ISOVALENT

cilium

Cilium Enterprise - Security Compliance & Forensics

Leverage the power of eBPF to secure your Kubernetes platform

Executive Summary

Cilium Enterprise leverages eBPF, the powerful new Linux kernel technology, to build high-performance, cloud native-aware networking, observability, and security. Going well beyond what is possible with traditional Linux networking like iptables, Cilium Enterprise enables zero-trust network security via powerful Kubernetes-identity and DNS aware network policies. Cilium Enterprise provides tooling to simplify and automate the creation of Network Policy, and allows security teams to delegate this responsibility to the application team while still providing high-level guidelines on what policies are or are not acceptable in terms of security compliance.

For SecOps teams to sign-off and allow critical workloads to run in a Kubernetes environment, they require the tools to perform efficient incident investigations and monitor all key compliance requirements. While the ephemeral nature of IP addresses in Kubernetes thwarts traditional tools, Cilium Enterprise efficiently monitors the precise Linux process and command, container, and Kubernetes pod identity for each connection. Cilium Enterprise exports this data to a SecOps team's existing SIEM, providing all the visibility needed to identify potential breaches, investigate attacks and lateral movement, and audit the environment for security compliance. Cilium's transparent encryption capabilities automatically encrypts communications between all workloads within, or between, Kubernetes clusters.

Cilium Enterprise includes a hardened distribution of Cilium, adds advanced observability and security workflows, and comes with 24/7 enterprise-grade support.

Cilium Enterprise Security Capabilities

Zero-trust Network Policy

Compliance requirements dictate network isolation between tenant workloads within a cluster and restricted access to external workloads, but traditional IP-based firewalls cannot implement such restrictions.

Cilium's eBPF-powered datapath natively understands cloud native identity, implementing not only basic Kubernetes Network Policy (e.g. Label + CIDR matching) but also supports DNS-aware network policies (e.g. allow to *.google.com), which dramatically simplifies defining zero-trust policies for accessing services outside of the Kubernetes cluster.

Additionally, Cilium supports L7 policies (e.g. allow HTTP GET /foo) for fine-grained access control to shared API services running common cloud native protocols like HTTP, gRPC, Kafka, etc.

Cilium also supports deny-based network policies, cluster-wide network policy, and host-layer firewalling.

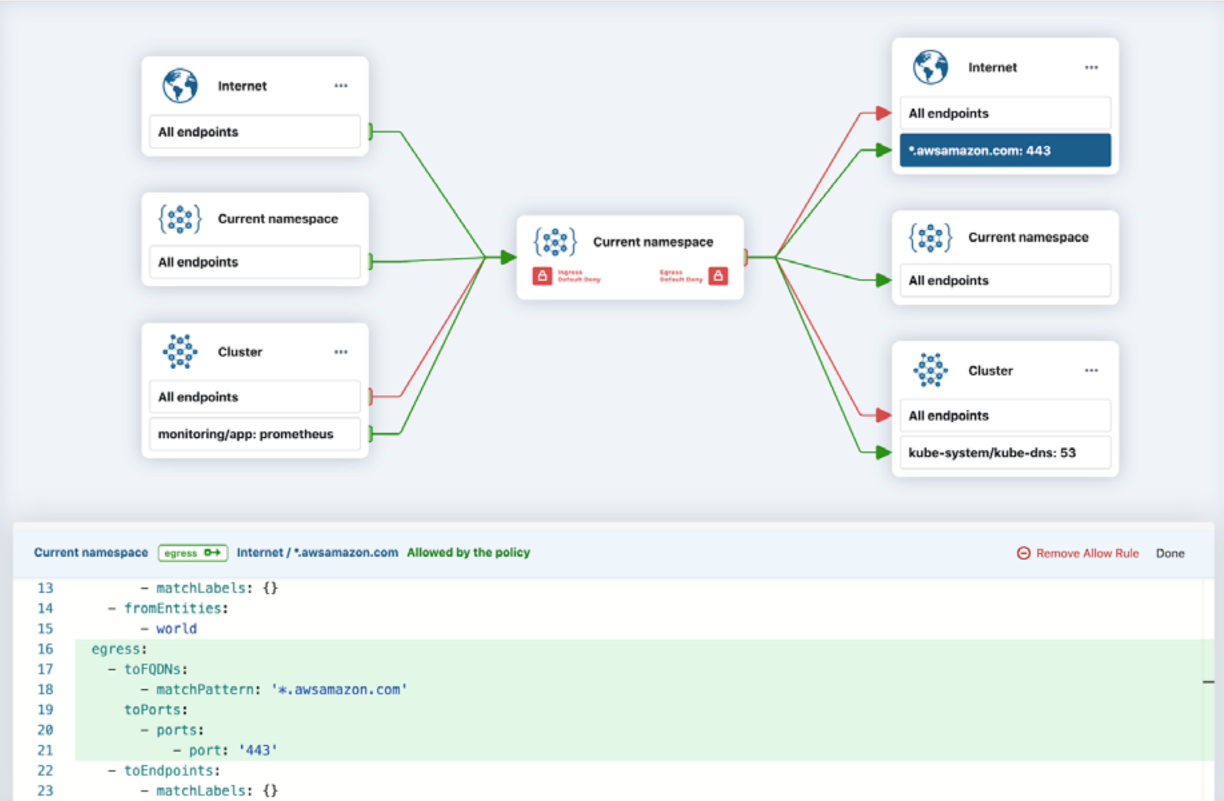
> *Cilium gives us isolation of tenants on our multi-tenant clusters. Thank you Cilium team.*

Brandon Cook
Sr. Platform Engineer
Adobe

Simplified Network Policy Creation

Achieving zero-trust network connectivity via Kubernetes Network Policy is complex as modern applications have many service dependencies (downstream APIs, databases, authentication services, etc.). With the “default deny” model, a missed dependency leads to a broken application. Moreover, the YAML syntax of Network Policy is often difficult for newcomers to understand. This makes writing policies and understanding their expected behavior (once deployed) challenging.

Cilium Enterprise provides tooling to simplify and automate the creation of Network Policy based on labels and DNS-aware data from Cilium Hubble. APIs enable integration into CI/CD workflows while visualizations help teams understand the expected behavior of a given policy. Collectively, these capabilities dramatically reduce the barrier to entry to creating Network Policies and the ongoing overhead of maintaining them as applications evolve.

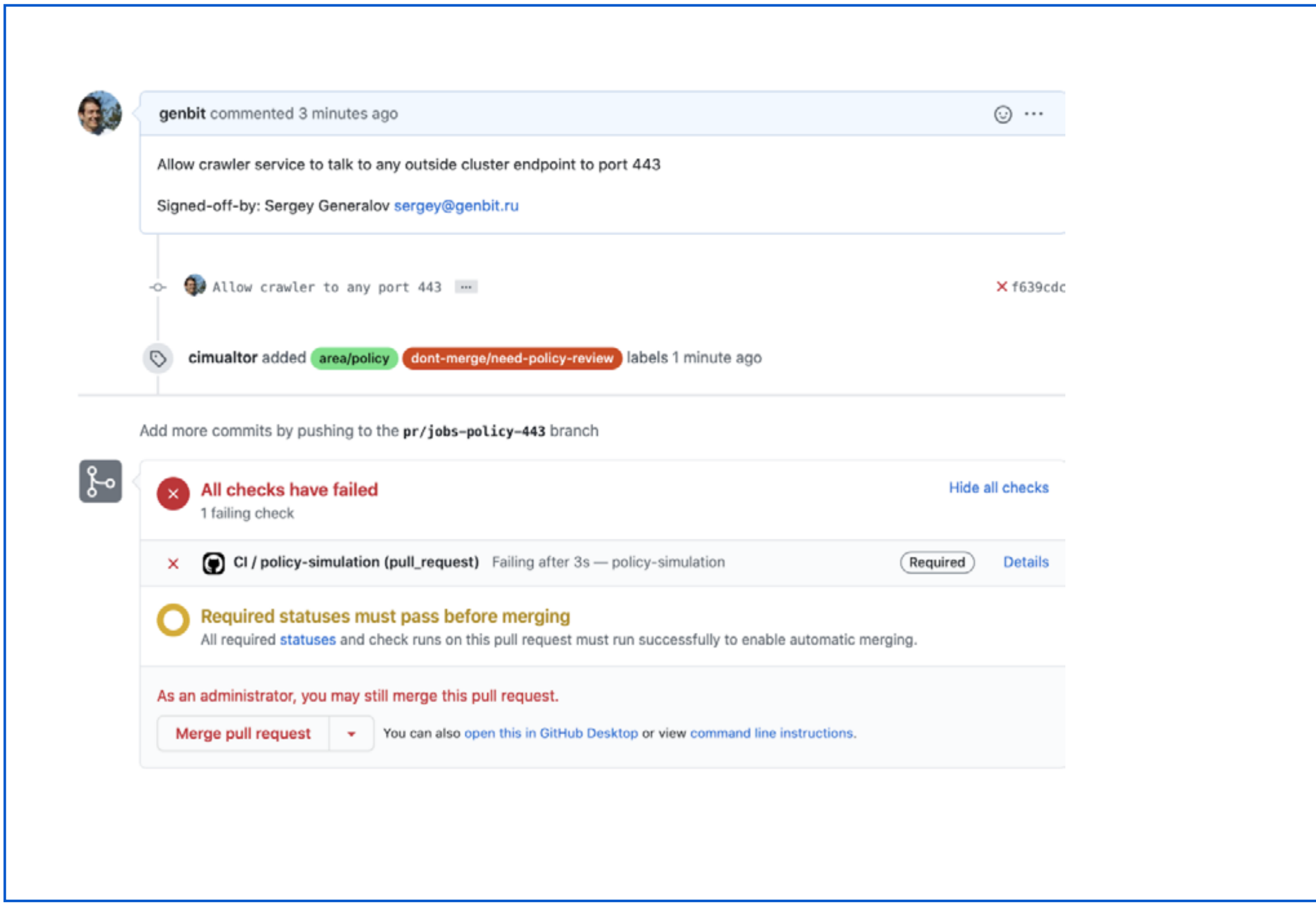


```
        - matchLabels: {}
    - fromEntities:
        - world
  egress:
    - toFQDNs:
        - matchPattern: '*.awsamazon.com'
      toPorts:
        - ports:
            - port: '443'
    - toEndpoints:
        - matchLabels: {}
```

Automated Network Policy Approvals

Because each application has a unique set of service dependencies that must be identified to create a Network Policy, security teams often delegate the ownership of network policy creation to application teams who are in the best position to service dependencies and how they evolve.

Cilium Enterprise allows security teams to delegate this responsibility to the application team while still providing high-level guidelines on what policies are or are not acceptable in terms of security compliance. Security teams can specify high-level properties (e.g., no applications can have unrestricted access to the Internet) and application teams receive feedback when they are crafting policies that violate these requirements. This process is entirely automated, saving time for both security and application teams and enabling Network Policy to integrate into application teams CI/CD workflows.



genbit commented 3 minutes ago

Allow crawler service to talk to any outside cluster endpoint to port 443

Signed-off-by: Sergey Generalov sergey@genbit.ru

`Allow crawler to any port 443` ··· ✕ `f639cdc`

cimualtor added area/policy dont-merge/need-policy-review labels 1 minute ago

Add more commits by pushing to the **`pr/jobs-policy-443`** branch

All checks have failed
1 failing check

✕ **CI / policy-simulation (pull_request)** Failing after 3s — policy-simulation

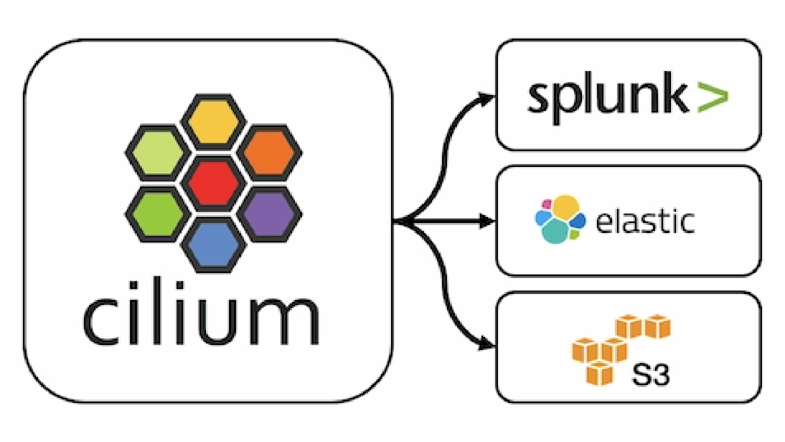
Required statuses must pass before merging
All required statuses and check runs on this pull request must run successfully to enable automatic merging.

As an administrator, you may still merge this pull request.

You can also open this in GitHub Desktop or view command line instructions.

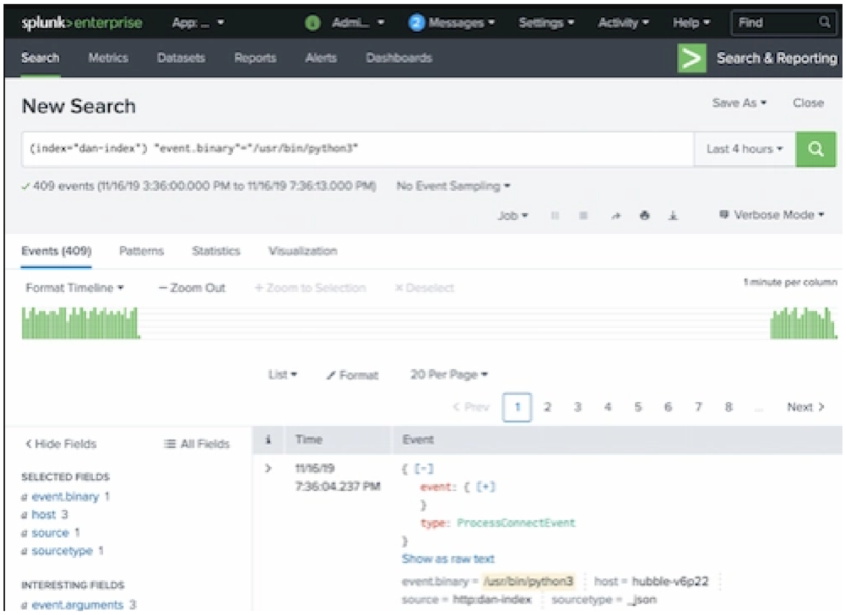
Identity-aware Event SIEM Export

Leverage Cilium's unique vantage point inside the network and the OS by exporting rich identity-aware events to any of the major SIEM and cloud storage providers without sacrificing performance and valuable compute resources. Flexible filtering and aggregation framework gives you control over what data to export, what signatures to alert on how much storage to consume.



Network Flow Visibility

Cilium efficiently extracts data about all network activities within the Kubernetes environment, providing L3/L4 and L7 flow events with full Kubernetes identity for pods and DNS-identity for external endpoints.



New Search

```
(index="dan-index") "event.binary"="/usr/bin/python3"
```

Last 4 hours

✓ 409 events (11/16/19 3:36:00.000 PM to 11/16/19 7:36:13.000 PM) No Event Sampling

SELECTED FIELDS
a event.binary 1
a host 3
a source 1
a sourcetype 1

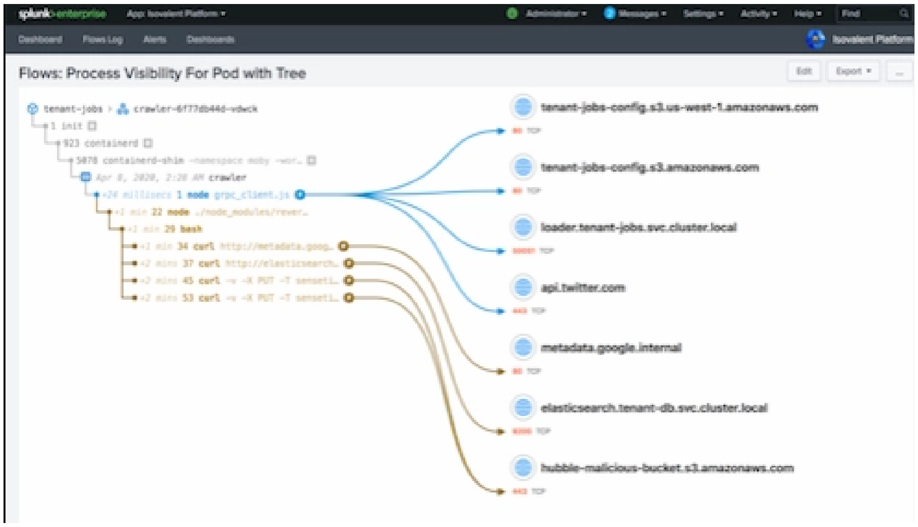
INTERESTING FIELDS
a event.arguments 3

i	Time	Event

>	11/16/19
	7:36:04.237 PM
		{ [-]
		event: { [+]
		}
		type: ProcessConnectEvent
		}
		event.binary = /usr/bin/python3 host = hubble-v6p22
		source = http:dan-index sourcetype = _json

Workload Runtime Visibility

Network flow data is combined with rich data about the binary executing inside the pod, including events for process execution with full process ancestry and associated security-relevant syscalls to investigate incidents and detect threats.



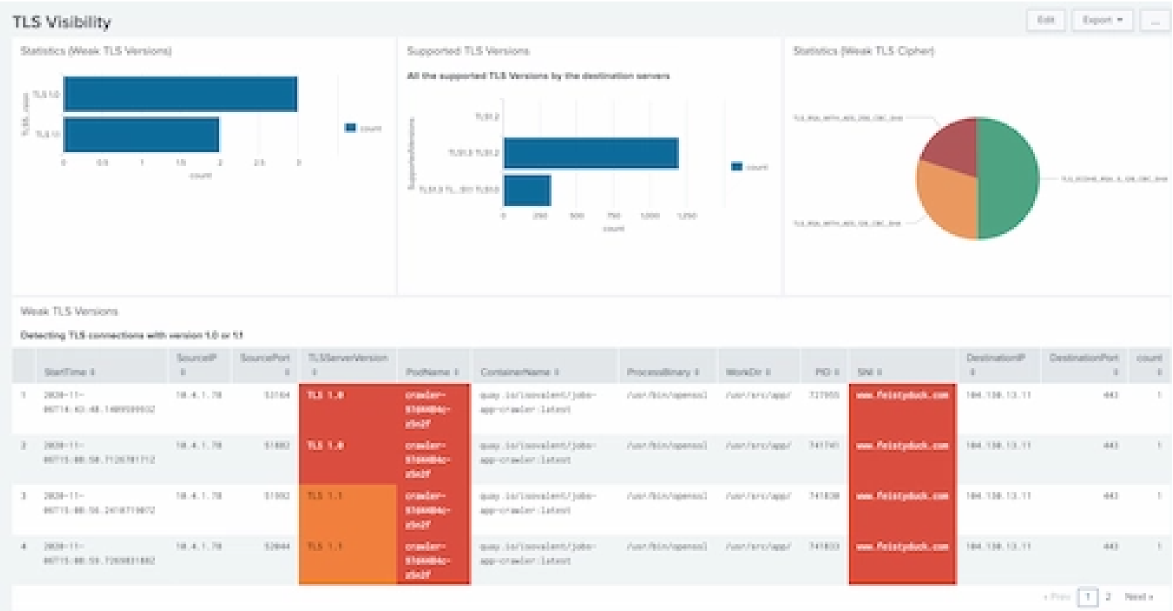
Flows: Process Visibility For Pod with Tree

```
tenant-jobs > crawler-6f77db44d-vdwck
└ 1 init
  └ 923 containerd
    └ 5078 containerd-shim -namespace moby -wor…
      └ Apr 8, 2020, 2:20 AM crawler
        └ +24 millisecs 1 node grpc_client.js
          └ +1 min 22 node ./node_modules/rever…
            └ +1 min 29 bash
              ├ +1 min 34 curl http://metadata.goog…
              ├ +2 mins 37 curl http://elasticsearch…
              ├ +2 mins 45 curl -v -X PUT -T senseti…
              └ +2 mins 53 curl -v -X PUT -T senseti…
```

- tenant-jobs-config.s3.us-west-1.amazonaws.com — 80 TCP
- tenant-jobs-config.s3.amazonaws.com — 80 TCP
- loader.tenant-jobs.svc.cluster.local — 50051 TCP
- api.twitter.com — 443 TCP
- metadata.google.internal — 80 TCP
- elasticsearch.tenant-db.svc.cluster.local — 9200 TCP
- hubble-malicious-bucket.s3.amazonaws.com — 443 TCP

Compliance Monitoring

Free your Security and Operation Teams from the need to review each policy change manually. Ensure that all traffic that needs to be encrypted is protected by the appropriate TLS version and ciphers, that the SNI matches the original destination DNS name, and that the certificate received is signed by a trusted certificate authority.



TLS Visibility

Weak TLS Versions

Detecting TLS connections with version 1.0 or 1.1

	StartTime	SourceIP	SourcePort	TLSServerVersion	PodName	ContainerName	ProcessBinary	WorkDir	PID	SNI	DestinationIP	DestinationPort	count
1	2020-11-06T14:43:48.[illegible]	10.4.1.78	53164	TLS 1.0	crawler-[illegible]-z5n2f	quay.io/isovalent/jobs-app-crawler:latest	/usr/bin/openssl	/usr/src/app/	737955	www.feistyduck.com	104.130.13.11	443	1
2	2020-11-06T15:08:58.[illegible]	10.4.1.78	51882	TLS 1.0	crawler-[illegible]-z5n2f	quay.io/isovalent/jobs-app-crawler:latest	/usr/bin/openssl	/usr/src/app/	741741	www.feistyduck.com	104.130.13.11	443	1
3	2020-11-06T15:08:56.[illegible]	10.4.1.78	51992	TLS 1.1	crawler-[illegible]-z5n2f	quay.io/isovalent/jobs-app-crawler:latest	/usr/bin/openssl	/usr/src/app/	741838	www.feistyduck.com	104.130.13.11	443	1
4	2020-11-06T15:08:59.[illegible]	10.4.1.78	52044	TLS 1.1	crawler-[illegible]-z5n2f	quay.io/isovalent/jobs-app-crawler:latest	/usr/bin/openssl	/usr/src/app/	741833	www.feistyduck.com	104.130.13.11	443	1

‹ Prev 1 2 Next ›

Transparent Encryption

Securing data in flight is an increasingly important requirement in security sensitive environments.

Cilium’s transparent encryption capabilities use the highly efficient IPsec capabilities built into the Linux kernel to automatically encrypt communications between all workloads within, or between, Kubernetes clusters.

This mechanism is simple: it requires only a single configuration setting in Cilium and no application changes. It is also highly efficient, with no side-car or other application layer proxying required.

> *We do hundreds of deployments per day and have clusters with thousands of pods... Cilium has allowed us to provide less friction to more and more teams while using modern technology to meet our security and regulatory requirements.*

Bradley Whitfield
Site Reliability Engineer
Capital One

About Isovalent

Isovalent builds software to connect, observe and secure cloud native workloads via it’s Cilium open source project and Cilium Enterprise product.

Cilium Open Source

Cilium Open Source provides eBPF-based networking, observability, and security with optimal scale and performance for platform teams operating Kubernetes environments across cloud and on-prem infrastructure.

Cilium Enterprise

Cilium Enterprise addresses the complex workflows related to security automation, forensics, compliance, role-based access control, and integration with legacy infrastructure that arise as platform teams engage with application and security teams within an enterprise organization.

US HEADQUARTERS

444 Castro St. STE 730
Mountain View, CA 94041 USA

SWISS HEADQUARTERS

Industriestrasse 25 8604
Volketswil Zurich, Switzerland

ISOVALENT

cilium