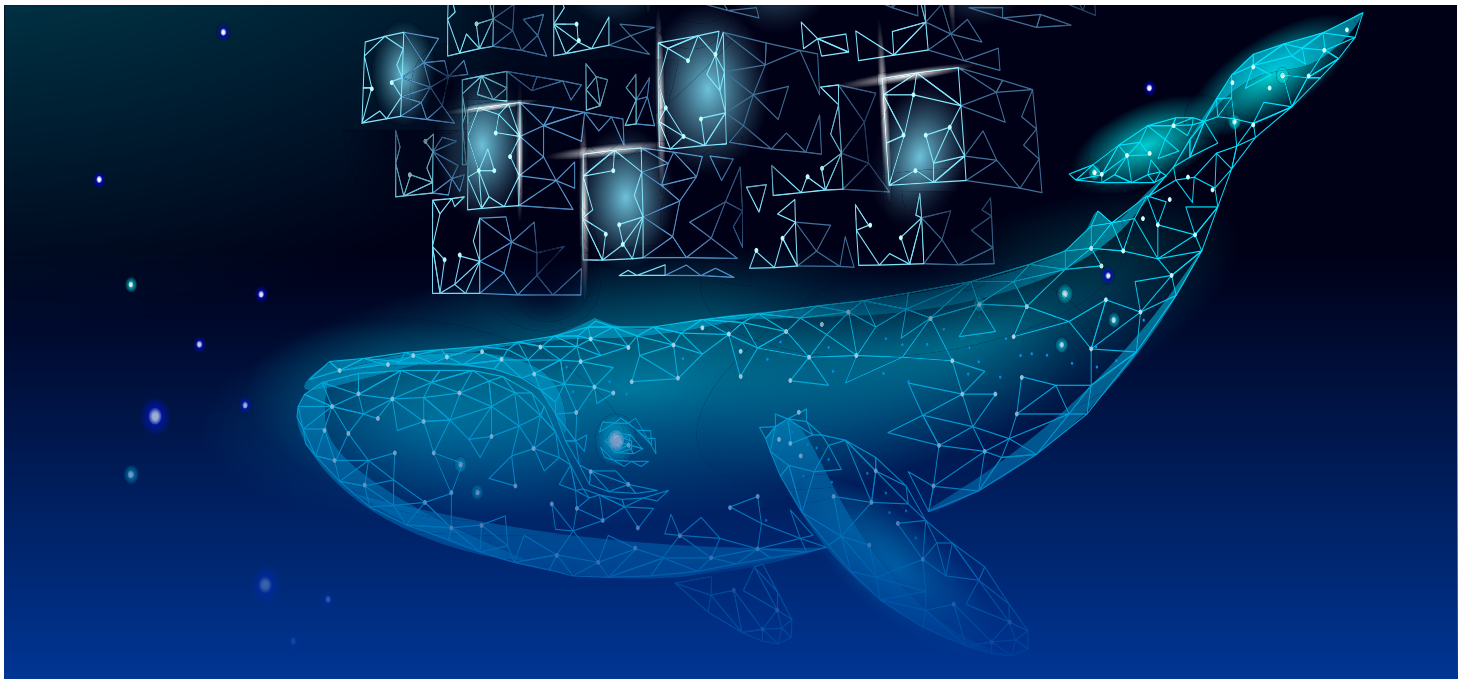
NETFOUNDRY™

Ozone Zitifies Private Kubernetes deployments with NetFoundry

ozone

CASE STUDY



Today, every company is heading towards container and container management tools like Kubernetes as a central part of their digital transformation strategy. Thanks to cloud providers, Kubernetes (K8s) Clusters can be launched in a few minutes, instead of self-installing everything. No doubt this cloud-native infrastructure enables rapid development and deployment of new applications, but there are still the pains of the Day-2 operations.

Day-2 operations demand continuous improvement not just application, but the way in which it operates in production environments. Having a K8s cluster up and running is only half the struggle of Day-2 operations as enterprises will still need to worry about things like integration, DNS, service discovery, or managing permissions and privileges within clusters.

Ozone addresses Day-2 operations concerns by offering a holistic approach to Continuous Delivery-as-a-service. Ozone supports enterprise integrations across any Kubernetes cluster to enable consolidation of application delivery and observability, without any DevOps headaches. Ozone is a Value Stream Delivery Platform (VSDP) solution for enterprises looking to achieve accelerated and standardized application delivery across multiple cloud platforms. Ozone is headquartered in the US, with offices across the globe. The Ozone platform enables enterprises to ship software at lightning speed without compromising quality and governance.

Ozone caters to enterprise customers across the globe, helping them achieve faster product iterations across any cloud platform. Customers can now integrate all existing DevOps tools and automate their application delivery process end-to-end, reducing downtime and driving faster time-to-revenue. Ozone's primary use cases, such as Release Management and Cluster management, reduce operational overheads of getting the code to customers. Beyond the core use cases, Ozone also enhances the security of continuous integration, continuous delivery, and continuous deployment (CI/CD) processes by providing Secret Management out of the box. This equips enterprises with end-to-end visibility over vulnerabilities and weaknesses in builds, allowing them to shift left with the security of their modern applications to reduce business risks.

Security challenges with private Kubernetes clusters

Kubernetes clusters allow containers to run across multiple machines and environments creating an "Immutable infrastructure", enabling enterprises to make sure their work is suitable for large applications - not just microservices. Hence enterprises would likely deploy to any K8s cluster, across a distributed environment, including both public and private clouds.

However, with existing mechanisms, the use case of deployment to private clusters poses a challenge for Ozone as they need to be able to provide:

- Private clusters, with no ability for external network attacks, for security-critical scenarios
- Automation for application delivery onto private clusters across clouds without violation of security compliance requirements

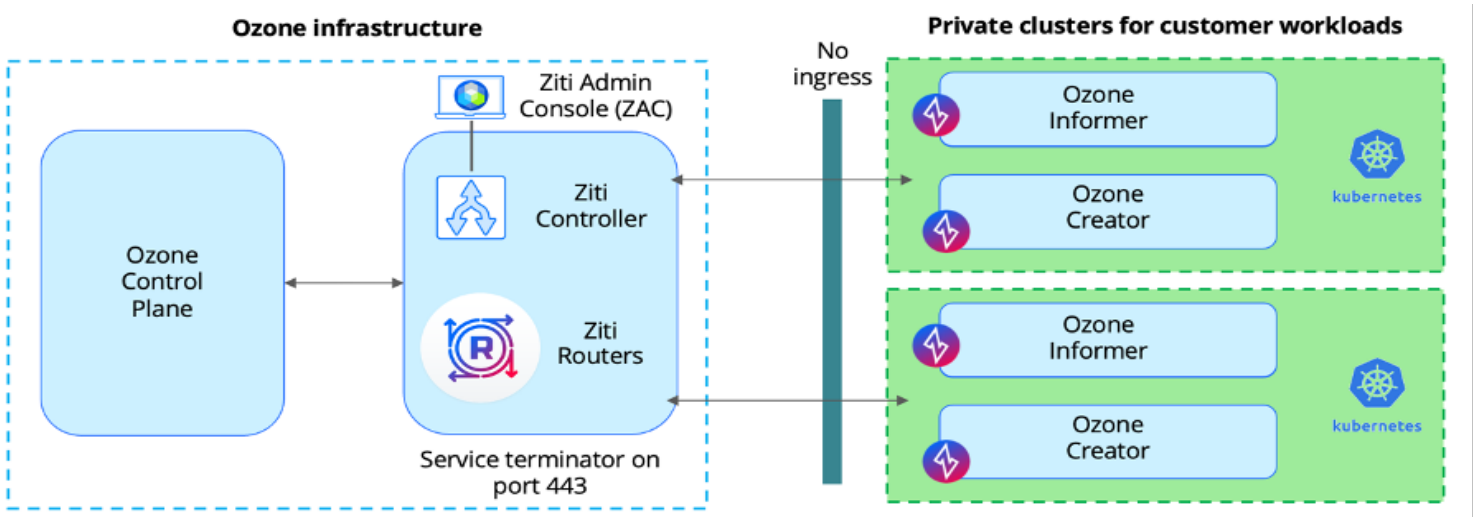
Unlike a public cluster, a private cluster has a control plane private endpoint. The clusters use nodes that do not have external IP addresses and nodes are isolated from inbound and outbound traffic. Hence, the deployment of apps to private clusters, automation and authentication ends up being tricky as there is no publicly exposed endpoint for VSDPs to connect to. Considering the speed and scale of requests that happen in a multi-cloud, microservice oriented environment, there is a need for a solution that can address these challenges, as governance and security can get complicated very quickly.

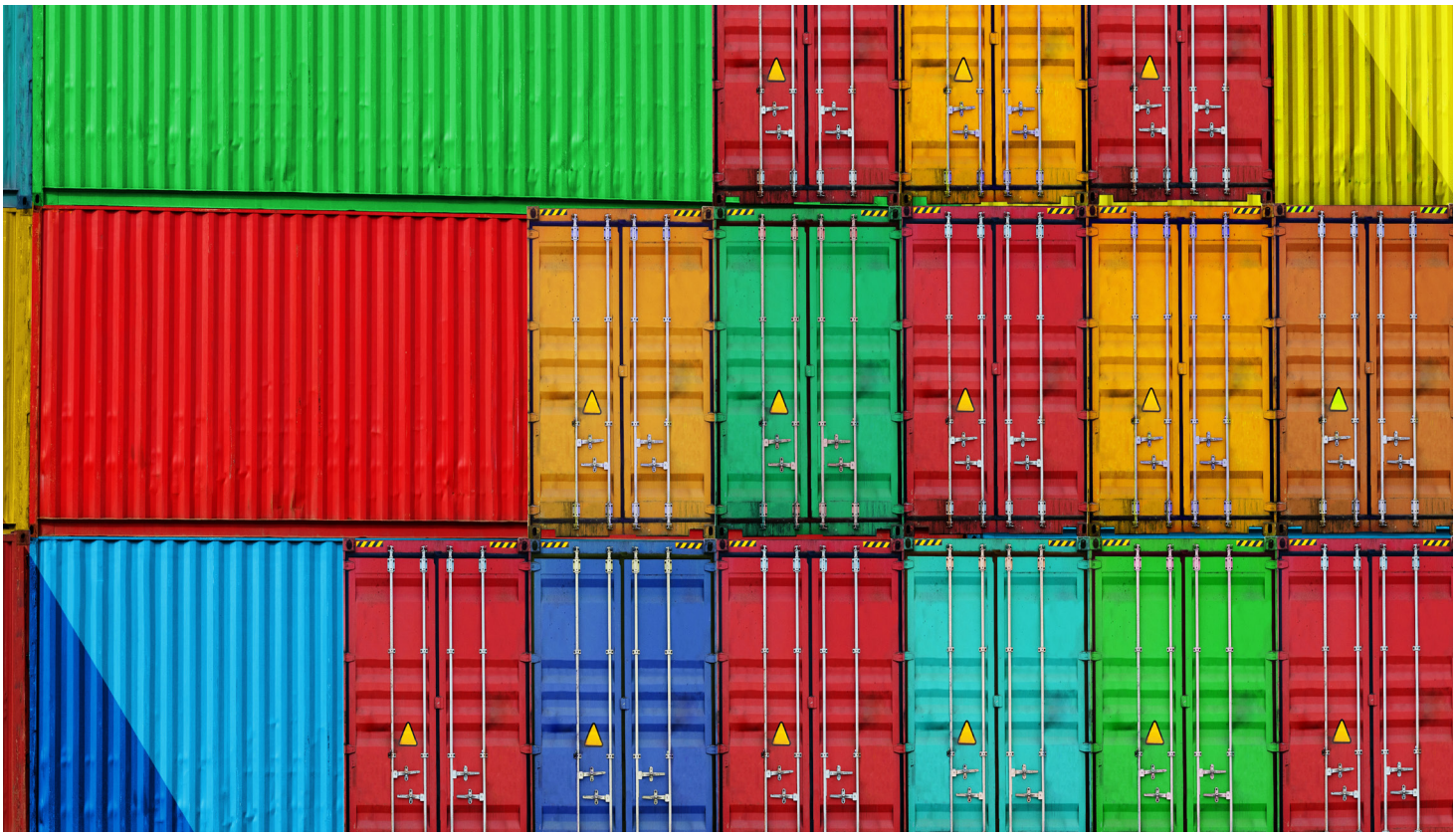
> "Ziti allowed us to innovate and drive new business with a competitive edge. Today, Ozone is the only CI/CD tool that automates private cluster deployments across any platform providing customers with zero trust, secured application delivery for private Kubernetes clusters.", Moteesh Reddy, Technical Lead

Zitifiying Ozone

Ozone was introduced to OpenZiti to overcome these challenges - https://ziti.dev/. Ziti, developed by NetFoundry, is an open-source project and community consisting of a collection of open SDKs and related tooling, that makes it simple to embed private, programmable zero trust networking into applications. With Ziti, there is no need for traditional alternatives like IP allow lists, virtual private networks, and bastion hosts. This also means the cluster can be anywhere, it can reach out to the internet, and the master API server need not be exposed to the public internet. Being a software-powered private network, Ziti allows Ozone to operate security-as-code within a DevOps/GitOps model.

Ozone integrated Ziti SDKs into Ozone agents so that they can communicate from a private network environment with Ozone's control plane through a secure tunnel provided by Ziti without the need for the customer to set up inbound communication. Now Ozone has zero trust, high-performance networking embedded inside it allowing private connectivity that overlays on any Internet connection from anywhere to anywhere, without traditional 'bolted on' networking and security solutions (e.g., VPNs).





Compliant and automated private Kubernetes clusters

The adoption of Ziti provided not only a solution for Ozone but also set them apart from competition. Ozone was able to demonstrate their capabilities to deliver cluster management, secure application delivery and observability across clusters on any cloud platform. Being able to deploy through a private tunnel rather than expecting the cluster to be made publicly available, enterprises were quite excited about the fact that they need not violate security compliance requirements to achieve complete automation for their Kubernetes workload management

Zitifying Ozone and Kubernetes deployments helped:

- Improve service delivery as customers can now automate application delivery to private clusters on any cloud platform.
- Reduce security risk as apps are deployed without making the clusters publicly available; no inbound communication or public IPs is needed, making external network attacks impossible
- Reduce cost by 50% as automation removes deployment complexities, reduces the need to re-invent processes and reduces overheads

Ozone's customers can now have automated and secure access to private K8s clusters, removing developers' painful process involving cluster certificates, access management systems, complex identity management, networking setup and firewalls.

ABOUT NETFOUNDRY

NetFoundry is the leader in Cloud-Native Networking, enabling businesses to simply, securely and cost-effectively connect distributed applications across edges, clouds and service meshes. The NetFoundry platform, delivered as SaaS, enables businesses to connect applications without the costs and complexity of VPNs, custom hardware and private circuits.

NetFoundry's platform is accessed via APIs, SDKs and DevOps tools integrations, enabling practitioners, application developers, and network administrators to get the levels of automation and agility which are only possible with connectivity-as-code. NetFoundry is headquartered in Charlotte, North Carolina, with offices in California, Colorado, New York, London, Bangalore, and Singapore.

Contact us

Share

For more information, visit us at www.netfoundry.io

NETFOUNDRY™

Address —
101 South Tryon Street, Suite 2700
Charlotte, NC 28280

Telephone —
+1.704.762.1405

Contact us

Share

For more information, visit us at www.netfoundry.io