

Atlassian Guard Standard Saves Time While Securing Sensitive Information

Atlassian commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Cloud Enterprise.¹ Cloud Enterprise is Atlassian's highest-tier cloud plan, equipped with comprehensive scale, data security and access management, regional and industry-specific compliance, unified data and analytics, and enterprise support. Atlassian Guard is a cloud security add-on that strengthens governance and protection across Atlassian cloud products. This abstract will focus on an organization using Atlassian Guard Standard, which is included with Cloud Enterprise subscriptions.

The interviewee is an engineering operations and support services section chief for a government organization. The organization has more than 5,000 Atlassian users and regularly deals with personally identifiable information (PII) and personal health information (PHI) outside of its Atlassian portfolio.



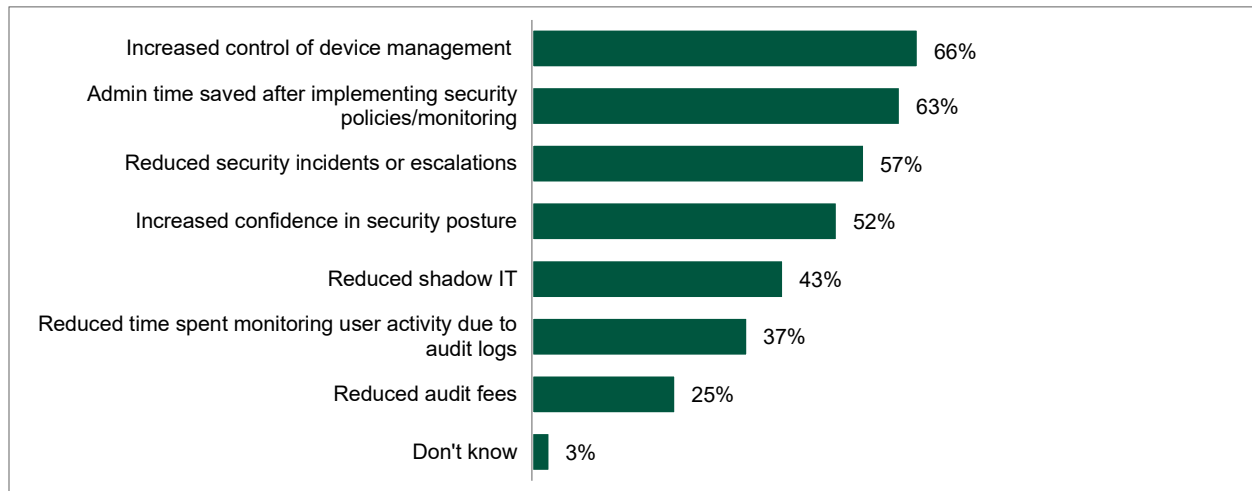
Reduction in investigation time with advanced audit logs

95%

“We can onboard and offboard users very quickly. That’s the time saver, and it’s a security risk mitigator being able to get people on and off as quickly as possible.”

ENGINEERING OPERATIONS AND SUPPORT SERVICES SECTION CHIEF, GOVERNMENT

“You indicated your organization improved data security and access management with Cloud Enterprise. In which of the following areas has it seen improvements?”



Base: 65 decision-makers who indicated their organization improved data security and access management with Cloud Enterprise.

Source: A commissioned study conducted by Forrester Consulting on behalf of Atlassian, January 2025.

INVESTMENT DRIVERS FOR ATLASSIAN GUARD STANDARD

The interviewee’s organization had used Atlassian cloud products for several years, although deployments were siloed and usage varied by team. As usage increased, the organization upgraded its subscriptions to Atlassian Premium and ultimately consolidated onto Cloud Enterprise as the number of users progressed into the thousands. As its Atlassian portfolio expanded, the organization recognized that it would need centralized tools to ensure secure usage — achievable with Guard Standard as part of its Cloud Enterprise subscription. Prior to using Guard Standard, the interviewee’s organization struggled with several challenges, including:

- **Lack of visibility and inefficient manual investigations.** The interviewee’s organization lacked full visibility into user actions within its managed account. It also could not run analytics or provide reports to uncover suspicious usage trends. Investigations were highly manual, and data was incomplete. The interviewee explained: “The regular logs within Jira didn’t give me all the information that the ones in Guard Standard do.

We had some people with admin access doing things that maybe they shouldn't and figuring that out wasn't always easy."

- **Managing access at scale.** One of the key capabilities the interviewee's organization needed was the ability to integrate with its active directory for a single source of authentication. This became increasingly important as the number of users ballooned from 1,000 to more than 5,000. The interviewee stated: "As word of mouth spread [about Atlassian cloud apps], more people started coming and wanting to know what the solution was. We needed to be able to support more users and increase the security."
- **Strengthening security posture by collaborating with the information security office (ISO).** As the number of users increased, the interviewee recognized that their organization would need to collaborate with the ISO and build standard governance protocols into its Atlassian cloud apps. The organization would need to manage this centrally to ensure that the thousands of users were all in compliance. The interviewee detailed: "As we continued to adopt the tool and more people were using it, we started seeing a greater need to collaborate with our ISO and see what policies and guidelines we needed to put in place with our tools."

"The single sign-on authentication creating the single security policy for all of our users to come through and having those managed accounts was really helpful. They allowed us visibility into when people would start creating discovered products outside of or within our managed accounts."

ENGINEERING OPERATIONS AND SUPPORT SERVICES SECTION CHIEF, GOVERNMENT

Read the full study 

KEY RESULTS FOR ATLASSIAN GUARD STANDARD

The results of the investment for the interviewee's organization include:

- **Identified shadow product usage in unmanaged accounts.** Guard Standard offers visibility into shadow IT by surfacing user-created cloud sites. Because this interviewee owns Cloud Enterprise, they also have access to app requests, which means they can not only see when users create new sites but also proactively prevent users from creating unauthorized sites. By using the app requests and discovered app capabilities, admins gain visibility into what their teams are doing and can set proactive policies to derisk their instances. The interviewee explained that they get between four and 10 requests per year, which if not blocked would require roughly 4 hours of work over several weeks to cancel and delete. The interviewee stated: "I always monitor the discovered products, but I also get notified by Atlassian that there's been a new discovered product that's been created in the last 24 hours. So I can immediately hop on that and mitigate it."
- **Reduced investigation time through enhanced security audit logs.** Guard Standard provides more detailed logs that improve investigation quality and time. The interviewee explained: "[With Guard Standard], I was easily able to put in some keywords and dates around a user and some activity that I thought they might be doing. And then of course you have very specific, granular detection types that you can choose from. So it allows me to easily nail down some specific items when we're looking for a specific user who might be doing something they shouldn't." The interviewee noted that without the advanced Guard Standard logs, they would have to reach out to their support team for additional information and investigations would take significantly more time. They estimated that this process would have required 10 to 20 hours in the past depending on the case but could now be completed in 30 minutes.

- **Improved admin efficiency.** The interviewee noted that Guard Standard helps accelerate user onboarding and offboarding. They detailed: “It’s just a matter of putting the users in our active directory into the right Azure group and then they’re automatically given the access that they need in our Atlassian products. So it eliminates having to go in and add those users to our instances individually.” The interviewee explained that this saved roughly 5 minutes per user in onboarding — a significant time savings at their scale: “We’ve continued to double our licensed users since I joined in 2021. So [we save] 5 minutes for one user. But if you’re doubling the amount of users that you’ve had over the year, it starts to become cumbersome.”
- **Strengthened security collaboration and reduced organizational risk.** As part of its security journey, the interviewee’s organization is in the process of upgrading to Guard Premium and collaborating with the ISO to define and enforce guardrails in all of its Atlassian products. This is especially important as the organization regularly handles PII and PHI outside its Atlassian portfolio. The interviewee stated: “It will really help the ISO to know that we’re meeting the standards and policy guidelines they have implemented. We’re putting their mind at ease with all of the guardrails that are in place, and the alerts and notifications can go directly to them. We’re just being completely transparent with the ISO about what’s in our applications and being able to mitigate when things that aren’t supposed to be in there are in there.”
- **Modernized infrastructure to accelerate secure and compliant growth.** Improving its security posture and demonstrating governance will allow the interviewee’s organization to adopt new products more quickly. The interviewee said: “Having these security protocols and guardrails in place is going to make those conversations for future products much easier, and I think it will mitigate a lot of the committees that things need to go through for approvals. I do think it will speed up the time to market for us.”

- **Eliminated expenses with Cloud Enterprise.** Guard Standard is included in Cloud Enterprise subscriptions. For the interviewee's organization that has more than 5,000 users, this is a savings of more than \$10,000 per month.

TOTAL ECONOMIC IMPACT ANALYSIS

For more information, read the full study: "[The Total Economic Impact™ Of Atlassian Cloud Enterprise](#)," a commissioned study conducted by Forrester Consulting on behalf of Atlassian, June 2025.

STUDY FINDINGS

While the value story above is based on one interview, Forrester interviewed 10 total representatives at organizations with experience using Cloud Enterprise, surveyed 162 respondents, and combined the results into a three-year financial analysis for a composite organization. Risk-adjusted present value (PV) quantified benefits for the composite organization include:

Reduced administrative burden for managing multiple sites, improving admin efficiency by 34% and saving \$247,000 over three years.

Eliminated the need for individual site licenses and subscriptions outside of the 150 site Cloud Enterprise allowance, saving \$160 per user and \$340,000 over three years.

Improved uptime and reduced context switching, saving users 26 hours per year valued at more than \$1.6 million over three years.



Return on investment (ROI)

230%



Net present value

\$2.4 million

Appendix A: Endnotes

¹ Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

FORRESTER®