryption in transit and at rest and equip IT teams with the internal controls they need to enforce organization-wide protection, including SAML SSO, enforced two-factor authentication, and the System for Cross-domain Identity Management (SCIM). Together, these measures help protect customer and company data from both internal and external threats – without needing the constant oversight of your IT team.

How Rockwell Automation modernized its security after 100 years of growth

Clearly, security is table stakes for enterprise cloud platforms today. At Atlassian, our product promise is to keep our customers up to date with the latest compliance regulations, so we've obtained and comply with all of the latest industry standards and regulations – including System and Organization Controls (SOC) 2, SOC 3, Payment Card Industries Data Security Standard (PCI DSS), ISO/IEC 27001, ISO/IEC 27018, the Voluntary Product Accessibility Template (VPAT 508), and GDPR. Data residency is also offered across Atlassian cloud plans, with in-scope data hosted within the realms of the European Union and the United States as needed.

By meeting new compliance regulations and monitoring external security risks, the benefit of using a cloud provider means being constantly up to date on security measures without ever needing to manually update software. Security is the foundation of our offering, and our dedicated security team consistently performs rigorous security testing, automated scanning, and third-party audits of our software. Through our partnership with Bugcrowd, a trusted provider of crowdsourced security testing, we have nearly 60,000 cybersecurity researchers constantly testing our products and reviewing our code.

Across our full suite of products, we also use encryption in transit and at rest and equip IT teams with the internal controls they need to enforce organization-wide protection, including SAML SSO, enforced two-factor authentication, and the System for Cross-domain Identity Management (SCIM). Together, these measures help protect customer and company data from both internal and external threats – without needing the constant oversight of your IT team.





02

Growing organizations need software that scales

When smaller companies' tech stacks include only one or two cloud tools, software management can seem fairly easy to handle at the employee level. But as teams grow and different teams adopt specialized tools, organizations' software toolboxes can quickly balloon to 10, 20, or hundreds of different pieces of software. For employees, this growing “cloud sprawl” and the use of multiple, disconnected tools can easily lead to the **emergence of silos** and decentralized information – leading to confusion and lack of collaboration across an organization.



Cloud sprawl

“Cloud sprawl” refers to the uncontrolled use of different – and often duplicate – cloud services across an organization. Including both approved tools and shadow IT (software that hasn't been approved by an organization's IT team), the average enterprise in 2019 used approximately **1,295 cloud services** across its ecosystem.

Without a central source of truth, valuable information can become siloed within different teams' preferred apps, decreasing organization-wide transparency, harming company culture, and costing employees valuable time as they chase down necessary information. And the effect on employee engagement matters: one [Harvard Business Review](#) survey found that while 81 percent of business leaders rate effective collaboration as important to their company's success, 67 percent of those same leaders run into organizational silos that impede collaboration.

Moving to a unified, cloud-first approach can seem like a time-consuming way to solve organizational cloud sprawl and fix cultural challenges. However, short-term solutions – which can include limiting employees' lists of approved apps or democratizing access to all apps across teams – can quickly lead to organizational tech debt, an outsized number of tools to manage internally, or the emergence of shadow IT, where employees adopt the use of new software without approval from IT teams. Moving to a single piece of scalable software, on the other hand, can provide employees with a single source of truth, boost productivity and engagement, and keep information flowing easily between teams.

Solution: Centralized solutions and tech stacks that scale

Multiple niche apps across an organization might provide each team with the precise tools they need for their jobs, but they don't allow for an enterprise to easily scale its methods and results. A better route for a growing organization to take is to consolidate tech stacks and centralize systems – allowing for huge efficiencies that can increase cross-team visibility and facilitate employee collaboration.

With Atlassian Cloud Enterprise plans, organizations gain access to the entire suite of Atlassian products but can customize different teams' access to those products depending on their security needs, business structure, and customization needs by setting up multiple product instances.



What's a product instance?

In the cloud, a product instance functions as one "installation" or license of a product. While some organizations only need to set up a single instance of a product, others require multiple instances.

Depending on business needs, your organization might set up one instance to be available organization-wide that contains all of the documentation, workflows, and tools needed by all employees. Other instances might only be available to certain teams or employees in order to maintain departmental autonomy, protect sensitive or proprietary data, or separate out different offices by region or specialization.

At Atlassian, as a team of [5,000 employees](#) spread across seven countries, we use multiple instances to power our best work. For instance, our Jira development team has their own customized instance, our finance and security teams work within their own instances (to keep sensitive data private), and our support team has a highly customized instance that keeps them up to date on incoming support tickets.

Instances can even be used to isolate data by geography – so you can ensure that your organization is meeting regional regulations to store data locally – or to access an app that you only want to pay a set seat license for. And on our Enterprise plan, not only are organizations able to set up as many instances as they need, but users are able to access as many instances of each product as they need without paying for extra access.

How Redfin used Atlassian Cloud Premium to scale in the cloud

When Redfin – a tech-powered real estate brokerage – first launched in 2004, the team consisted of a small group of engineers. Employees were welcome to use whatever documentation or communication tools they preferred, and collaboration across teams remained manageable.

However, as Redfin grew, so did its challenges in using multiple, disconnected tools. With 3,000 employees across the organization, Redfin needed to streamline its project management, documentation, and communication systems. Having used multiple Atlassian tools in the past, the Redfin team decided to move to Atlassian Cloud Premium – and their processes transformed.

“Before, there wasn’t a unified place to get anything,” says Evan Lerer, director of engineering at Redfin. “We couldn’t really track where the work was, especially when people who are not in engineering are involved. At a certain point, we needed a different level of communication and sharing, and a better way to manage big, cross-team projects... We needed a centralized workflow to enable that, and none of the tools we had could do it.”

Since making the switch, Redfin hasn’t looked back. The team uses Confluence for organization-wide documentation, Jira Software to create agile and centralized workflows, and Bitbucket as a central code repository. Just a few months into making the switch, Redfin’s cost savings hit \$60,000, and the organization adopted an agile, collaborative approach. “Teams started building their own processes, and it created this agile mindset across all the different teams,” Lerer says. “Atlassian helped us get there. It was really powerful.”





03

IT Managers Need Centralized Software Governance and Control

In today's distributed organizations, the role of IT teams has shifted dramatically. These days, rather than fixing bugs, setting up hardware, or maintaining on-prem servers, they're often making more strategic decisions, taking on buying roles and having to balance IT headcount with software costs within their departmental budgets. And for the **91 percent of enterprises** whose systems live at least partially in the public cloud, managing ballooning software costs and governing an enterprise's systems can become a time-consuming task.

When organizations use a dispersed set of tech tools, IT managers must evaluate and monitor new and existing software to ensure they meet safety and privacy requirements. When new employees onboard, they must be added to the multiple (and specific) tools needed to effectively do their jobs, and when existing employees leave the company, their accounts must be closed or permissions revoked. Across the entire organization, IT managers must ensure that both tools and employees are complying with company policies around security and privacy. In the case of any issues around security or downtime, IT managers also need to have a playbook in place for what to do.

For modern IT managers to be successful, they need full visibility into exactly who is using their products, how those tools are being used, and what information is being accessed (and by who). With a bird's-eye view of those details, managers can then zoom in and decide which portions of their tech stack require more involvement from their IT team and which portions can exist independently. With a limited budget and competing priorities, any tools that can give IT teams added visibility into potential issues can save them valuable time and scale their effectiveness in an enterprise environment.

Solution: Centralized governance and admin controls

To ensure the security of scaling organizations – and the efficiency of their IT teams – IT managers need centralized admin controls that allow them to automate user provisioning, monitor product usage at a glance, and ensure security standards across systems.

[Atlassian Access](#), which is included in the Cloud Enterprise plan, provides IT admins with the centralized controls they need to effectively and efficiently monitor and control their organization's suite of products. With Access' centralized hub, you can monitor which of Atlassian's multiple cloud products are in use and use organization insights to track employee adoption of different Atlassian products. With the ability to see an individual product's monthly active users (MAU) at a glance, admins can determine which seats are worth paying for and make data-driven decisions on products' ROI.

Access also allows IT managers to tackle issues of security from one central portal. Through Access' administrative controls, admins can [enforce two-step verification](#) for all users across Atlassian cloud products, helping keep users' accounts secure even if their passwords are compromised. To keep logins simple for users, admins can also set up [SAML single sign-on](#), allowing users to authenticate Atlassian products using their organization's identity provider.

This allows employees to use the same credentials across Atlassian cloud products while also enforcing identity-related security controls at scale. Using Access' organization insights, admins can then also track how many users have enabled two-step verification or SAML single sign-on (SSO), helping IT teams keep a keen eye on security and solve problems directly at the source.

The security supports within Access don't stop with current employees, either. With Access, admins can also sync product access to their external directories, so that user provisioning and de-provisioning happens automatically as employees are hired or leave the company. Whenever a user is added to your external directory – say, for instance, a new employee joins the engineering team – Access automatically grants them access to the different apps they'll need to do their work. If they're removed from your external directory, Access automatically removes their access to those same apps, saving you money on user licensing and reducing the risk of a data breach by a former employee.

If the employee remains with the company but simply switches teams (for instance, from engineering to product), they would lose access to the apps they no longer needed and gain access to those used by the product team.

CASE STUDY

How **Canva** keeps security at a premium while managing a staff of 1,000+

Since Canva first launched in 2013, the accessible design company has grown to manage over 1,000 employees in offices around the world, including Manila, Sydney, and Beijing. As Canva has grown, its team has embraced cloud solutions, and Canva's engineering team uses Jira Software, Jira Service Management, and Confluence to document policies, onboard new staff, manage hiring and payroll, self-direct incident reporting, and track internal goal-setting.

Canva uses Atlassian Access as a way to restrict access to sensitive information (such as payroll and human resources data) and onboard new employees and contractors strategically. A few days before their first day at Canva, new employees are automatically granted permission to view a restricted set of documents and processes, and contractors are able to access Canva's system externally using Access' SSO and enforced SAML. All user provisioning and de-provisioning happen through Access' sync with identity provider Okta.

"[Contractors and new employees] aren't able to see anything but the documents we send them, because access is restricted through user group access mapping," says Jeff Lai, Canva's internal infrastructure expert. "Everyone across the organization also has access to the edit history, so that's another layer of security to make sure no one is doing anything dodgy to the documents!"





04

Growing teams require flexible solutions for their unique use cases

While most IT admins would love to unify their umbrella of cloud apps onto one centralized cloud platform, there is one glaring challenge that comes with doing so: for most enterprise-level organizations, one cloud provider won't be able to meet every department's needs. With hundreds or thousands of employees working across an enterprise, a single tool out of the box probably won't be able to serve every use case or unique workflow in one busy department, let alone across an entire organization.

No matter how solutions-oriented they may be, any cloud platform out there – Atlassian included – will have a limited research and development budget and won't be able to provide ready-made adaptations for every single use case out of the box (especially when you consider that Atlassian services over 150,000 clients worldwide). This becomes especially true in scenarios where enterprises are working in highly regulated fields and must follow very specific compliance regulations within their workflows, such as permanently deleting completed Jira tickets or getting approval at specific stages of a production process.

The solution to serving multiple departments' complex requirements, however, isn't to add dozens of niche apps to your organization's SaaS toolbox. That approach isn't scalable, nor does it allow for the collaboration and customization growing teams require. For most organizations, a more permanent solution lies in finding the software multi-tool that can be infinitely modified and customized to fit different teams' unique needs

Solution: Cloud platform customization and extensibility

At Atlassian, customization and flexibility have been part of our product's DNA since 2004, when we first introduced the concept of our [Atlassian Marketplace](#). Marketplace allows cloud users to customize their Atlassian products to serve the exact use cases they need – whether they need to integrate with messaging and email apps or introduce poll functionality within Confluence. Our third-party app marketplace enables Atlassian solutions to be the endlessly adaptable Swiss Army knife to allow for your organizations' many use cases.

Today, our marketplace is [home to well over 4,000 apps](#) – with new apps added monthly – allowing Atlassian users to find the exact add-ons they need to customize their products. Over [25,000 active developers](#) use Forge, our serverless app development platform, to build trusted, secure, and scalable apps within our Atlassian-hosted infrastructure.

And if no app exists yet for the use case you need, your developers are welcome to build an all-new solution within Forge's robust ecosystem or commission a new app from one of our authorized app partners. To make sure all apps meet our enterprise-level security for your organization, we require developers to fill in the [Cloud Security Alliance's Consensus Assessment Initiative Questionnaire \(CAIQ\)](#) for all new apps and proactively scan created apps to ensure they meet security requirements. Our [bug bounty program](#) also extends to the Atlassian Marketplace so that all new and existing apps are routinely tested for any vulnerabilities.

Each time you choose an app, you have a minimum of 30 days to try it out before licensing it. And with [Atlassian's Sandbox feature](#) – available as part of our Cloud Premium and Enterprise plans – you can easily experiment with new apps and preview changes before you make them in production.

CASE STUDY

HOW DOMINO'S PIZZA USED MARKETPLACE APPS TO DELIVER PIZZA MORE QUICKLY (AND SAVE \$100,000)

For several years now, Domino's Pizza leadership has branded the global pizza chain as a "tech company that sells pizza." As part of that tech-first approach, Domino's DevOps team has used both Confluence and Jira Software to share specifications, track tickets, and manage tasks. For a long time, however, Domino's security team wasn't looped into projects early enough.

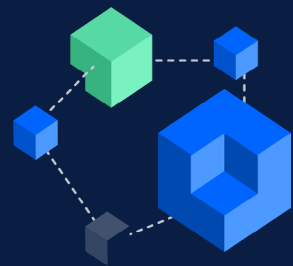
"Security can be viewed as an impediment to progress when there are barriers to collaboration between developers and security," says Michael Sheppard, senior application security engineer at Domino's. "It took hours of meetings just to determine security requirements on projects. We needed to find a faster, easier way to participate in DevOps."

Domino's decided it needed an automated solution to bring DevOps and security closer together. Looking at the way the DevOps team used Jira Software and Confluence, Domino's decided the best solution would be to have DevOps fill in a Confluence form early on in a project's development process, which would automatically submit relevant information to the security team. Working with authorized Atlassian app partner Forty8Fifty Labs, the DevOps team procured an app that would add a 10-question Confluence form into DevOps' development workflow, automatically creating Jira tickets based on the answers.

"We knew our developers liked using Confluence to collaborate and document requirements," says Sheppard. "Security just joined a workflow that already worked well. It takes a few minutes to fill out the form, and about four minutes to get back the corresponding Jira security requirement tickets. What used to require more than 20 hours of meetings and review now takes minutes."

Based on its success in layering Forty8Fifty's app into its workflow, Domino's added a second Marketplace app to its overall workflow, helping the DevOps team better see trends in the support tickets Domino's received and actively build new solutions to tackle them.

“With these two apps, [the DevOps team] were able to save \$100,000 annually, reduce risk by 75%, and highlight this business value to management,” Sheppard says. “In a sense, the apps we found in the Atlassian Marketplace are helping us deliver more pizza faster than ever before.”



Scaling Safely and Securely in the Cloud

In 2020, the COVID-19 crisis pushed many enterprises to move to a [cloud-first approach](#) in as little as 23 days – and according to a survey by McKinsey, the majority believe they'll stick with the change. With many companies continuing to work remotely, the shift to distributed work and agile workflows has only increased. Cloud adoption among enterprises shows no sign of slowing.

In today's rapidly changing digital landscape, many organizations have run into legitimate challenges in moving to a cloud-first approach, but we've built our Premium and Enterprise plans with secure and flexible solutions in mind. As the landscape of cloud technology continues to evolve, you can count on Atlassian to do the same, ensuring that we're future-proofing our partners' organizations along the way.

Interested in unifying your cloud systems on a single platform? Our Premium and Enterprise plans, outlined below, are designed to empower teams to streamline their processes and scale endlessly.

ATLASSIAN CLOUD

PREMIUM

- Standard +
- Unlimited storage
- 99.9% SLA
- Premium support
- IP allow listing
- Sandbox
- Release tracks
- Archiving
- Automation
- Jira Advanced
- Roadmaps
- Admin insights
- IP Allowlisting
- 24/7 Premium Support

ENTERPRISE

- Premium +
- Unlimited instances
- 99.95% SLA
- Enterprise support
- Data residency
- SAML SSO
- User provisioning
- Org audit log
- Dedicated support
- 24/7 Enterprise Support

 **ATLASSIAN** Access
INCLUDED

[Contact us to learn](#) more and discuss how we can help you accelerate your growth, double down on your security, and cut your costs in the cloud.

