ATLASSIAN

The paved path to balancing security and innovation

Enterprises operate in high-change, highly complex environments and need to be even more flexible with their processes and innovative in adapting to changing needs and delivering on business outcomes. External constraints however can make this difficult. Business leaders are dealing with the complexities and increased security risks resulting from remote and hybrid teams, growing cloud adoption, the macroeconomic environment, and more.

PwC's 2023 Global Digital Trust Insights report revealed that cloud-based threats increased at nearly 40% of organizations surveyed, yet fewer than 40% of senior executives reported having fully addressed the risks associated with their evolving environment. So how do you balance security controls with the agility and speed needed to maintain or accelerate business outcomes?

The solution is to build security controls into the foundation of your cloud infrastructure, processes, and workflow. By doing so, your teams will be free to innovate and do their best work securely from the very start.

Atlassian's approach to security

At Atlassian, our mission is to unleash the potential of every team. Internally, this involves providing our own teams with the tools and resources needed to foster a culture of constant innovation. From an IT and security perspective, enabling innovation means allowing teams the flexibility to choose how they want to work, but also giving administrators the necessary security controls to keep data safe.

As a globally distributed company with over 10,000 employees, we constantly think about how to balance flexibility and empowering our teams to make the impossible, possible, with the strict controls needed to ensure our products and organization practices and processes are secure.

This balancing act is top-of-mind for our Chief Information Security Officer (CISO) Bala Sathiamurthy so we spoke with him to understand his approach to security, and how Atlassian scales our security practices to build innovative products for our customers.

Manage control with a 3-lever approach

In securing your internal environment while still providing teams with the flexibility to innovate, Bala recommends three main levers of control:

Have a 'secure by default' approach

Build security controls into the foundation of your cloud infrastructure so that teams have the flexibility to get started with their work, in line with security policies. Bala shares that at Atlassian, "we have very clear, set patterns on the types of hosted images we are allowing on our cloud infrastructure. We have default configurations in place to make sure that when you're spinning up resources, they are secure by default." For instance, S3 buckets created are only accessible within Atlassian's network by default. These patterns are built into Atlassian's internal platform-as-a-service **Micros** which enforces default configurations and security controls automatically so that engineers can deploy and operate services in AWS as quickly, easily, and securely as possible, and Security teams have one less thing to worry about. Bala explains, "this gives folks leverage to do more things in what we call a 'paved path'. The approved base."

Split cloud environments and have different levels of controls

In the production environment where there is customer data, enforce tighter controls and restrict admin access. In contrast, for non-production environments such as developer sandboxes, Bala explains, "we know there is low risk in environments that don't contain customer data. In these cases, we don't want to control what AWS services engineers use because they're experimenting and may want to use something new." With this structure, enterprises can overcome the tension that typically exists between engineering teams who want flexibility and speed to develop, and security teams tasked with protecting sensitive information.

Automate security guardrails

Bala often hears from engineers that they need admin rights for their day-to-day, such as provisioning certain services in AWS. For those in similar situations, he advises teams ask themselves - "is there a way for me to write this into code, push it, and have it run on its own?" If so, these are opportunities to "define infrastructure as code." Automation reduces the need for admin level access, streamlines processes, and allows teams to focus on their core competencies. These automations can also be audited, enabling you to meet compliance requirements.

Ultimately there are many ways to empower teams to innovate while still maintaining security controls. However, if security controls become blockers to the software development lifecycle (SDLC), it is an 'anti-pattern.' As Bala explains, "this indicates that the controls we're putting in are not done in the right way. At this point, we'd explore where we can use automation or other mechanisms to help unblock engineers." Because as Bala asserts, "security and innovation are actually very well aligned."

Maintain visibility across your entire organization

A **Gartner study** on cloud visibility reported that the majority of business leaders surveyed were not confident that they had the full visibility needed to safeguard their organization. However, in order to provide a secure and flexible environment that allows innovation to come from anywhere within the organization, you need visibility to be able to identify vulnerabilities and act fast.

Atlassian has a multi-faceted approach to maintaining visibility across our products and platforms, and ensuring we are proactive in identifying and resolving security threats for secure and reliable development.

We use various monitoring tools as part of our threat detection and response strategy, aggregating the logs and flagging any suspicious activity for further investigation and escalation. In addition, a 24/7 Security Incident and Response Team has improved time to detection and resolution of security incidents, and a number of processes allows our security team to monitor infrastructure and applications throughout development.

One key area is the vulnerability management program. As Bala explains, “we started out looking at a vulnerability platform for the infrastructure, we then went into scanning containers of images, and now we are going one level up to look at scanning code as it is committed. We are moving upstream.” This is further supported by source code analysis tools which detect whether there are known vulnerabilities in any open source and third party libraries that are used in software builds, and automatically raises a Jira ticket with the relevant security team.

By embedding threat detection into every SDLC stage and utilizing a centralized approach, we can automate proactive notifications, escalations, and reporting for end-to-end visibility, while continuing to empower our teams to iterate fast.

Scale security and boost innovation with education and partnership

Teams want flexibility to innovate and build secure products. Security teams want visibility and control to protect their organization’s most valuable asset - data. This is complex when the security team is outnumbered, and risks originate from multiple places, not just during software build and release phases. According to Bala, that’s where education and partnership come in.

Fostering a security mindset to make sure all teams know how to work securely is critical. At the bare minimum, this involves security awareness training for all employees and secure development training for engineers. However, the real mindset shift comes in the form of partnerships with Security.

> I always tell my teams that if you make it easy to do the right thing, most people will not only do it, but they will be very eager to do it.
>
> **BALA SATHIAMURTHY**
> Atlassian Chief Information Security Officer

As Bala contends, "most engineering and product teams want to do the right thing for security. They want to build secure products, but it's complicated." This is why organizations need to help teams realize that Security is a risk management partner. He continues, "you need to align to the business, be nimble, and see yourself as a coach and an enabler." Security teams aren't out to block work, but they do need to be involved early on so that they can enable innovation in a way that's secure for you, your teammates, and your customers.

At Atlassian, a **security champion** is assigned to each product and service team to promote key security practices. Security champions also provide guidance on **product security scorecards**, an accountability and monitoring system that measures security posture for each product and service across Atlassian. In addition, our product security team runs a **security partnership program** providing guidance to product teams and ensuring security processes are integrated into the development lifecycle. By establishing security as part of company culture, you'll build knowledgeable teams who see Security as partners to their innovative ways of working, not blockers.

Conclusion

The perception that security and innovation are at odds is shortsighted. Security and innovation can co-exist if enterprises build security controls into the foundation of innovation. By having a clear set of patterns and paved paths that teams operate within, the tools to maintain visibility, and a partnership between Security and the broader business, enterprises can maintain a greater sense of control and global oversight, while still allowing their teams to innovate and do their best work. At Atlassian, we continue to invest in our cloud products, infrastructure, and processes so that enterprises like yours are empowered to collaborate, and drive secure innovation at scale.

Learn more about Atlassian's approach to security and the latest developments at **atlassian.com/trust/security**

©2023 Atlassian. All Rights Reserved. CSD-4418_DRD-05/23

ATLASSIAN