CASE STORY

Defense Unicorns Simplify Kubernetes Management and Meet Zero Trust Mandates with the Service Mesh

> “
> Service mesh is the way forward for Kubernetes (K8s) workloads. Tetrate’s government-ready service mesh, along with their expert support, plays a pivotal role in simplifying K8s complexities, elevating security standards and ensuring compliance in mission-critical environments where security is paramount.

Defense Unicorns, a software integrator, specializes in making software delivery easy for the most secure systems in the world Aerospace, Defense and Healthcare and Finance. They provide secure, open source and infrastructure agnostic applications and tools that enable their partners to rapidly accelerate their software acquisition and delivery processes. Staffed by a team with decades of experience delivering technology programs across the U.S. Department of Defense as well as the broader U.S. federal market, the company uses and creates open source tools like Zarf, LeapfrogAI and Pepr.

A key open source project they leverage is the Istio service mesh to enable DevSecOps across cloud-based and high-security, air-gapped environments. Defense Unicorns and its clients often rely on AWS infrastructure services, including AWS GovCloud. Tetrate provides Defense Unicorns with enterprise-level Istio support, enabling the company and its clients to maximize the operational and security advantages of Istio to manage distributed applications on AWS and on-prem environments.

Challenge: Simplify Kubernetes Management and Meet Federal Mandates for Zero Trust

Most new applications and capabilities being built today in the defense sector and enterprise are based on Kubernetes (K8s). Navigating the intricacies of Kubernetes while adhering to rigorous federal zero trust mandates can be challenging. Kubernetes-based, “cloud-native” workloads are disaggregated into collections of microservices across many different containers, which

Challenges:

- Reduce K8s complexity
- Multi-cloud environment
- Lack of operational insight
- Comply with federal Zero Trust mandate

Solution:

- Tetrate Istio Subscription (TIS)
- Enterprise service mesh support

Benefits:

- Streamline K8s management
- Automate routine processes for operational efficiency and dev productivity
- Improve visibility and troubleshooting
- Accelerate time to compliance

makes the task of observing, managing and securing those workloads quite onerous, particularly at scale. A service mesh presents a comprehensive solution to not only streamline Kubernetes complexities but also seamlessly align with stringent zero trust requirements, which the federal government has now mandated for all civilian government agencies (by September 2024) and the Department of Defense (by 2027).

“There's this notion in the defense space that you want to disassociate the people building software capabilities from the people that have to secure those capabilities,” explains Austen Bryan, Director of Product at Defense Unicorns. “The idea is to abstract the complexity away from application developers so that they can move faster, which is great, but somebody still has to collect all the insights from the containers and ensure that security protocols are being met and data is being safeguarded as it is ported from one environment to another. We use an open source Istio service mesh to implement that. It is part of our core technology stack that we take to everybody everywhere.”

Solution: Tetrate Istio Subscription and Expert Enterprise Support

Like Kubernetes, Istio is complex, so Defense Unicorns relies on Tetrate to guide its clients on implementation and provide support to the Defense Unicorns team. “TIS has grown alongside Istio, solving a real problem for regulated environments who need application networking that delivers a standardized zero trust architecture out of the box to include strong NIST compliance mapping,” said Austen Bryan, product lead at Tetrate partner Defense Unicorns.

Bryan has been with Defense Unicorns since February 2022. Prior to that, he was active duty Air Force for just shy of 12 years. During his military tenure, he assisted multiple program offices in helping the Air Force acquire engineering solutions of all kinds. “Over the years, in choosing who to work with, I have learned to seek value alignment more than anything. Certainly cost always matters, but at Defense Unicorns we are obsessed with open source, involvement in the Cloud Native Computing Foundation, and working towards standardization across tech stacks. Not everyone has that same value system. But Tetrate does. We have seen Tetrate collaborate with NIST to establish zero trust guidelines and help move the government forward, and that’s appealing to us. They also built the industry’s first FIPS-compliant Istio distribution. Even more important, we trust Tetrate. They have proved through our relationship that they are going to show up and help. My best advice regarding service mesh is this: First, not using a service mesh today would be irresponsible, especially if you’re running containerized workloads,” says Bryan. “And, second, if reliability is required by your mission, you need to have some level of support. Tetrate is our go-to for Day 2 Istio operations. It’s hard to find people with deep experience running Day 2 operations on cloud-native technologies like service mesh, but Tetrate has it.”

Benefit: Accelerate “Time to Compliance” with Zero Trust Built into the Product

Defense Unicorns chose Tetrate for Istio support because of its deep expertise not only in delivering a secure and reliable runtime, but also in accelerating time to compliance. Says Bryan, “The organizations we work with have to go through a third-party accreditation process to ensure the security of data. The more secure the data must be, the deeper the audits and compliance checks. The process can take six months to a year, or even longer. That’s why we particularly value Tetrate’s work with NIST and the way Tetrate leans into OSCAL. Tetrate is directly involved in working with NIST to establish what good software security practices look like and how to sustain them, and, obviously, those best practices map to Tetrate's services and product features. Tetrate saves downstream users like 100s of man hours in the compliance process, and it's one of the driving factors for why we want Tetrate to be involved in the projects we do for the Department of Defense, the Centers for Medicare and Medicaid Services, and others in the government arena. Tetrate helps us move faster to compliance and reduces the risk of regulatory fines caused by accidental non-compliance."

Benefit: Overcoming Kubernetes Complexity and Improving Developer Collaboration

"The potential to reduce standard lead time for delivering applications and capabilities can go from weeks to days and a matter of minutes with the right automation across every layer", according to Bryan. Additionally, developers and platform teams need to collaborate to enable a centralized workflow for both adopting the cloud and increasing delivery speed." Core to supporting this approach to software development is a strong DevOps foundation that enables developer collaboration and limits the manual work that is required to support developer workflows. The service mesh takes the onus of connectivity and security (especially certificate management) off the shoulders of developers and puts it into a dedicated infra layer that's mostly invisible to developers. For platform teams, the service mesh offers those capabilities and assurances as a product offering to dev teams as their internal customers. With Tetrate, Dev teams can consume connectivity, security and resiliency as - essentially - a cloud service, instead of having to build it themselves.