Tigera Case Study: Atlassian

About Atlassian

Founded in 2002, Atlassian serves more than 125,000 customers around the world. The company delivers a suite of Software-as-a-Service (SaaS) products that enable efficient communication and collaboration across teams, with popular services such as Jira, Trello, Confluence, and BitBucket.

Challenges

Prior to their adoption of containers on Amazon Web Services (AWS), Atlassian's on-premises platform ran a separate virtual server for every customer. Each of these ran a single-tenant instance of Confluence and Jira – resulting in hundreds of thousands of instances. Each of these required its own monitoring, maintenance and carefully coordinated upgrades. With data centers full of equipment and a lot of unused capacity during off-peak periods, Atlassian was not able to operate with the efficiency and scale necessary to keep up with the growth of its business. To achieve more efficient operations, Atlassian turned to AWS. Moving to AWS enabled Atlassian to consolidate compute resources and re-architect its applications for multi-tenancy.

Security and compliance were also of paramount importance for Atlassian with the migration to AWS. The move included not just applications touching customer-sensitive data, but also the Bitbucket/Bamboo code management and continuous integration and deployment (CI/CD) platform. The security approach had to be strong enough to not just isolate Atlassian application code but also external customer application code executed in Bitbucket/Bamboo.

After a multi-year effort, Atlassian successfully re-architected applications to run securely on a Docker-based platform-as-a-service (PaaS). With the re-architecture to multi-tenancy and migration to AWS completed, the team then turned to Kubernetes to improve container orchestration and lower the cost of running containers.

Solution

Why AWS?

After exploring a few different vendors, Atlassian chose AWS for its rich portfolio of managed services, such as Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS) and Amazon DynamoDB, its highly reliable infrastructure and auto-scaling capabilities. These features were critical for their vision on the cloud. They needed a platform that would enable them to standardize their container platform. AWS enabled Atlassian's Kubernetes team to run their workloads on managed compute infrastructure, thereby consolidating compute and removing the operational heavy-lifting from other teams. This has also enabled them to more closely align their costs to actual resource consumption, instead of paying for unused compute capacity.

Why Tigera?

To establish more secure operations, Atlassian required a security solution that could manage the complexity of their Kubernetes and hybrid cloud environments. As part of the installed policies for clusters (the de facto standard for the Kubernetes Network Policy), the Atlassian team found Tigera helped them to deploy a defense in depth posture that ensured security across the network using a zero-trust model. They also appreciated that Tigera was easy-to-configure and deploy, well-documented, and had features to meet all their needs out-of-the-box.

Tigera complements native AWS security policies, enabling Atlassian to establish more granular controls. For example, Atlassian has set up protections to limit the blast radius of potential threats. Security groups are placed on each node to stop them from talking to certain areas of the network, while AWS Access Control Lists (ACLs) run on top of them for more general policy enforcement.

Benefits

Atlassian relies on Tigera to provide a layer of defense-in-depth, establishing a security posture in which only authorized traffic flows are permitted. Working with their Security Intelligence teams, Atlassian has developed an extensive list of policies that must be enforced to keep workloads isolated, and safe from bad actors.

Better yet, Tigera works at the speed of AWS. Using the Kubernetes Network Policy API, development teams can define specific application connectivity requirements and push changes across their dynamic architecture in seconds. These policies work in tandem with the cluster-wide policies defined by the operations and security teams. This is critical to enabling the kind of agility that Atlassian was seeking to gain by adopting a microservices architecture on the cloud.

"We can programmatically alter and enlarge or add new IPs, or remove IPs from our Tigera rules. That's a real benefit to using Tigera for us, it plays real nicely with our CI/CD pipeline…we can make changes in minutes."

— Corey Johnston, Kubernetes Platform Senior Team Lead at Atlassian

Stopped a bitcoin mining abuse in less than 15 minutes

In one instance, a bad actor covertly started to use resources mining bitcoins by spinning up new instances on BitBucket, which consumed resources for legitimate customers on the platform. In a matter of minutes, the Atlassian team was able to identify the incident and deploy a global policy that blocked all connections from containers across the cluster (approximately 40 – 50 nodes) to the specific IP addresses receiving the mined coins. This ended the abuse immediately. Without Tigera, they may have had to go into each node manually, which could have taken 24 hours to complete, all while the abuse continued to cost Atlassian additional money.

Improved agility across the company

Tigera enables teams to stay ahead of potential attacks by defining and applying new rules faster than before. Moreover, the hierarchical policy feature allows different teams to establish their own set of policies, after Atlassian's core, cluster-wide policies (as defined by the platform team) have been applied. This helps prevent any lapses in security coverage and/or compliance violations.

Enhanced organization-wide scalability

The Kubernetes-Tigera integration helped Atlassian securely achieve micro-segmentation of its container workloads. The API-based nature of the solution simplifies the extension of network security policies across on-premises and cloud environments. As a result, they are leveraging Tigera to extending their network security policies beyond Kubernetes workloads, to running on thousands of virtual machines running on AWS.

Achieved an 800% increase in daily JIRA deployments

When operating on-premises, deployments used to take Atlassian more than 24 hours. Not only that, but any update meant customer downtime. Updates to their services required them to take instances out of production, make lengthy security firewall rule changes, then redeploy into production. Leveraging the Tigera hierarchical policy model and AWS multi-tenanted application design, Atlassian is able to deploy updates with minimal impact to customers.

What's next?

Atlassian's next-generation platform as a service (PaaS) is based on Kubernetes and aims to host all of their microservices workloads there in the future. Kubernetes will enable Atlassian developers to build and ship applications more quickly. They are currently exploring how they can leverage Tigera's Application Layer Policy (ALP) to more intelligently manage traffic on a per-application basis.

Other relevant Tigera capabilities include the ability to control access to other VPC resources (e.g. Amazon ElastiCache) and the ability to adopt Windows nodes on their existing clusters to support a broader range of Docker environments on BitBucket.

"As we've been building-out our next-generation compute platform with Kubernetes, we've developed a close relationship with Tigera. Tigera's Calico has pretty much had all the features we've needed. We've never had to explicitly ask for new features, as they've already been on the roadmap."

— Corey Johnston, Kubernetes Platform Senior Team Lead at Atlassian

About Tigera: Tigera provides zero-trust network security and continuous compliance for Kubernetes Platforms. Modern applications are dynamic and break traditional static security models. Our flagship product, Tigera Secure Enterprise Edition, meets enterprise needs for security and compliance and supports multi-cloud and legacy environments with a universal security policy that is automated and delivered as code.

Tigera Secure Enterprise Edition builds on leading open source projects: Kubernetes, Calico, and Istio, which Tigera engineers maintain and contribute to as active members of the cloud-native community.

For more information about Tigera Secure Enterprise Edition and how it can help you secure your modern applications and demonstrate compliance, email us at contact@tigera.io or call us at +1.415.612.9546.

About AWS: For 10 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS offers over 100 services for compute, storage, databases, analytics, mobile, Internet of Things (IoT) and enterprise applications from 49 Availability Zones (AZs) across 18 geographic regions in the United States, Canada, Europe, Asia, Australia and South America. AWS services are trusted by more than a million active customers around the world – including the fastest growing startups, largest enterprises, and leading government agencies – to power their infrastructure, make them more agile, and lower costs. To learn more about AWS, visit http://aws.amazon.com.

aws | TIGERA