ATLASSIAN

Atlassian Cloud: Our resilience philosophy

Introduction

Digital transformation and the resulting application sprawl have increased risk of system downtime for you. According to a Gartner survey, each hour of downtime can cost mid to large-sized enterprises over $300K/hour, underscoring the need for robust system resilience.

In the past, the job of keeping everything running smoothly in a company's computer network was done by administrators. They had to make sure all the data and operations were secure and online. But with Software as a Service (SaaS), things have changed. Now, you need to focus on picking the right SaaS providers that can offer reliable services and quick recovery if anything goes wrong.

Atlassian has been offering solutions for enterprises for over two decades, and we have designed our cloud based products to be robust and reliable. Our cloud based products are designed to provide a high level of availability, effective recovery solutions in case of issues, and proactive management against security risks. Our emphasis on cloud-based resilience allows you to have more time and reduces risks for your organization.

This e-book dives into how Atlassian approaches resilience and the technical capabilities we offer. We'll talk about six key aspects of enterprise resilience that can be applied to any critical business application. Our technical capabilities in these six areas aim to support your resilience goals, ranging from preventing data loss to recovering from system outages.

We don't approach resilience alone; we work in partnership with our infrastructure provider, AWS, and our customers to build resilient solutions. Let's take a closer look at our shared responsibility model.

Shared responsibility: Resilience as a partnership

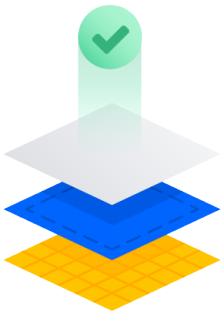
In the world of system resilience, shared responsibility is critical and lies at the core of our trust philosophy. This becomes even more important as our services are built on AWS infrastructure. This model below describes how responsibilities are shared across you, Atlassian, and AWS.

Amazon Web Services	Atlassian	You
Physical security and redundancy of data centers	Building resilient and scalable applications on top of AWS	Managing the secure use of Atlassian's products, such as correctly configuring ACL's and permissions
Providing a high level of network security and system availability	Ensuring the network and application security of its products	Ensuring the safe handling, classification, and access to their data within Atlassian's services
Providing services compliant with global regulations and standards	Adapting AWS's services to provide reliable and secure Atlassian products	Educating staff on secure practices and guidelines provided by Atlassian
Offering robust disaster recovery procedures	Safeguarding the integrity of customer data stored on Atlassian's servers	Ensuring their use of the service aligns with specific industry regulations and their internal policies
Managing and responding to security incidents affecting its infrastructure	Coordinating with AWS to respond effectively to security incidents	Responding to incidents that originate from their own usage of the service, such as data breaches due to misconfigured settings

AWS ensures the physical, infrastructure, and network security of its services. This provides a solid platform upon which Atlassian builds its applications. Atlassian, in turn, is responsible for maintaining secure and resilient application layer. We are also responsible for managing the security of customer data on our application. Your role is managing your application settings, user activities, and organizational requirements.

This three-level shared responsibility model works with the strengths of each party, thus improving system resilience. It allows you to focus on your strategic tasks, with the knowledge that your underlying cloud infrastructure is robust and reliable.

We now dive into each of the 6 components of enterprise resiliency and our associated technical capabilities. As you navigate through these components, you will gain an understanding of the best in class resilience offered by Atlassian Cloud.



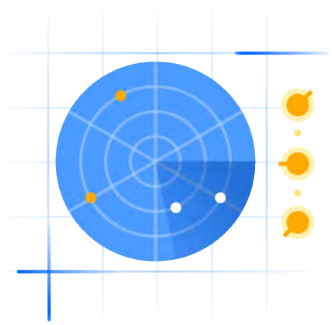
1. Infrastructure availability and redundancy

The core of our approach to redundancy is reliability and availability. We help you avoid the complications of managing backup hardware. When you use Jira Software and Confluence in the cloud, you enjoy the benefits of AWS's wide-reaching infrastructure. This supports our promise of a 99.95% monthly uptime, as set out in our Service Level Agreement (SLA)[1].

We maintain high availability by keeping standby copies of data spread across multiple AWS zones. This built-in redundancy lowers the risks linked to outages and ensures your essential services continue to function. We strengthen our redundancy strategy by regularly testing the switch to backup systems, enhancing our overall service stability.

This setup allows you to concentrate on strategic projects, while we handle the specifics of redundancy planning and hardware management. Your organization reaps the benefits of reduced hardware expenses, higher system availability, and increased productivity.

Alongside ensuring infrastructure reliability, we also give top priority to keeping it secure. Thus, Infrastructure Security Management is a key part of our focus.



2. Infrastructure security management

Keeping our infrastructure secure is not just a defensive strategy–it's fundamental to how we operate. This is especially true for important applications like Jira, Confluence, and Jira Service Management in the cloud. They help protect your IT systems from many different threats.

As a System Administrator, your role in keeping your IT systems secure is very important and ongoing. We share this responsibility with you for Jira, Jira Work Management, and Confluence.

We've put in place strong security features, including Transport Layer Security (TLS) for safe data transmission, and encryption for data storage. These features are part of our cloud infrastructure layer, which is designed to create a safe space for your applications.

On top of these measures, we use a central management system. This system makes sure we have a single approach to managing security. This makes it easier to coordinate and respond to any security issues.

The next important step is to make sure your data, which is stored in our secure infrastructure, is also protected against unauthorized access and removal.

3. Data protection against exfiltration

Keeping data safe from unauthorized removal, also known as data exfiltration, is a very important part of securing SaaS applications. This is true for the application data stored in Atlassian Cloud too. If data exfiltration not handled properly, it can harm your organization, both in terms of money and reputation. Stopping data theft before it happens helps your operations keep going smoothly. It also keeps trust high and can lower the time and cost of recovery.

We use strong methods to stop unauthorized data transfers. One of these is Amazon GuardDuty. This service uses machine learning and threat intelligence to spot harmful activity. This reduces the risk of data breaches. We also give you tools to keep track of active users and to monitor the use of two-step verification for both managed and unmanaged users accessing your products. We offer integration with the McAfee MVISION Cloud software. This allows for automatic security monitoring and behavior analysis.

With us, you can focus on other parts of your job, knowing that your applications are safeguarded by thorough security measures.

4. Data backup and disaster recovery

While it's very important to protect against data exfiltration, it's also key to be able to recover data effectively when required. This helps keep your organization resilient, even when there are disruptions. As an Administrator, you have an important job in this. You oversee the regular recovery of data and recovery after disruptions. At Atlassian, we work with you and use AWS's strong infrastructure to back up data regularly across different Availability Zones.

Atlassian Cloud protects against accidental data loss with strategies like delaying site and product deletion. We're also planning to add a required 'soft-delete' process soon. However, in our shared responsibility model, you also have an important role in managing and doing individual backups to protect against specific operational issues. We also do full and incremental backups that are immutable with a maximum of 1 hour data loss with a 6 hour recovery time.

In our shared responsibility model, we provide strong system-level backups. As a System Administrator, you manage your own data backup and recovery strategies. This approach ensures full data resilience and helps you protect your organization's valuable data effectively.

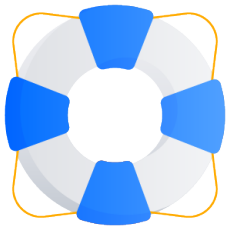
5. Incident management and communication

We realize that dealing with big incidents, particularly ones caused by issues in Atlassian's systems, can be a tough task during busy times for you. To ease this challenge, we offer useful tools and steps to lower your workload and solve problems faster.

Our strategy includes a clear guide for managing big incidents. We use Opsgenie for alerts, Slack for quick text chats, and Zoom for video chats. We keep track of every incident as a Jira issue and create a new issue to track after-incident reviews. We also use Confluence for our incident status docs and sharing post-incident reviews via blogs. We practice and update regularly to make our incident response better and keep your main applications safe.

But remember, you too play a key role. It's vital for you to have your own incident management plan in place. This ensures you can respond promptly when incidents occur, enhancing the reliability of your services.

Beyond just responding, we also work on communication during incidents. We make sure to let people know about incidents across different channels quickly. This keeps you informed and helps you make decisions and act faster. We've also made it easier for you to contact us with a simple system and clear instructions. This makes things smoother during critical times.



6. Incident support availability

We understand how hard dealing with critical incidents can be and we're committed to providing strong incident support. Our improved support offers 24/7 Escalation Management coverage, making sure that help is available whenever an incident happens.

To keep up this level of service, we've increased our Escalation Management coverage around the world. Support teams in major regions provide help all day, every day, so no matter where you are, we're here to assist with and resolve incidents quickly.

Our support doesn't just stop at being available. We've invested a lot in staffing our support teams with product and sales specialists. Their deep understanding of Atlassian's products enables them to offer specific solutions and guide you through tricky incidents.

By using our improved incident support system, the burden of managing incidents internally is lessened. You can count on quick, expert help when you need it, giving you more time for important initiatives. With our incident support, you can focus on making a big difference to your organization's success.

Atlassian is devoted to resilience as a key design principle moving forward.

We know how important your data is and how vital it is for our platforms to be dependable, secure, and robust. Our resilience philosophy is built around shared responsibility and continuous innovation. As we keep growing and changing, we remain dedicated to strengthening our platform resilience.

Learn more about

Atlassian's approach to resilience and reliability

ATLASSIAN