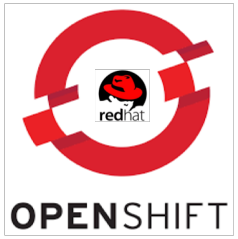
Sysdig and Red Hat Empowering OpenShift and Prometheus

Dmitriy Sandler
Senior Sales Engineer
@dmitriy_sandler

Sysdig



Sysdig snapshot

MISSION: Enable enterprises to operate reliable and secure containerized cloud-native applications

Company Snapshot

- Founded in 2013
- HQ in San Francisco; global presence
- $120M+ in capital from top-tier VCs
- Built on an open core with millions of downloads and a strong community

PROMETHEUS · SYSDIG INSPECT · FALCO · ANCHORE · KUBERNETES

Illustrative Customers

Disney · Northern Trust · Goldman Sachs · experian · Standard Chartered · COMCAST · BNY MELLON · MLS · Symantec · CISCO · American Express · worldpay · Shopify · Home Office · McKinsey&Company

Strong Momentum

- ARR growing exponentially
- Customers have a pattern of expanding scope and use cases
- Strong eco-system alliances

Red Hat OpenShift Container Platform · amazon web services · Google Cloud · IBM Cloud · MESOSPHERE · docker

Buying Catalyst: Containers in Production / Scale

"I cannot be in production with no ability to troubleshoot issues"

Bank Of New York

"Our internal audit has decided that OpenShift is now large enough and it is within the purview of their audit. They found a host of issues that we need to address immediately"

Barclays

"***Moving to a more modern platform using Openshift - Data needs to be more resilient and highly available because when sabre has issues., it makes the news"***

Sabre

"We are moving all our applications to the cloud…we need to know what happened, not just that it happened"

DnB

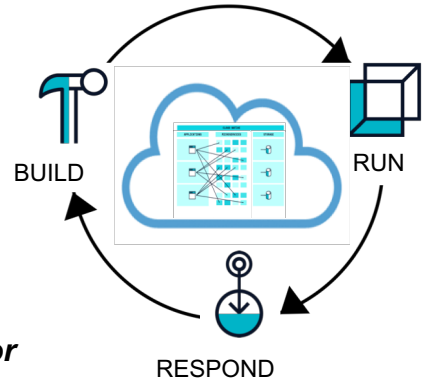
The challenge with cloud-native applications

"We need to be able to drill down from high level views all the way to mounted file systems within containers"

Fasthosts Internet

"Polling every 60 seconds is not enough when containers can come and go in seconds"

Top 5 Global Investement Bank



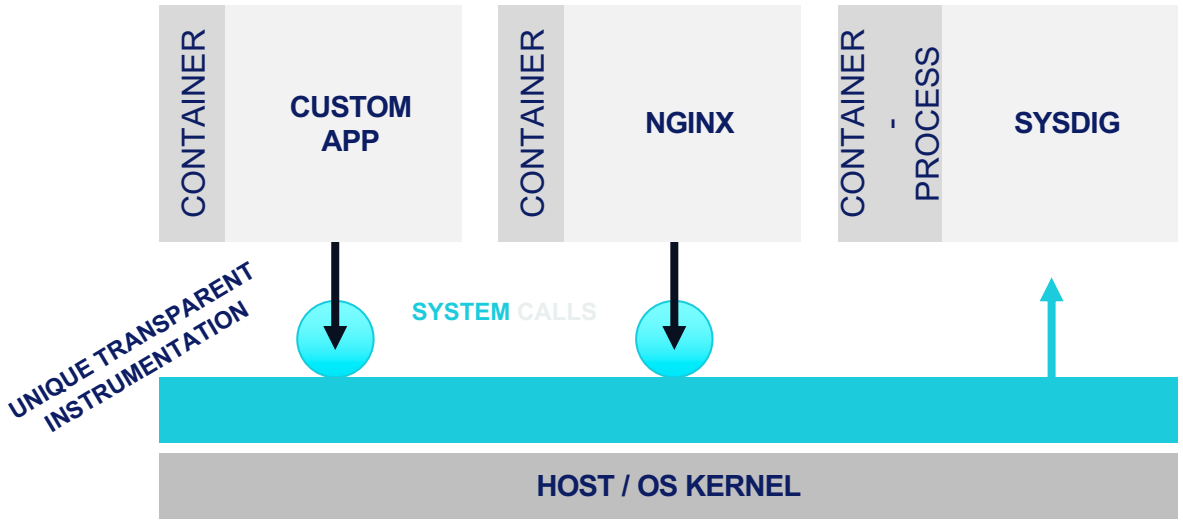
"How do we ensure PCI compliance for our Kubernetes environment in AWS and GCP?"

Nordstrom

"We have Newrelic but need operational monitoring…things are going to go wrong and we need to know within 5 minutes"

Premiere Global Services

Sysdig Architecture



Kernel instrumentation sees all app, container, host, and network system calls.
Monitor, detect, protect, and troubleshoot from a single instrumentation point.

Our Approach

Our Mission: Enable enterprises to operate reliable and secure containerized cloud-native applications

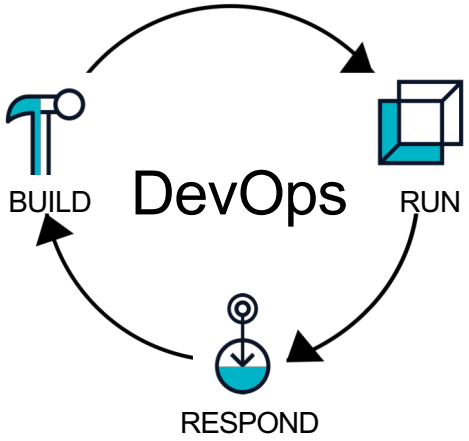
Comprehensive, scalable and context-rich record of all activity

Core principles:

1. No instrumentation
2. No pre-meditation = always on
3. Container-native
4. Applications and infrastructure
5. Deeper data

Automated monitoring, detection and forensics/ troubleshooting

Cloud-native operations is fundamentally a data challenge



BUILD

How can we scan & block vulnerable images and enforce best practices pre-production?

RUN

How can we block threats, enforce compliance and monitor application and service performance?

RESPOND

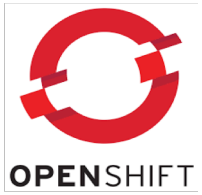
How can we proactively alert on incidents, reduce MTTR with forensics, and capture detailed audit records?

SYSDIG

Solution Portfolio.

Robust commercial software offerings…
Built on the most popular cloud-native open source solutions.

Stronger Together:



End-to-end Security

Scanning
Compliance
Runtime Detection
Incident Response
Forensics

Deep troubleshooting and observability across the stack

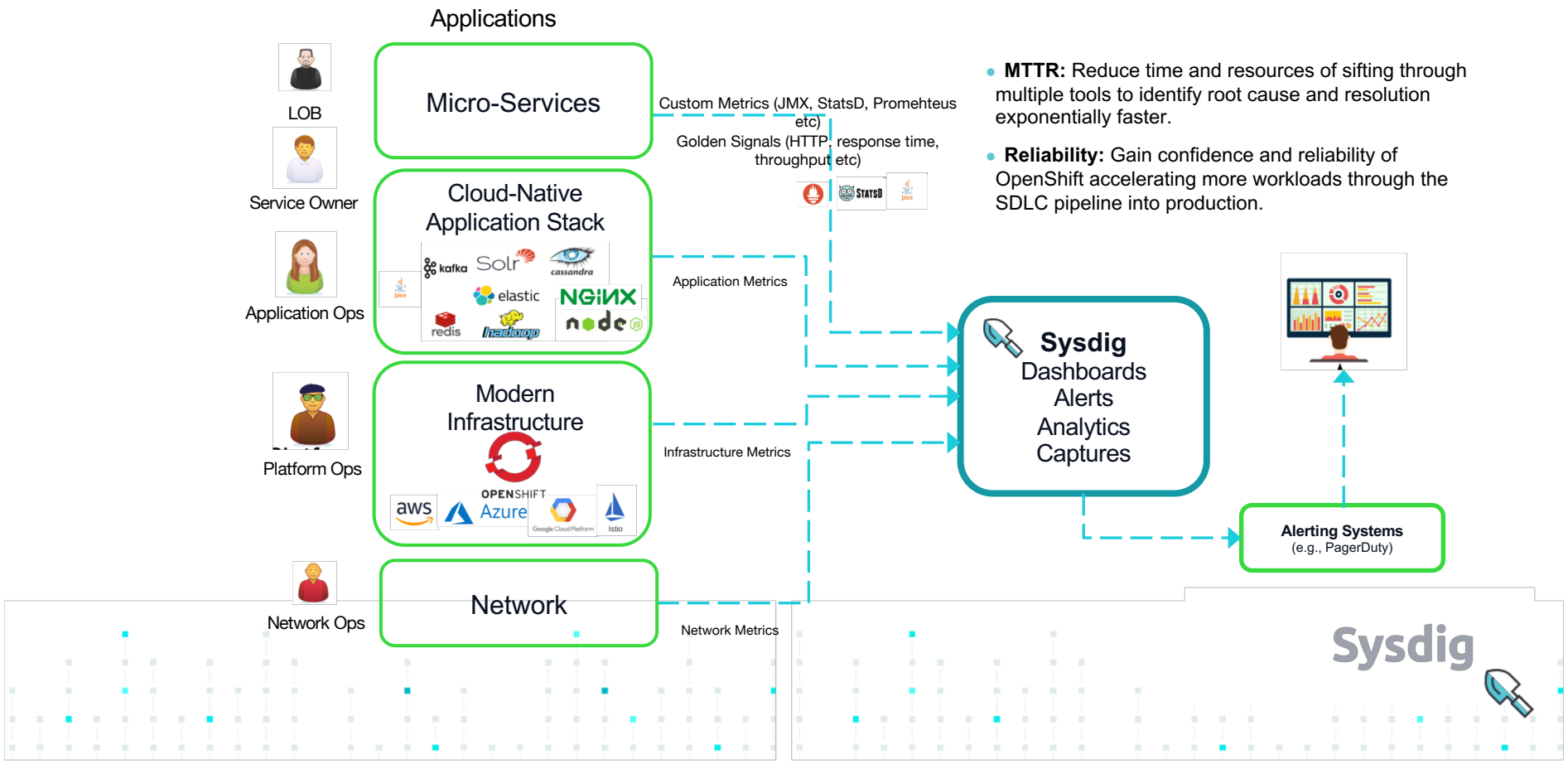
Applications
Middleware
Infrastructure (hosts & containers)
Orchestrators
Cloud Platforms
Network connections
Process and syscall activity
Custom metrics
Events

Enterprise-grade Prometheus

Scalable
Simple
Secure
Supported
Service Topology and workflows

Sysdig

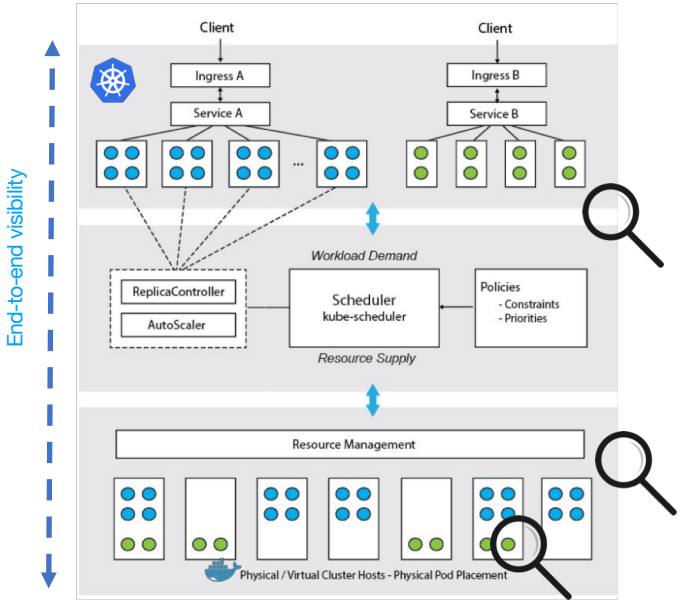
Telemetry across the **stack**, across **clusters**, across **clouds**



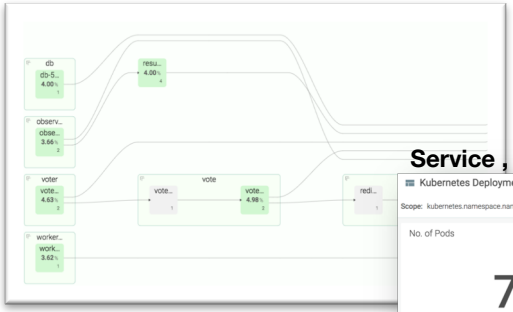
- **MTTR:** Reduce time and resources of sifting through multiple tools to identify root cause and resolution exponentially faster.
- **Reliability:** Gain confidence and reliability of OpenShift accelerating more workloads through the SDLC pipeline into production.

Dynamic Service Monitoring & Troubleshooting

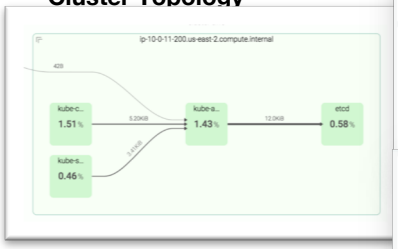
- Dynamic **discovery** of micro services
- Deep **Kubernetes insights** (native monitoring of kube components, kube-state metrics, Istio monitoring, out of the box dashboards & alerts)
- **Service level topology**, dashboards and alerts
- **In depth troubleshooting** from service level down to infrastructure level to system call level
- **Multi-tenant**, service based teams and roles



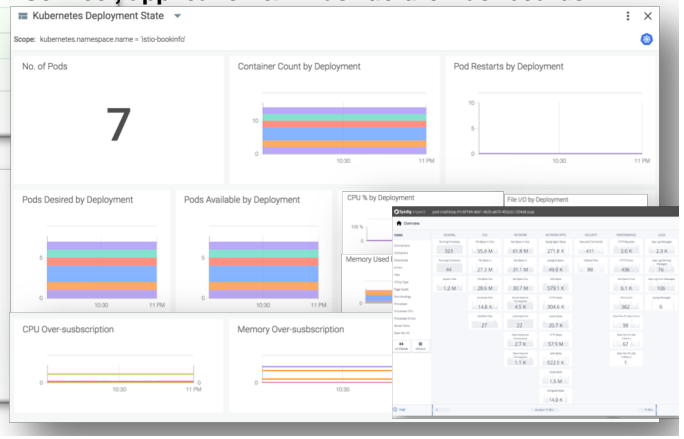
Service Topology

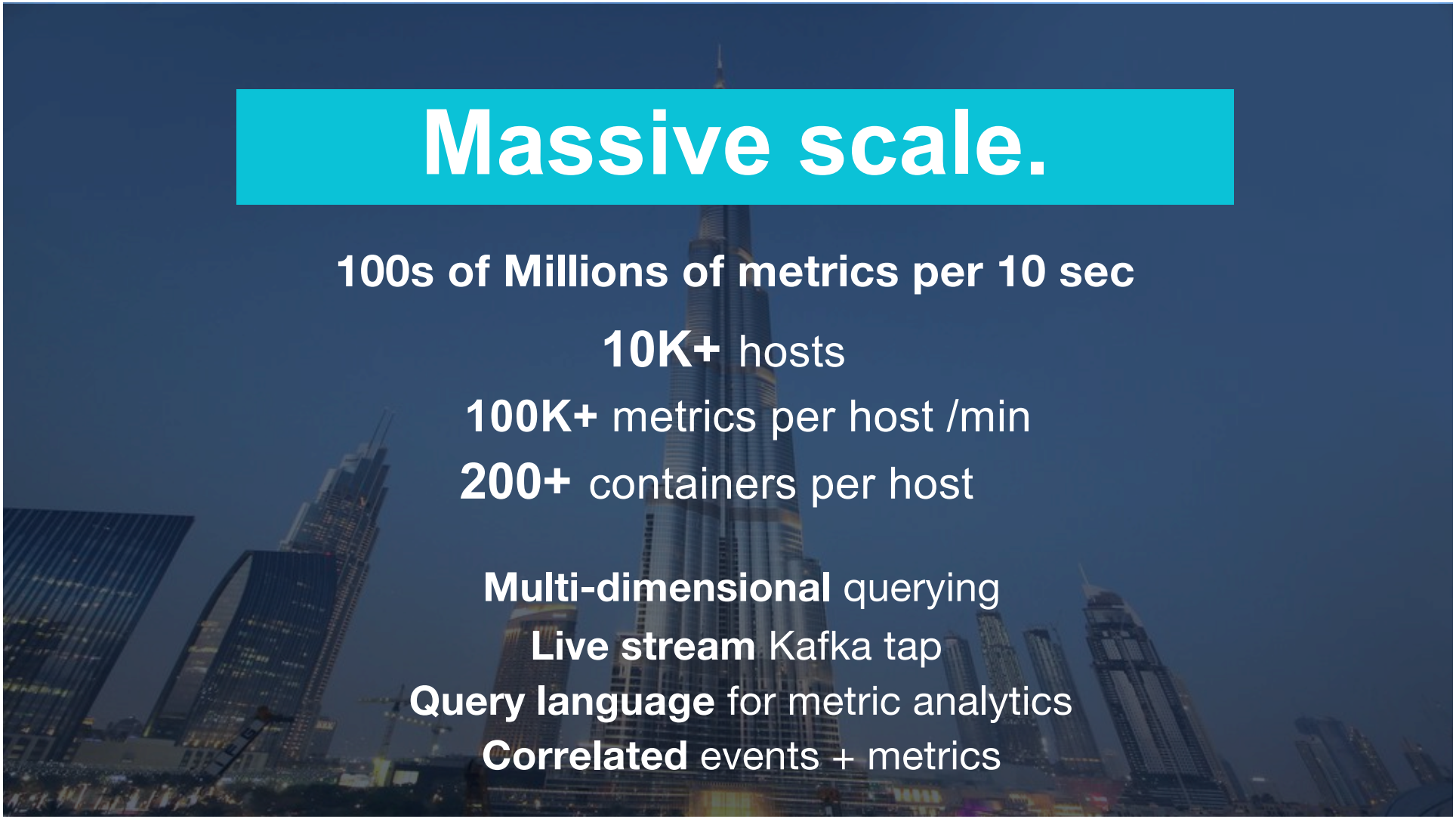


Cluster Topology



Service , application & infrastructure Dashboards




Massive scale.
100s of Millions of metrics per 10 sec
10K+ hosts
100K+ metrics per host /min
200+ containers per host
Multi-dimensional querying
Live stream Kafka tap
Query language for metric analytics
Correlated events + metrics

Prometheus Customer journey: adopt, expand, scale

Stage #1: dev-led, single app, DIY

Who: App developers or service owners

What: Grafana community dashboards
PromQL queries to create flexible dashboards & alerts

Why: Prometheus + Grafana enables them to instrument & monitor their code using a combination of open source prom exporters for well-known services + their own custom metrics

How do I…?

…scale metrics per sec (1,000 → 15,000)

…view multi-cluster cloud?

…run a global query across clu

…view data older than 2

…view service-to-service performance?

… integrate with enterprise workflow?

… What is my troubleshooting workflow?

cortex M3

Step #2: scale out, multi-cluster, multi-cloud

Sysdig's Enterprise Prometheus (Turn key)

Easily scale out to 100M metrics / second*
Service-oriented workflow & topology for problem isolation
Troubleshooting detection, isolation & resolution
Simple deployment
Simple user experience for all users (plus PromQL)
Long term data retention
HA and Disaster Recovery
Access control, data isolation
Enterprise-grade support

Scale out w/ Thanos / Cortex / M3 (DIY)

Why: Federated scale out model
~~Service-oriented workflow & topology for problem isolation~~
Troubleshooting detection, isolation & ~~resolution~~
~~Simple deployment~~
~~Simple user experience~~ users *requires* (PromQL)
Long term data retention
HA and Disaster Recovery
Access control, data isolation
Enterprise-grade support (soon)

cortex M3

Enterprise Prometheus from Sysdig

Auto-discovery, collection and tagging: Ingest and visualize Prometheus metrics automatically with no developer changes.

Scalability, reliability and long-term data: Industry-leading, horizontally scalable metric store, long-term data retention, full HA and highly performant querying at 100s of millions of metrics/sec.

Multi-cluster, multi-cloud visibility: Aggregate, query, and visualize metrics and events across data centers, clusters, and clouds.

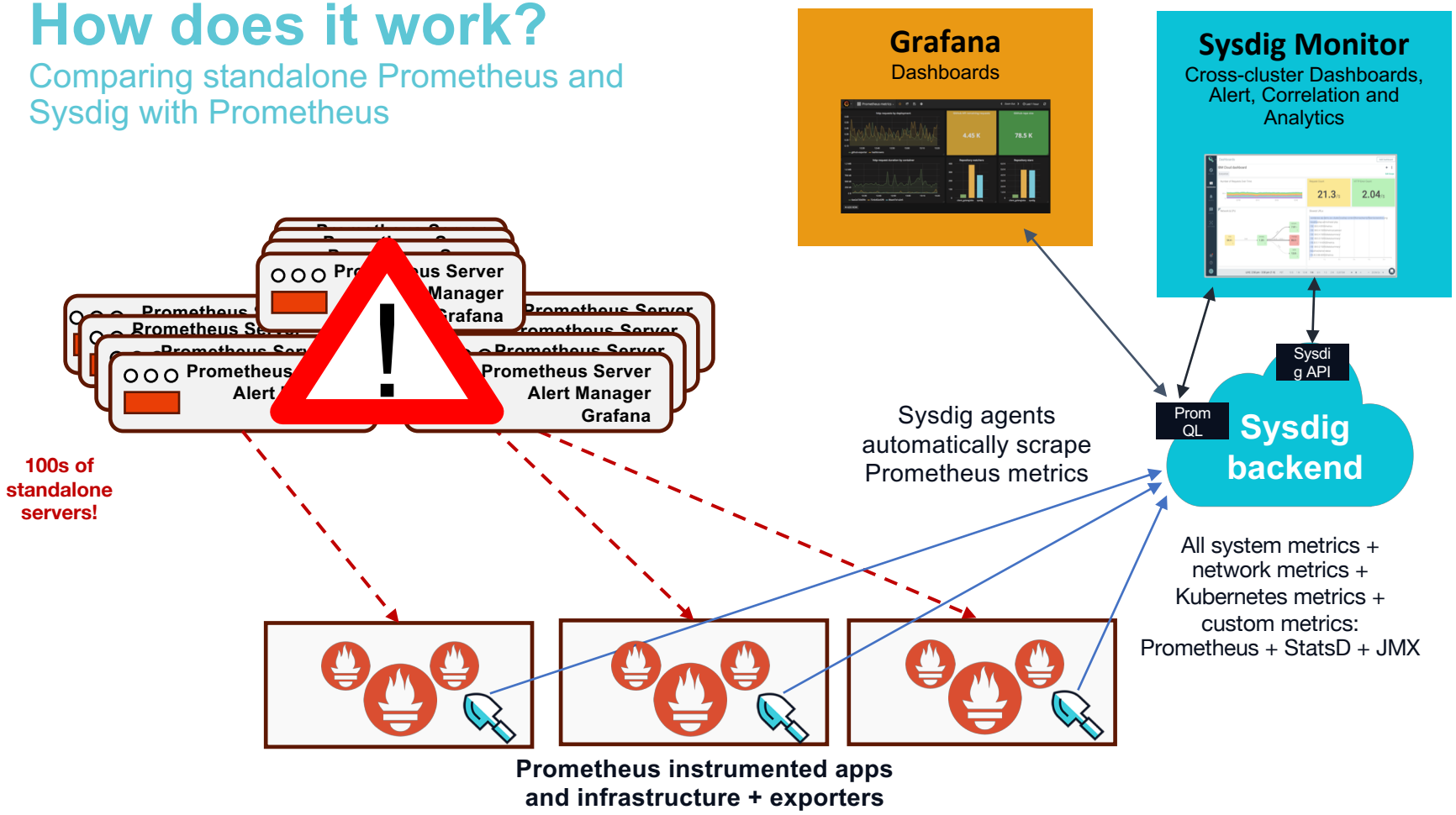
Service-oriented workflow and topology maps: Tooling and workflows designed for microservices without code instrumentation or pre-meditation

Deep troubleshooting out-of-the-box: Full-stack telemetry from services, applications and infrastructure down to the container process with network level data with event correlation. No hooks, plugins or additional configurations to collect data at any layer.

Lower total cost of ownership with an enterprise-ready solution: Role-based access control, Teams, encryption, audit and compliance, support and more.

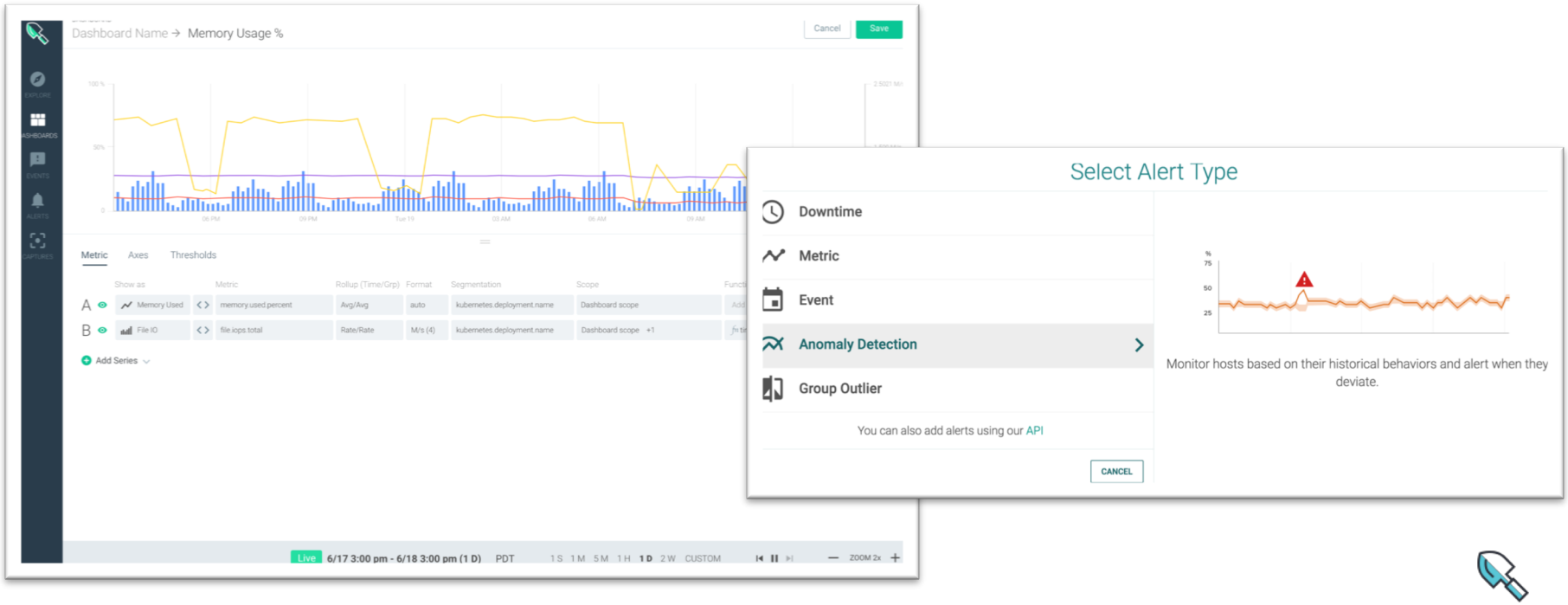
How does it work?

Comparing standalone Prometheus and Sysdig with Prometheus

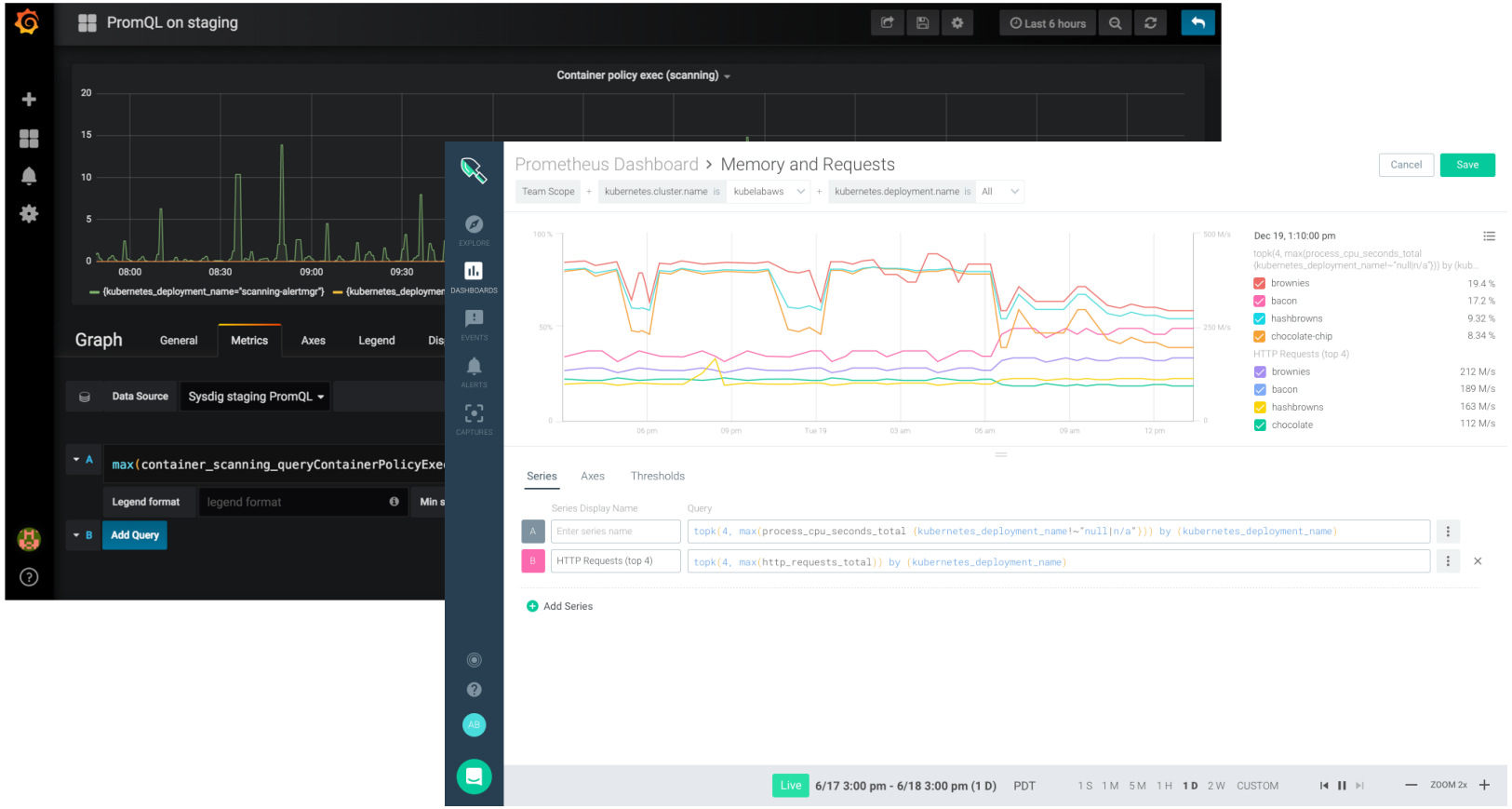


Dashboarding and Alerting

- Rich and flexible dashboarding
- Real time alerting and anomaly detection
- Best practices based out-of-the-box dashboards and alerts



Building charts with Prom Query Language



End-to-End Security for Microservices

BUILD

VULNERABILITY MANAGEMENT

CI/CD, static image scanning, runtime vulnerability management.
Openshift provides with OpenSCAP.

RUN

RUNTIME DETECTION

Identify and block threats in real time, prevent lateral movements based on behavioral intelligence

RESPOND

FULL STACK FORENSICS

Drill down from policy violations into 100% granularity captures of pre- and post-attack activity.

COMPLY

AUDIT & COMPLIANCE

Schedule compliance scans, log user actions, and command-line arguments.

SERVICE ORIENTED SECURITY

Protect distributed, dynamic, and ephemeral services with a single service policy and no manual configuration.

Red Hat and Sysdig – Stronger Together

Pillar 1: Security- Openshift provides Image Scanning and integration with CI/CD process via OpenSCAP. Better together with system call level security and behavioral analysis along with deep forensics to better understand the internal or external actors motives and address accordingly.

- ***Run time security:*** *stop zero day and internal threats, prevent lateral movements based on behavioural intelligence*
- ***Enforcement & Forensic Captures*****:** Create detailed system captures for any policy violation or incident enabling ability to take actions against malicious activity.
- ***Service Oriented Incident Response*****:** View of your security policy violations based on orchestrated services.

Pillar 2: Troubleshooting/ Reliability - Sysdig's unique instrumentation point allows Openshift users to take advantage of troubleshooting capabilities to provide your nodes, pods, services, and deployments an additional highly potent reliability tool… even after your pods or services are no longer there… providing better Root Cause and Mean Time to Repair

- ***MTTR:*** *Reduce time and resources of sifting through logs to identify root cause and resolution exponentially faster.*
- ***Reliability:*** *Gain confidence and reliability of OpenShift accelerating more workloads through the SLDC pipeline into production.*

Pillar 3: Enterprise Grade Prometheus- what does that mean on top of all the goodness you receive with OpenShift's exciting Prometheus OOTB support: The 5 S's will help your OpenShift Platform be your platform of choice for your container workloads.

- ***Scale*****:** Provides a horizontally scalable distributed Collector that handles tens of millions of metrics per second with cross-cluster aggregation to keep pace with large, complex environments.
- ***Scope*****:** Collects, analyzes, and correlates Prometheus metrics with granular metrics and events for system processes, applications, cloud platforms, networks, orchestrators, and customer metrics like StatsD and Java TM Management Extensions (JMX), with advanced visualizations like topology maps.
- ***Simplicity*****:** Reduces complexity with a turn-key solution that eliminates the headaches of managing multiple isolated monitoring systems and services.
- ***Security*****:** Integration with Openshift's Industry leading RBAC and Secrets Management
- ***Support*****:** Extends technical support and services to enterprise Prometheus users to resolve issues more rapidly

All this with one platform…..OpenShift+Sysdig