Deploying Applications with Security, Control, and Simplicity

Tigera Secure: Policy-driven Secure Application Connectivity for OpenShift

OpenShift provides a declarative, automated platform to integrate developer workflows into application deployments leveraging open source building blocks such as Kubernetes.

As deployments move to production, organizations struggle with the inability to integrate their legacy application infrastructure with the dynamic orchestration of OpenShift and Kubernetes. Tigera Secure helps overcome those challenges, enabling organizations to deploy OpenShift-based applications with declarative and automated security, compliance and control across private and public clouds.

TIGERA

Table of Contents

Security and Connectivity Challenges in OpenShift

The migration to microservices-based applications deployed within an OpenShift Platform-as-a-Service (PaaS) environment poses challenges to several parts of an organization.

- **Developers and DevOps** need secure application connectivity and microsegmentation between the containerized portions of the application stack. That includes services that run in OpenShift as well as to services and data platforms that run on VMs, cloud instances and bare metal hosts.
- **Cloud Architects** need to design for seamless migrations of workloads between on-premises deployments and public clouds. They also need infrastructure oversight and policy control over hybrid and multi-cloud deployments.
- **Lines of Business** must meet regulatory compliance, governance, application agility and other needs required for business operations.

- **InfoSec teams and CISO's** struggle to enforce security monitoring and control over infrastructure, networks, and applications that span on-premises and cloud environments. Orchestrated environments like Kubernetes amplify this challenge because instances and artifacts like IP addresses are dynamic and transient.
- **Operations and Site Reliability Engineering (SRE)** teams are tasked with continuous and automated management, monitoring and alerting for applications that are dynamic, transient, and potentially span hybrid or multi-cloud deployments.
- **Public Cloud Providers and Internal Service Providers** need to provide individual tenants with fine-grained security controls while still asserting broader controls over each tenant as well as isolation between tenants.

Each of these roles typically has an interest in OpenShift application deployments. However, their goals generally are not congruent. Friction between teams and functions hinders the adoption of new platforms like OpenShift and Kubernetes despite the available benefits.

Tigera Secure delivers policy-driven security and application connectivity. Tigera Secure was built to enable organizational alignment and is operationally simple and secure for both multi-cloud and legacy applications.

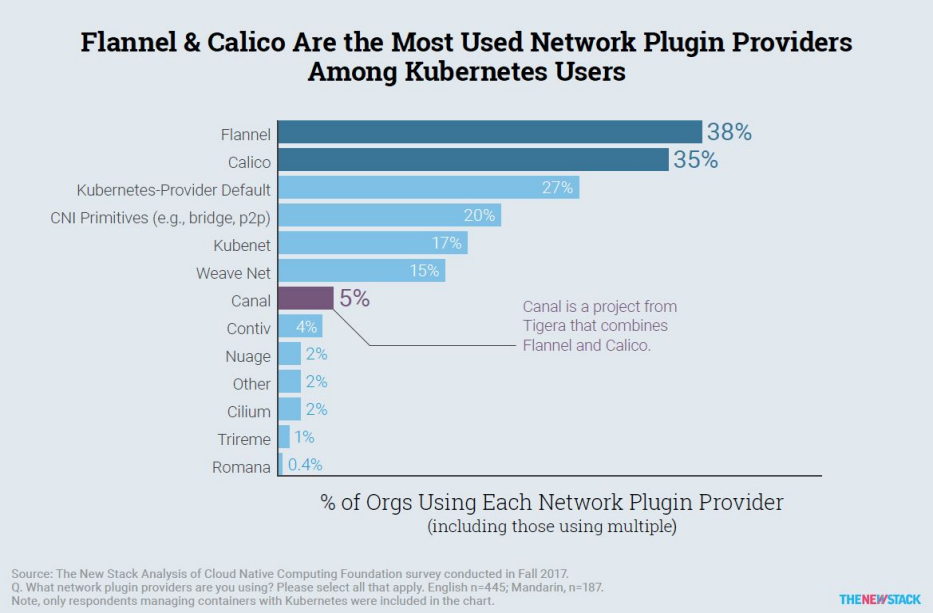
Tigera Secure: Seamless, Scalable, Secure Application Connectivity

Tigera Secure provides policy-driven security and micro-segmentation along with non-overlay IP connectivity between applications in OpenShift. Tigera Secure also supports virtual machines (VMs) and host instances both on-premises and in the cloud. Furthermore, Tigera Secure can be

used for policy-driven dynamic security for the OpenShift nodes themselves, as well as services exposed on the node such as Kubernetes nodePorts.

This holistic approach provides a consistent policy implementation between OpenShift and the hosted public Kubernetes service offerings from the major public cloud providers.

Another key capability of secure application connectivity is the ability to control, analyze, and cryptographically secure application layer connections. Tigera is an active participant in the Istio and Envoy communities, and the Tigera Secure solution builds on the capabilities of those projects.



Policy as Code

Tigera Secure utilizes the concept of “policy as code.” In practice, policy as code is enabled by two capabilities:

1. **Declarative Policy Language** - Policies are defined using a high-level, declarative language that is easy to understand. They define which workloads the policy applies to based on metadata that is resident in the platform, rather than network arcana such as VXLAN segments or IP addresses, and a clear definition of what is allowed or denied. A pseudo-code example of this might be the following: *Anything with the label LDAP_CLIENT is allowed to connect to anything with the label LDAP_SERVER.*
2. **Policy Versioning and CI/CD Pipeline** - While a policy can be created using either a text editor or the Tigera Secure Manager GUI, the policy artifact can be treated as an immutable fragment of code. The policy can be checked into your version control system and automatically feed into your CI/CD pipeline. As the policy refers to objects using metadata rather than specific instance data such as IP address, it is possible to apply a set of policy objects and continuously achieve the same policy state in your infrastructure.

The policy as code approach offers many benefits. Your infrastructure can revert to a known state by simply deploying the same set of policy artifacts, just as you would for any application in your OpenShift environment. OpenShift provides a declarative environment for your applications, and policy as code enables you to bring your application connectivity environment inside and outside of Openshift into alignment with your automated OpenShift operational model.

If you are running your OpenShift environment in a public cloud, such as AWS, you already have a declarative infrastructure. In this case, Tigera Secure enables you to have a completely automated, declarative environment, spanning from your infrastructure all the way up the stack to your services and applications.

Development Phase

Developers and DevOps teams can easily connect applications in OpenShift to other workloads within OpenShift as well as to services and databases elsewhere. This includes VMs and cloud instances, all using simple, highly performant, non-overlay IP networking. Secure leverages the Calico network policy engine to provide a superset of Kubernetes network policy. This delivers additional flexibility and syntax options for developers to encapsulate application and network policy rules. It also adds additional developer tools and features to aid in automated development and troubleshooting of Policy.

- **Non-overlay IP Connectivity** - Tigera Secure enables easy, non-overlay IP connectivity between applications built and deployed in OpenShift with applications and services that reside outside OpenShift, including on bare metal hosts, VMs, other orchestrators like OpenStack, as well as on major public cloud platforms.
- **Operational Flexibility with "Log-and-Drop" Override** - Development of Network Policy for secure application connectivity is facilitated by the use of the Tigera Secure "Log-and-Allow" Drop Action Override. Using an approach resembling the SELinux Permissive mode, this allows network policy to be applied but not enforced while simultaneously enabling the development and tuning of network policy for the application.

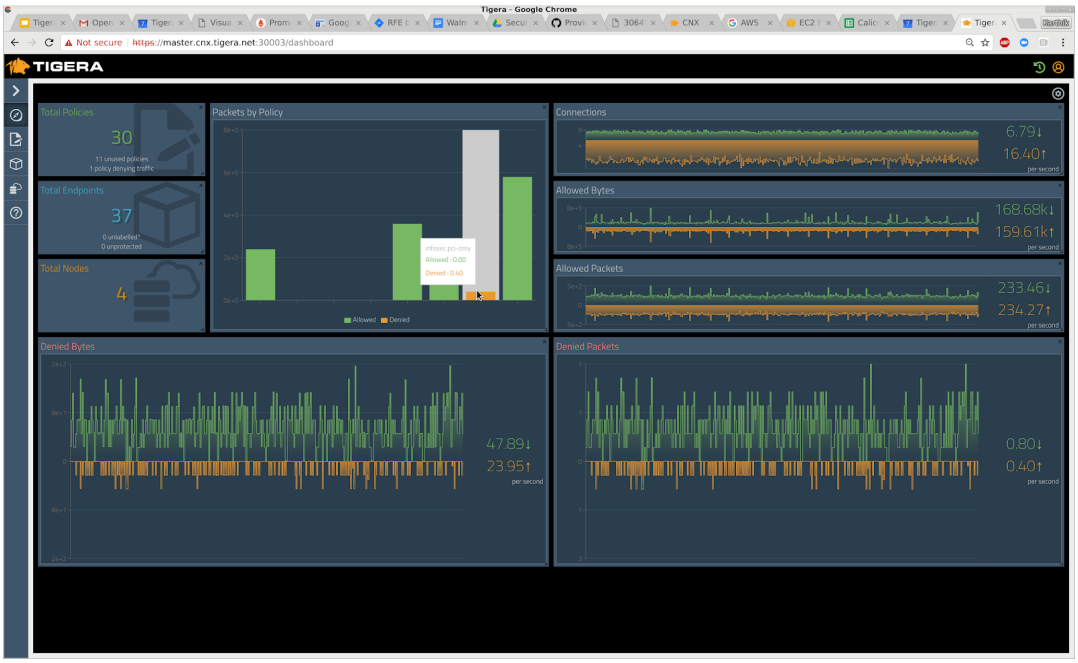
Deployment Phase

Cloud Architects benefit from a consistent network policy implementation across on-premises and cloud-based OpenShift deployments. This covers host instances including VMs, cloud instances

and bare metal hosts, along with the hosted Kubernetes services from major public cloud providers.

- **Network Policy for Hosted Kubernetes from Cloud Providers** - Amazon EKS, Microsoft AKS Engine, Google GKE, and IBM Cloud integrate Calico's Network Policy implementation with their hosted Kubernetes offerings and recommend it to their customers. OpenShift deployments with Tigera Secure provide cloud architects with a consistent Network Policy implementation across these providers.
- **Simple Deployment** - deploying Tigera Secure with OpenShift is simple, and only requires eight lines of configuration options specified within the standard openshift-ansible installation host inventory file.
- **Integration with OpenShift** - Tigera Secure integrates seamlessly with OpenShift user authentication and Role-based Access Control (RBAC) authorization via OpenShift's API aggregation so that users and roles defined in OpenShift can be seamlessly extended to Tigera Secure functions accessible in the Tigera Secure Manager.

Operations Phase



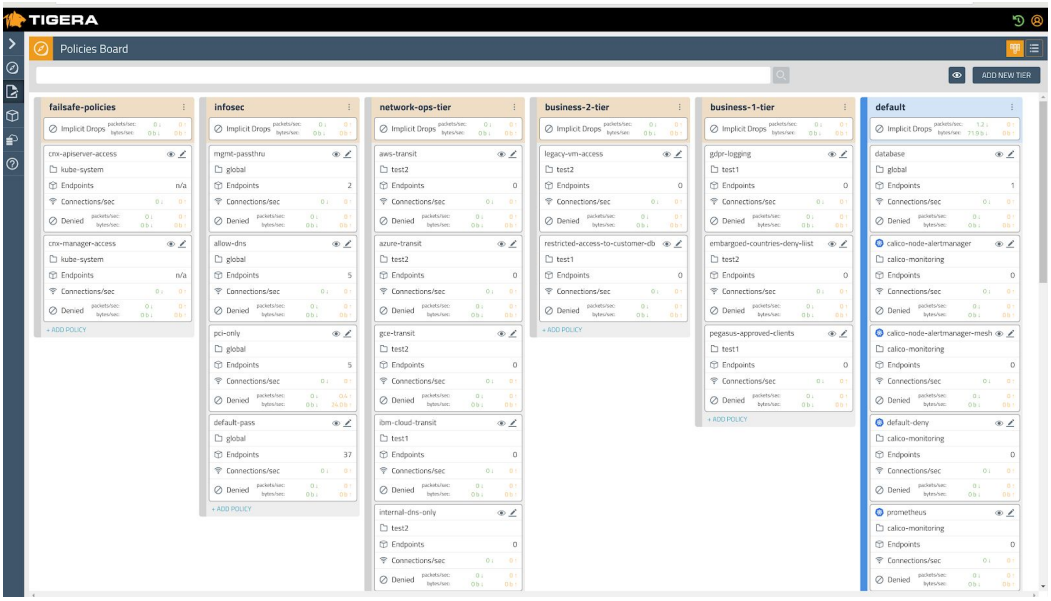
Operations and site reliability engineering (SRE) teams can automate management and monitoring of applications on OpenShift using label-based policy control and monitoring of dynamic and transient containerized deployments. Troubleshooting complexity is easy with Calico's simple, non-overlay IP connectivity. Calico's Layer 3 networking approach also provides scalability to massive cluster sizes while using generally accepted networking practices used across the Internet.

- **Monitors Application Flows** - Higher precedence Pass Policy Tiers can dynamically instrument and monitor application flows between OpenShift workloads and services/endpoints on VMs, cloud/host instances and external IP address ranges (CIDRs).
    - For example, to monitor all customer A's traffic between an application and a database, an SRE creates a higher precedence policy to Pass traffic from (application: *AppServer* && tenant: *CustomerA*) to (application: *Database*

&& tenant: *CustomerA*). This rule defers to other lower precedence rules to determine network policy, while simultaneously providing statistics on customer A application->database flows independent of IP addresses, the number of OpenShift pods, and agnostic to if these workloads run within OpenShift or VM/cloud instances outside.

- **Monitors and Alerts on Policy Violation** - Tigera Secure enables operations and security teams to automate management and runtime monitoring of applications and security through tools like Prometheus, with configurable thresholds and alerting to common Alerting systems such as Alertmanager.
- **Operational Flexibility with "Log-and-Drop" Override** - policy as code complements monitoring and alerting with the Tigera Secure Log-and-Drop Drop Action Override. This transparently and immediately logs and captures packet 5-tuple headers, correlated by policy, from data streams attempting to violate policy.
- **Avoids Layer 2 Bridges & VSwitches** - Tigera Secure, leveraging Calico, avoids the use of Layer 2 networking bridges and vswitches and is biased towards a simple and highly scalable IP-routed non-overlay network. This approach enables simple troubleshooting in production at scale. SRE and Operations teams benefit from the use of knowledge, skills, and tooling already in common use across the Internet.

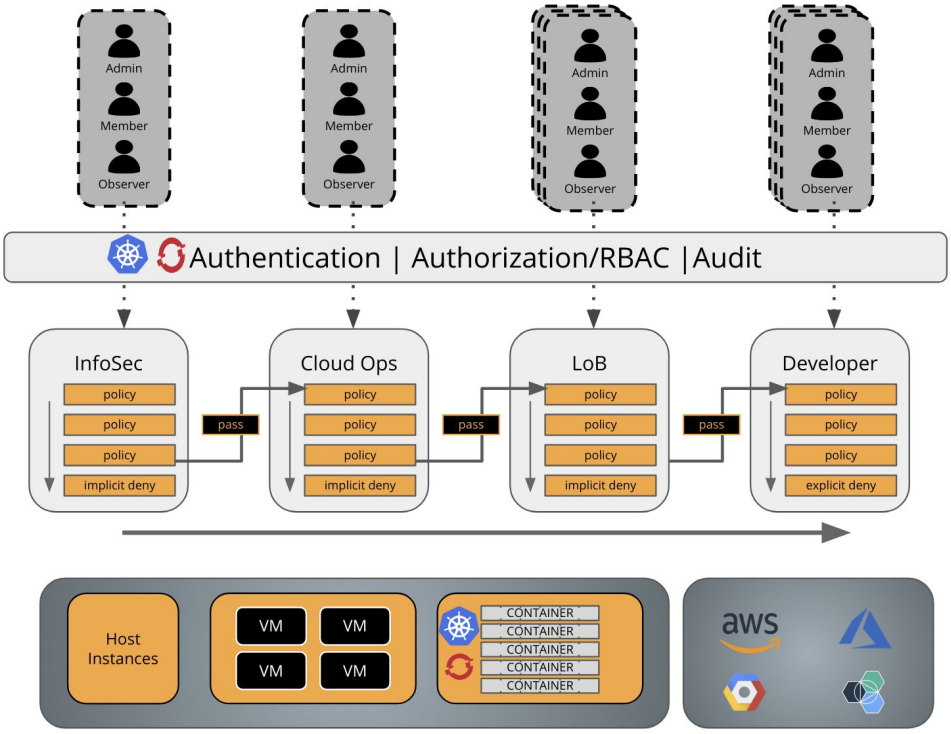
Hierarchical Organizational Controls and Regulatory Compliance



Maintaining control and meeting compliance requirements is a requirement for most production deployments. Lines of Business and IT organizations can dynamically apply higher precedence policy to application connectivity as required for enterprise business reasons as well as for regulatory or geographical compliance reasons.

- **Hierarchical Policy Tiers** - Tigera Secure policy tiers enable Line of Business and enterprise organizations to superimpose higher precedence policy over application connectivity and security. These “tiers” can be aligned to organizational hierarchy, enabling DevOps or security rules to provide runtime overrides to developer or other lower priority policies.
- **Compliance and Control through Policy-driven Connectivity** - Policy tiers provide runtime controls that enforce policy-guided connectivity and security rules mandated by regulatory compliance and operations.

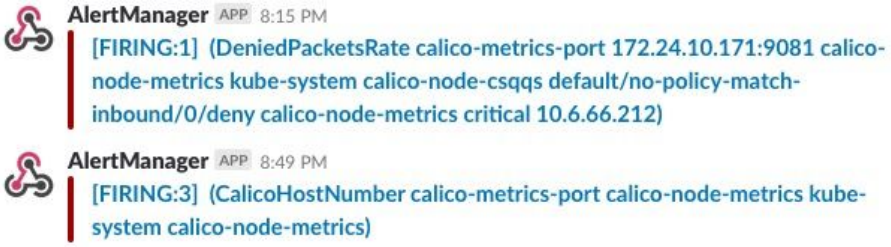
- **Integration with OpenShift Authentication & RBAC Authorization** - Tigera Secure integrates seamlessly with OpenShift user authentication and RBAC-based authorization using OpenShift's API aggregation. This enables users and roles defined in OpenShift to be extended to Tigera Secure functions, including the Tigera Secure Manager.



Security Controls and Monitoring

Security teams frequently need to change the existing policies to respond to new threats. For example, new threat intelligence could require blacklisting certain IP addresses. Tigera Secure enables security organizations to migrate from current, slow-moving manual security review and audit processes to continuous, automated, policy-as-code.

- **Hierarchical Policy Tiers** - Tigera Secure Policy Tiers enable automated, higher-precedence security controls that have been codified and are continuously enforced on application deployments at a higher precedence developer-defined rules.
- **Label-based Policy Enforcement** - Dynamic label-based policy enforcement with flexible syntax options frees DevSecOps from having to worry about how to deal with transient artifacts such as IP addresses, both within containerized OpenShift deployments as well as on VMs and host/cloud instances outside OpenShift.
- **Policy Violation Attempt Monitoring and Alerting** - Tigera Secure policy violation attempt monitoring and alerting enables operations and security teams to automate the management and runtime monitoring of applications and security through tools like Prometheus, with configurable thresholds and alerting to common Alerting systems such as Alertmanager.
- **Flexible Operations with "Log and Drop" Action Override** - Policy violation monitoring can be complemented by the automated addition of Tigera Secure "Log-and-Drop" Drop Action Override. This function transparently and immediately logs and captures packet 5-tuple headers, correlated by policy, from data streams attempting to violate policy.
- **Visibility Tied to OpenShift Authentication and RBAC** - The Tigera Secure Manager provides dynamic visibility and is tied to OpenShift user authentication and RBAC authorization.



Summary

Tigera Secure addresses the security and application connectivity challenges faced by organizations migrating to Kubernetes and OpenShift. Tigera Secure contributes critical capabilities to help various stakeholders for the successful adoption of OpenShift within the enterprise and enables these roles to migrate from manual, slow-moving processes to automated, continuous policy-as-code. This increases the agility of application deployments while providing dynamic security and micro-segmentation.

About Tigera

Tigera delivers solutions for secure application connectivity for the cloud-native world. Tigera technology is used by the world's largest enterprises and public cloud providers to power connectivity for application development and deployment and to address the connectivity and security challenges that arise in at-scale production. Tigera Secure meets enterprise needs for zero trust network security, multi-cloud and legacy environment support, organizational control and compliance, and operational simplicity. Tigera Secure builds on leading open source projects Kubernetes, Calico, and Istio, which Tigera engineers help maintain and contribute to as active members of the cloud-native community.

tigera.io

email: contact@tigera.io

phone: +1.415.612.9546

Tigera, Inc. 58 Maiden Lane, Fifth Floor, San Francisco CA 94018 USA