ATLASSIAN

Ask an Atlassian: Security and compliance with Data Center

Q&A about top customer trends

We've been talking to you a lot recently about security, governance, and compliance. Through these conversations and research, it's clear that many of your organizations are under tremendous pressure to respond to meet aggressive business objectives while ensuring the security of corporate data and keeping up with changing compliance requirements.

Modern enterprises depend on complex systems, but the more complex the environment, the higher likelihood of error. Your tools need to have appropriate features to support your evolving needs, and the importance of having the right tools and systems in place only increases as your organization matures over time.

About the authors

Maggie Roney
Senior PMM Team Lead
Data Center

Alison Huselid
Head of Product
Server and Data Center

Junie Dinda
Head of Marketing
Server and Data Center

Marek Radochonski
Senior Product Manager
Platform

Ben Magro
Product Manager
Data Center

Our Atlassian team has joined together to provide answers to the most frequent questions you've asked about trending security, governance, and compliance topics. Let's take a look at what our customers are asking.

Q: ***With remote work on the rise, are you seeing more customers going VPN-less with deployments, and integrating with SAML services like Okta, OneLogin?***

–David

A: We have heard a few reports of these cases from some of our self-managed customers. Here is a blog we recently wrote on a few of the trends we are seeing, particularly its impact on administrators.

–Maggie Roney

Q: ***How do I know my breaking point? With so many variables to consider, how do I determine when to go from Server to DC?***

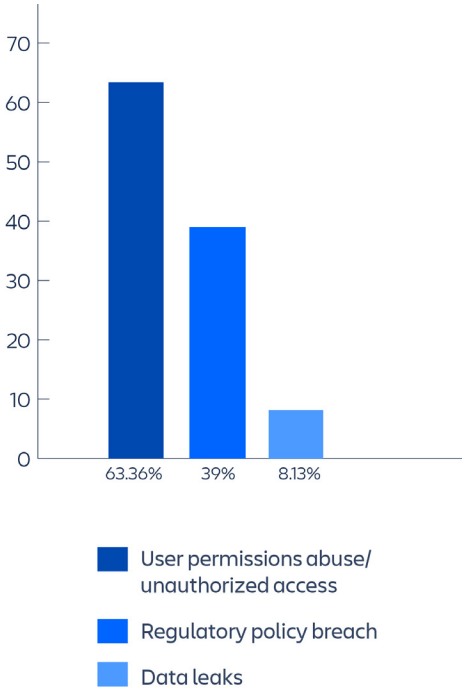
–Joey

A: There's a number of different reasons organizations move to Data Center. Sometimes it's due to the size of their user base, other times it's because they're looking for specific security features like SAML or advanced auditing capabilities. For more resources, check out our blog about the differences between Server and Data Center and our whitepaper that provides a complete guide to Data Center.

–Alison Hueslid

In a customer poll from our webinar *Building for Change*, we learned 25% of companies had to readjust their infrastructure to securely support the work from home mandates due to COVID-19.

What is your top security priority for 2020?



Q: ***What's the best way to ensure I have the right infrastructure for a secure Data Center deployment?***

–Antje

A: To help our customers deploy confidently, we've created documentation to clearly lay out our infrastructure guidelines and recommendations

Additionally, if you're deploying on AWS or Azure, we've also created Quick Start guides crafted with pre-set defaults to help you stand up a Data Center deployment using best practices from Atlassian, AWS and Azure.

–Alison Hueslid

More than 50% of Data Center deployments are on AWS.

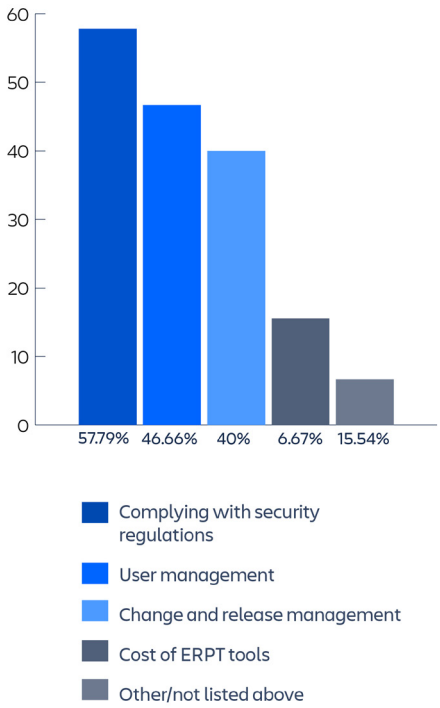
Q: ***What tools are available in Atlassian products to help me manage permissions?***

–Mikale

A: The majority of our Server and Data Center products have delegated administration and permission capabilities. In Confluence, we also have new advanced permission capabilities in Data Center. These features help minimize overheard with auditing, troubleshooting, and bulk editing capabilities.

–Junie Dinda

What are your biggest security, risk, and compliance challenges?



AUTHENTICATION

Q: ***Which Identity Providers can I integrate with using OpenID Connect?***

-Johanna

A: For OpenID Connect, you can integrate with any identity provider that supports OpenID Connect. Check with the identity provider to determine whether it integrates with OpenID Connect or SAML, and determine which would work best for your organization. We support both OpenID Connect and SAML within our Data Center products.

-Marek Radochonski

PROVISIONING

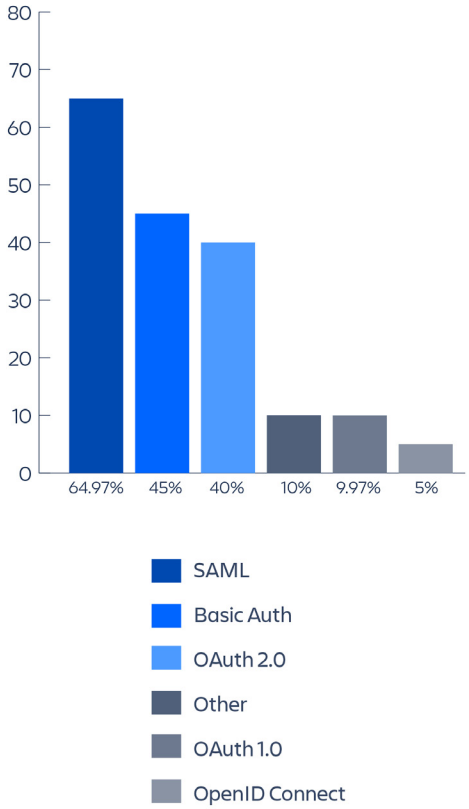
Q: ***Which authentication methods will be supported with Just In Time provisioning?***

-Steven

A: Just-In-Time (JIT) provisioning works with both SAML and OpenID Connect.

-Marek Radochonski

What security standards are in place at your organization for managing users?



PROVISIONING

Q: ***With auto user provisioning, how will you get the user ID, display name and email? Can it come from a cookie, or from some other external source?***

-Carlton

A: The user ID, display name, and email would come directly from the identity provider (IdP) response. With JIT for SAML, they will come as "attributes" from your IdP response, and with JIT for OpenID Connect, they will come as "claims" from your IdP.

-Marek Radochonski

PROVISIONING

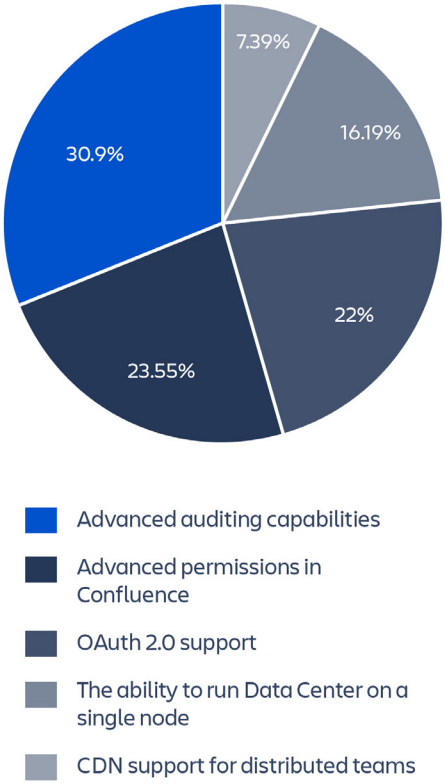
Q: ***How do I clean up JIT provisioned users?***

-Felic

A: There is a special marking attribute. You can run a query to identify these deprovisioned users and obtain a list of all those who have been marked.

-Marek Radochonski

Which security and compliance Data Center capability are you most excited about?



ADVANCED AUDITING

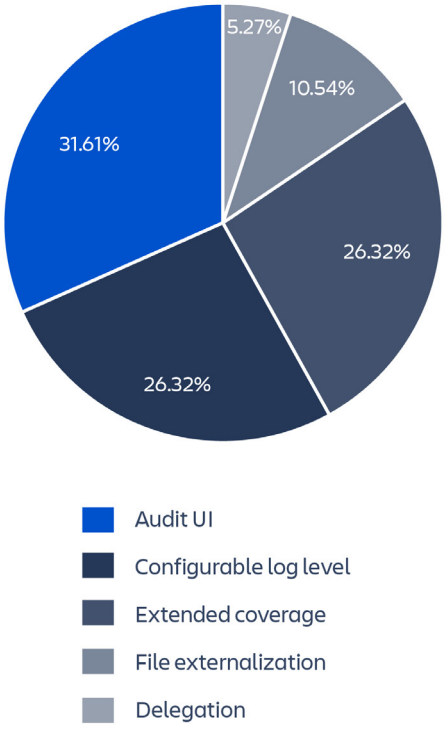
Q: ***What is the best way to determine which auditing coverage level is right for me?***

-Pooja

A: Within our auditing capabilities, there are three levels you can choose from when selecting your coverage. The first level is Base, which is available for Server and Data Center customers. The next levels are Advanced and Full, which are available for Data Center customers, and you're able to set these on a per-coverage level basis. Depending on what you're auditing, you can determine which level is right for you and your organization. As you go up in levels from Base to Advanced and Advanced to Full, you'll be increasing the number of events you're logging. You can also review the following documentation for Confluence, Jira, and Bitbucket which describes the individual auditing events that are contained within each different area. If you're in a highly regulated industry, consider turning on logging events for all criteria just to be safe.

-Ben Magro

What advanced auditing feature are you most excited about?



ADVANCED AUDITING

Q: ***Do I need to be worried about the volume of auditing events being logged and how it will impact my instance?***

-Annalisa

A: You should think about the number of events that are being logged and the volume of those events logged in your system. We think of the database as short-term storage, and we've built in a cap of 10 million records so you don't overload your database with records, and a cap of 100 log files to prevent you from running out of space. We also expose the events via a file for long-term storage. You can plug this file into your logging platforms like Splunk, Cloudwatch, Sumo logic, or ELK. If you're on AWS, you can even send the data to an S3 bucket for storage.

-Ben Magro

ADVANCED AUDITING

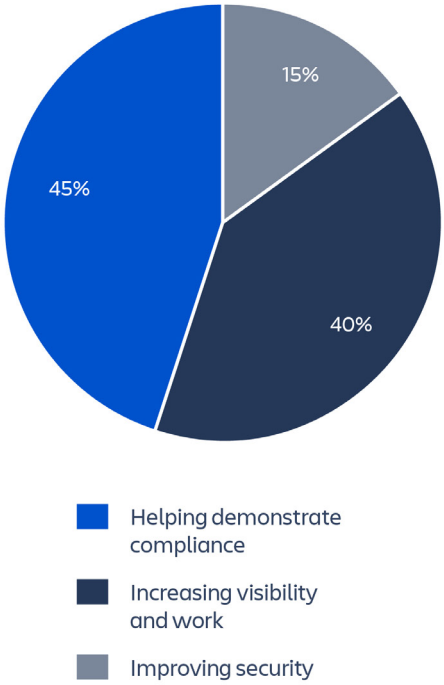
Q: ***In regards to the new advanced auditing capabilities, what if an event we need to capture is not currently audited?***

-Diego

A: We're always looking for customer feedback on our products. While it's possible we may miss some audited events you wish to cover, we'll continue to build onto the capabilities of advanced auditing. Please raise a ticket on JAC here if you ever have any requests, as we do take our customer's voice seriously when prioritizing our roadmaps.

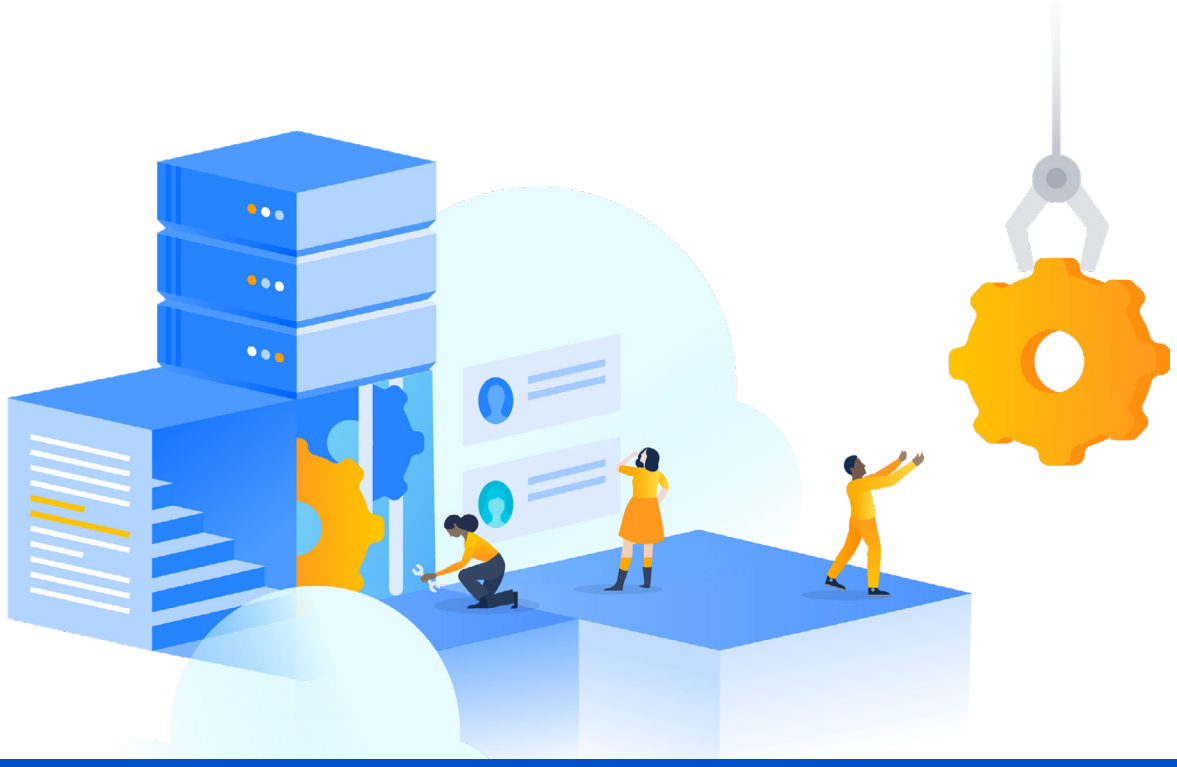
-Ben Magro

How do you see advanced auditing benefiting you the most?



Do you have more questions about security and compliance in the enterprise?

Get our handbook for managing security and compliance for self-managed environments.



ATLASSIAN