ATLASSIAN

The top 5 security risks of using unsupported software



Calculating the consequences – the cost of a data breach

It's no secret that the use of unsupported software is highly risky, making you susceptible to cyberattacks and potential data breaches. And not only does the use of unsupported software jeopardize the security of your data and privacy of your users, it has the potential to impact your bottom line. The costs of downtime, lost revenues, remediation efforts, and legal fees can have long-lasting effects on your business. In fact, according to a report by IBM in 2022, the average cost of a data breach amounted to a staggering $4.35 million dollars.

How to safeguard your business after server support ends

You've likely heard that Atlassian is ending support for server products. After February 15, 2024, Atlassian and Marketplace partners will no longer provide technical support, security updates, or bug fixes for vulnerabilities on server products or apps. To keep your business safe and secure, we strongly recommend migrating to Atlassian cloud.

Moving to cloud is a big decision requiring thorough research, resources, and alignment from your team. And while it might be tempting to continue using unsupported server products while you make a plan, doing so could put your organization at risk. The Cybersecurity & Infrastructure Security Agency identifies the use of unsupported software as the #1 security bad practice businesses should avoid at all costs.

The top 5 security risks of using unsupported server products

In today's fast-paced digital landscape, maintaining the security of your company's data is undeniably one of the most crucial challenges. As technology rapidly evolves, malicious actors are constantly adapting their tactics to exploit vulnerabilities in your software. According to a report by Forrester published in 2022, this is the leading cause of external cyberattacks. By relying on unsupported server products and apps, you're introducing unnecessary and avoidable risks, such as:

#1: Unpatched vulnerabilities expose your business to security threats – After February 15th, security patches and updates will no longer be provided to server products, which exposes your business to potential security risks. Without patches or updates, vulnerabilities can go unaddressed, making it easier for malicious actors to target and gain unauthorized access to your data and systems. Using unsupported software not only increases your risk but also places an extra burden on your IT teams. They may need to reallocate their time and attention away from strategic initiatives that could drive your company's growth and success to manage, troubleshoot, and secure your products without Atlassian's support.

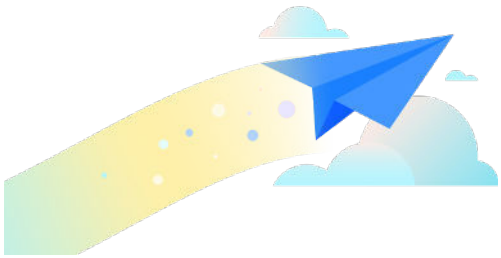
What you can do to secure your business

We understand how important it is for you to keep your organization safe and secure. To protect your business, we strongly recommend migrating to Atlassian cloud, which has data protection baked into the foundation of our cloud platform. By sharing responsibility with Atlassian experts, your team will gain peace of mind and the time to have a more strategic lens in security initiatives – including leveraging Atlassian Cloud-native capabilities to safeguard data.

WHAT END OF SUPPORT MEANS

As part of our efforts to create a world-class cloud platform, we made the choice to discontinue support for server products. We announced this decision in 2020 and since then, we've gradually taken steps toward the end of support, including ceasing new feature development and server license sales.
We understand that this final stage, with the approaching February 15th deadline, may feel overwhelming. The good news is that there's still plenty of time, support, and resources to help you make the move.
Learn more about server end of support

Jumpstart your cloud journey by contacting our team today. They'll help you evaluate your app portfolio, build a business case, make a migration plan, and more. If you're looking for additional expertise and hands-on support, get in touch with a Solution Partner from our network. You can also join our Atlassian Migration Program Community Group to get advice from peers and experts.



#2: Violating privacy and compliance requirements – Using unsupported server products can have severe implications for privacy and compliance requirements, especially for heavily regulated industries like healthcare and finance. Such industries have strict measures to protect sensitive data and customer privacy. Using unsupported software increases the risk of vulnerability exploits, which in turn increases the likelihood of being out of compliance, potentially resulting in legal consequences and financial penalties.

#3: Downtime and potential data loss – Another potential consequence is significant downtime. Unsupported software exposes you to risks from both well-intentioned individuals and malicious actors. They could unintentionally or deliberately disrupt your systems, potentially resulting in data loss or manipulation, and even causing your systems to go completely offline. Consequently, this downtime not only impacts your operational efficiency but also hinders your ability to provide seamless customer support.

#4: Obsolete security technology – Beyond losing technical support and security updates, you also miss out on the latest advancements in security technology. Without access to these innovations, your system becomes increasingly vulnerable to evolving cyber threats.

#5: Risks from unsupported Marketplace apps – You can no longer buy new apps for your existing server licenses. And as we mentioned above, Marketplace partners will also no longer be expected to provide technical support, security updates, or bug fixes for vulnerabilities, which multiplies your susceptibility to security threats.