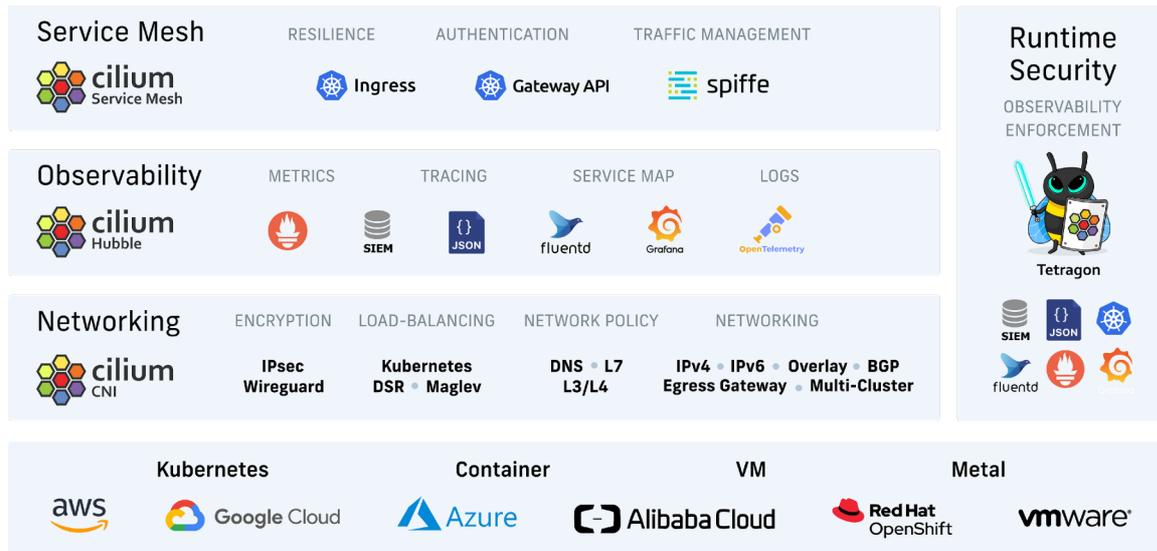


Supercharge OpenShift with Isovalent Cilium Enterprise

Secure & scalable connectivity for open hybrid cloud with eBPF superpowers



Enterprises are often faced with difficult trade-offs between optimizing for a truly cloud-native platform and achieving traditional enterprise goals like security and compliance, as most legacy tooling struggle to keep pace. They fail to understand cloud native identities, struggle to work with changing setups and cannot provide meaningful insight into container operations.

Isovalent Cilium Enterprise removes many of the hassles, provides a single comprehensive data plane that combines three key functions of cloud-native networking: connect, observe & secure.

Let's understand more on how Isovalent Cilium Enterprise can bring additional value to Red Hat OpenShift by providing secure and scalable connectivity for the open hybrid cloud.

Challenges for organizations moving to the cloud native world

- Container world is new and difficult.
- Not enough support for multi-cloud, scale or developer's needs.
- Lack of deep visibility & controls for SecOps teams
- Increased cost & overhead with legacy tooling
- Centralized bottlenecks in scaling
- Missing Operational capabilities
- Missing Cloud native dataplane solution
- Providing Ops teams secure and scalable connectivity

What is Isovalent Cilium Enterprise

Isovalent is the company founded by the creators of Cilium and eBPF. Isovalent Cilium Enterprise is a supported, tested and hardened Kubernetes data plane for enterprise users. It provides cloud native insights and control independent of legacy approaches. Isovalent Cilium Enterprise provides eBPF-based networking, observability, and security to platform teams operating Kubernetes environments across clouds, clusters and premises. Isovalent Cilium Enterprise is backed by multiple public cloud vendors, like AWS, Google and Alibaba.

Isovalent Cilium Enterprise is built on eBPF, the new standard to program Linux kernel capabilities in a safe and efficient manner. It has revolutionized cloud native tooling covering networking, security, and observability use cases. Cilium is available as a certified operator via the Red Hat Ecosystem Catalog.

How to supercharge OpenShift with Cilium

Secure Connectivity

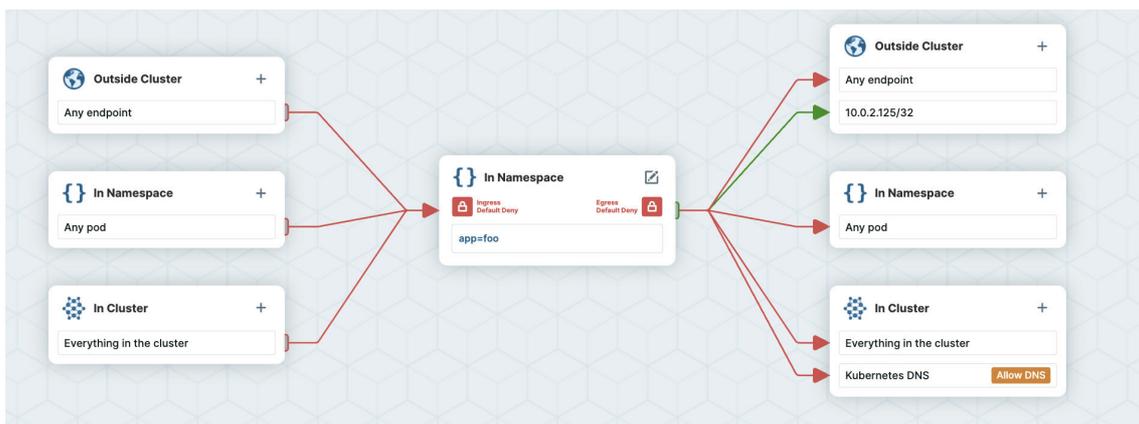
Thanks to Isovalent Cilium Enterprise, OpenShift can be integrated into traditional environments on both ends, north/south and east/west. When combining multiple OpenShift clusters, Cilium Cluster Mesh provides pod routing and service discovery across clusters and with other Kubernetes-based platforms, becoming a unified data plane for all cloud native workloads. This also works across different cloud vendors, connecting different OpenShift clusters independently of where they are hosted.

This flexibility is also the reason cloud providers choose Cilium as a key component of the cloud native networking offering:

- [AWS picks Cilium for Networking & Security on EKS Anywhere](#)
- [Google announces Cilium & eBPF as the new data plane for GKE](#)
- [Alibaba Cloud uses Cilium for High-Performance Cloud-Native Networking.](#)

Instead of IPs Cilium uses labels as identifiers, enabling cloud native policies to micro-segment services and tenants. When legacy services protected by traditional firewalls need to be connected to Cilium, static egress gateway IPs allow Kubernetes nodes to act as gateways for cluster-egress traffic, always contacting the external service via the same IP. This removes the need for

- Zero trust Network Policy
- Cluster Mesh
- Advanced Network Policy
- Compliance Monitoring
- On-prem/legacy Integration
- Sidecar-free Service Mesh



Embedded Policy Editor

more complex solutions like routing traffic customized solutions. It also greatly simplifies the management of the traditional firewall policies. Additionally, Cilium can also be installed on traditional VMs or bare-metal servers that are connected to OpenShift. This allows the VMs or bare-metal servers to join the Cilium cluster, allowing OpenShift platform teams to apply label-based policies on the traffic between application pods and external nodes. The external nodes, on the other hand, will get access to cluster services and can resolve cluster names. As the use cases grow, Cilium also offers advanced networking capabilities like SRv6, BGP support and NAT46. Cilium has also integrated, sidecar-less service mesh capabilities, enabling platform teams to take advantage of service mesh approaches without the need for large performance impacts or complex architectural changes.

Operational and Application Observability

In leveraging eBPF, Cilium provides network visibility to application developers running workloads on OpenShift, including flow traffic details between the pods displayed in the service graph or available in the CLI. Additionally, Cilium collects extensive metrics for developers to monitor TCP, UDP and HTTP golden signals like HTTP return codes, latency, requests per second, and used TLS ciphers.

These data can be exported to open telemetry. Since cloud native is all about APIs, developers running their apps on OpenShift can take advantage of API visibility: Cilium has insight into L7 traffic, making it possible to track the API endpoints being used and the ones that are not reachable. Leveraging Cilium Network Policy you can also define access to these L7 services by path or verb. Everything you can observe you can also enforce - without any sidecars or proxies, and across all clusters.

This is complemented by eBPF's unique security runtime visibility: Cilium provides OpenShift platform teams with a single source of data for cloud native forensics, threat detection and compliance monitoring. It provides the deep security visibility needed to predict breaches, hunt threats, investigate

-  Application Monitoring
-  Sidecar-free Tracing
-  Golden Signals
-  Runtime Visibility
-  API/endpoint Visibility
-  Metric History



Metrics and Monitoring

possible attacks, follow lateral movement, and audit the environment's security compliance.

Cilium's observability capabilities are backed by role-based access controls (RBAC), enabling OpenShift platform teams to give their app developers self-service access to the relevant observability data.

What is Red Hat OpenShift

Red Hat OpenShift is an Enterprise Kubernetes container platform that helps rapidly build and deploy cloud native applications. It offers rich self-service capabilities for application developers and a stable platform underneath, supporting Kubernetes operators in on-premise and public cloud deployments.

Find out more about Red Hat OpenShift.

Operational and Application Observability

Isovalent Cilium Enterprise offers DNS and L7 transparency, can export data to SIEM, and has a UI to modify network policies intuitively. This allows for fine-grained policies based on the namespaces and labels of the workloads, providing easy enforcement of micro segmentation to ensure zero trust.

To better manage and secure traffic, Cilium also offers FQDN-aware policies. Operators and app developers can restrict communication with external services based on the domain names. Cilium's L7 transparency provides an even finer-grained control. With insights into the specific aspects of a URL that a service is talking to, Cilium enables security operators to investigate the API endpoints that are contacted.

Cilium provides transparent encryption based on IPsec or Wireguard that encrypts traffic between nodes and between clusters, thereby securing hybrid cloud workloads.



SIEM Integration



Transparent Encryption



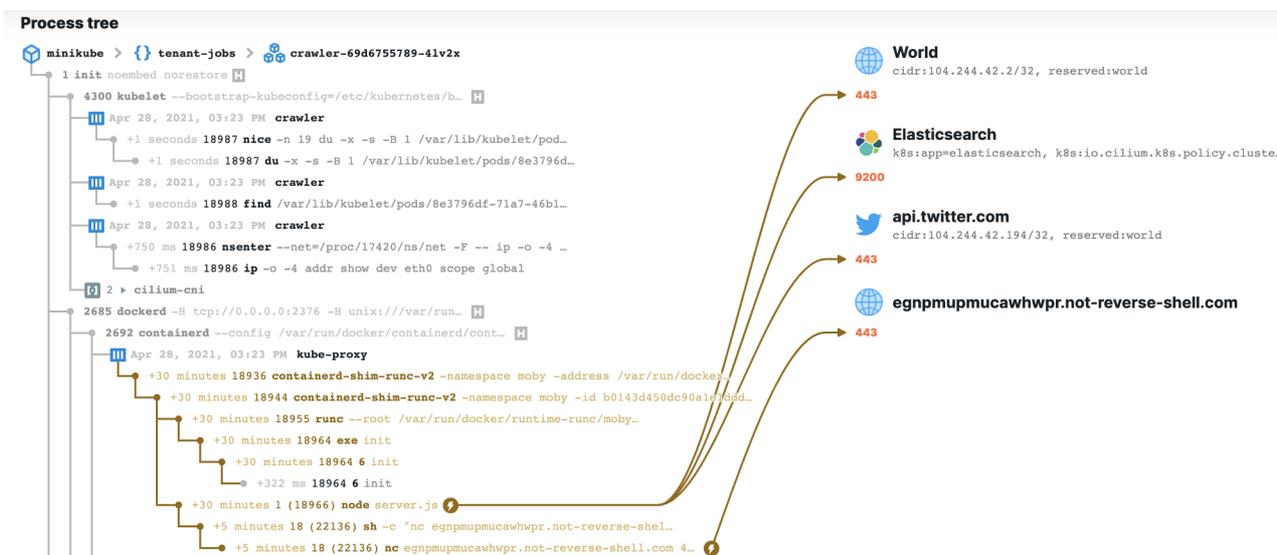
Micro-segmentation



FQDN-aware Policies



Runtime Protection



Process Tree with combined network and runtime visibility for faster investigation

Conclusion

Isovalent Cilium Enterprise brings advanced operations to OpenShift, providing secure and scalable connectivity to platform teams and enabling observability from OS to application level. It enables developers to get a deeper insight into their applications behavior, enables them to track metrics critical for their services and secure and trace their applications.

Learn more about how Isovalent can help building a networking and security layer that provides cloud native visibility, security, and control, and reach out to schedule a demo with a technical expert.

About Isovalent

Isovalent is the company founded by the creators of Cilium and eBPF. Isovalent builds open-source software and enterprise solutions solving networking, security, and observability needs for modern cloud native infrastructure. The flagship technology Cilium is the choice of leading global organizations including Adobe, AWS, Capital One, Datadog, GitLab, Google, and many more. Isovalent is headquartered in Mountain View, CA and is backed by Andreessen Horowitz, Google and Cisco Investments. To learn more, visit isovalent.com or follow [@isovalent](https://twitter.com/isovalent).