

Arion异常监控系统与其他相关开源软件对比

Wei Yue

12/2022

Arion异常监控系统与其他相关开源软件的对比

- **NetData**

- 没有探针动态加载机制
- 探针挂载不够灵活（例如socket只能按类挂载）
- 不涉及resource integrity 检测与保护

- **Pixie**

- 基于bpftrace的探针动态加载，具有一定的局限性，只能加载metrics collection的事件
- 没有动态异常上报以及即时处理的能力
- 不涉及resource integrity 检测与保护

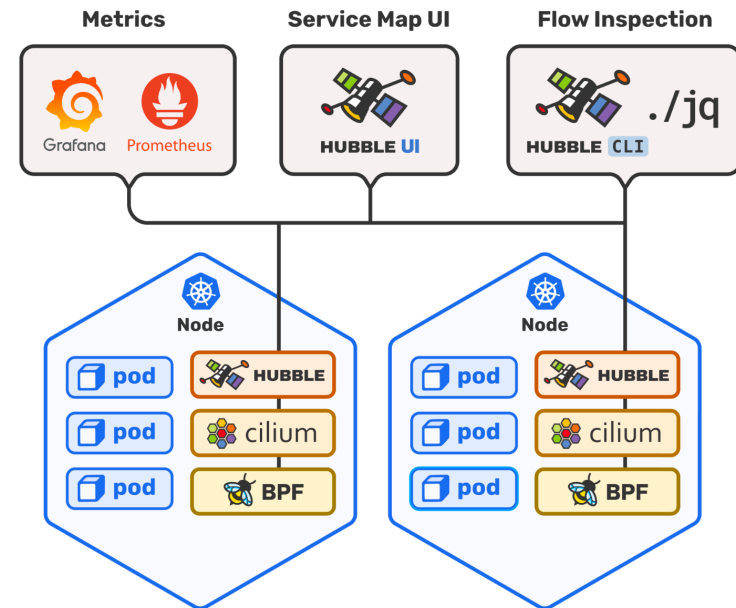
- **Arion Monitoring**

- 灵活的动态创建与部署监控event，监控事件不受限
- 对异常检测有即时上报以及本地处理的能力
- advanced resource access control机制（例如对eBPF map的保护）

Arion异常监控系统与其他相关开源软件的对比

- Hubble

- Cilium的eBPF based网络监控平台
- 主要监控能力包括：
 - service dependency graph
 - Metrics & Monitoring
 - Flow visibility
- 不具有动态创建以及部署监控event的能力
- 不涉及resource integrity 检测与保护

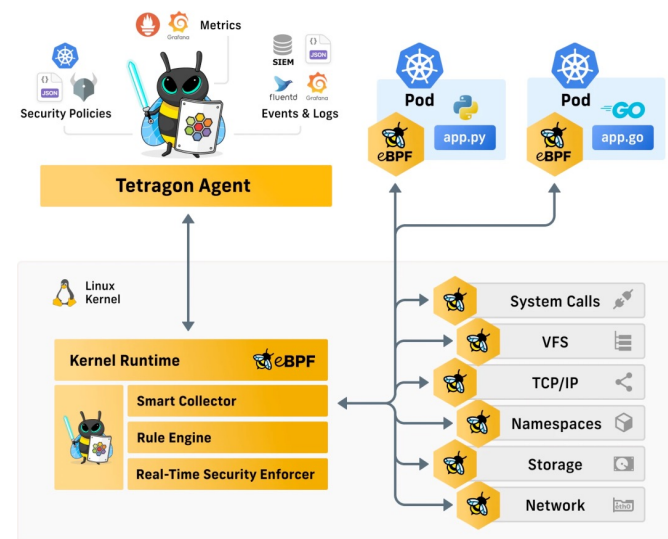


Arion异常监控系统与其他相关开源软件的对比

• Tetragon

- Cilium 针对Hubble的局限性，添加了实时性监控以及Runtime enforcement
- 有Enterprise和开源版，开源版功能 is limited
- 有了对敏感文件访问监控的能力（需集成Splunk）
- 理念上跟Arion monitoring system最接近（Tetragon在我们的proposal后开源），我们在propose后的技术探讨方案中所解决的一些问题也是Tetragon在试图解决的问题

- *Tetragon tightly coupled with Cilium*
- *Tetragon提供通用solution*
- *Arion 在场景deep dive基础上的 optimal solution*
- *Our advantage*
 - *快速闭环反馈机制基础上的动态部署*
 - *Advanced resource control mechanism*



Tetragon

Visibility

- Process & Syscall Visibility
- L3-L4 Network Visibility
- File Access Monitoring
- Capabilities & Namespacing

Enforcement

- System call-based enforcement (kprobes, tracepoints)

ISOVALENT

Tetragon Enterprise

Advanced Visibility

- Extended Network Visibility
- DNS, HTTP, HTTPS, TLS
- SIEM Integration
- Process Ancestry Information
- High-performance Protocol Parsers, Aggregation, & Filtering
- File Integrity Monitoring (Digest SHA256)

Advanced Enforcement

- Extended Runtime Enforcement Capabilities
- Threat Detection
- Baseline Policies

ISOVALENT